Backup Exec 2010 R3
Agent for VMware Virtual Infrastructure
Technical Feature Brief
Contents

Introduction........................................................................................................................................................................3
Business Value..........................................................................................................................................................................3
Underlying Principles.................................................................................................................................................................5
Licensing Considerations............................................................................................................................................................8
Agent for VMware and Other Backup Exec Agents and Options............................................................................................10
Backup Exec Management Plug-in for VMware........................................................................................................................14
Performance Recommendations.....................................................................................................................................................16
Configuration Examples.................................................................................................................................................................17
Current Limitations........................................................................................................................................................................18
For More Information.................................................................................................................................................................19
Introduction

This feature brief is primarily intended to assist technical personnel as they design and implement Backup Exec and the Agent for VMware Virtual infrastructure, and make related decisions. Additionally, the business value of the Backup Exec Agent for VMware Virtual Infrastructure (referred to commonly as the VMware Agent in this document) and the licensing of the VMware Agent will be touched upon lightly in this feature brief.

For step-by-step instructions on installing and configuring Backup Exec or the Agent for VMware Virtual Infrastructure, consult the Backup Exec Administrator’s Guide.

This feature brief will help technical personnel as they make design and implementation decisions for Backup Exec and the Agent for VMware through the exploration of the following topics:

- How Backup Exec integrates with the VMware platform
- Technical requirements of certain key features
- Best practices
- Pitfalls and things to avoid
- Performance factors
- Agent limitations
- Example configurations

Business Value

VMware’s Virtual Infrastructure 3 (VI3) and vSphere 4.0 have become widely adopted in organizations that want to adopt virtualization in their IT environments to reduce costs. As a result of larger numbers of systems becoming virtualized, companies are looking for more efficient backup and recovery of their virtual systems to maintain business productivity and cost savings that server virtualization delivers. This includes not only the guest virtual machines, but also the applications that have been installed on those guest virtual machines, such as Microsoft Exchange®, SQL Server®, and Active Directory®. A lost VMware server could impact productivity for up to several hours, or even days, for multiple departments while the IT administrator struggles to recover the virtual environment and the individual guest virtual machines.

Designed for Virtual Environments

Administrators who want to protect their VMware environments understand the frustration and time involved with backup technologies that are not built specifically for protecting virtual environments. Administrators and companies who rely upon classic backup and recovery solutions that are not specifically designed for virtual environments will face several limitations, such as:

- Impacting the Virtual Environment performance when processing backups inside Virtual Machines
- Having to shut down guest virtual machines in order to protect them completely
- Slow file-by-file backups that capture redundant data in each guest virtual machine over and over
- Long restores of an entire guest virtual machine in order to recover a single file
- Separate backups for virtualized applications like Microsoft SQL, Active Directory, and Exchange
- Not being able to leverage SAN backups for fiber connected virtual machine DataStores
Integration with the Latest VMware Technology

Backup Exec 2010’s Agent for VMware natively incorporates VMware’s latest backup technology, the vStorage API, to help eliminate these challenges and provide faster backups with less overall storage consumption. This is accomplished through the following:

- VMware “Ready” certified integration with VMware vStorage API’s for Data Protection
  - Enables backup of all guest virtual machines
  - Eliminates the need to shut down production virtual machines in order to protect them properly
- vSphere block-level Incremental and Differential backups
  - Differential backup: Enables quick and efficient backup of only what has changed in the guest virtual machine since the last full backup
  - Incremental backup: Enables quick and efficient backup of only what has changed since the last backup
  - Add integrated data deduplication technology to further reduce backup storage requirements
- Integrated Granular Recovery Technology
  - From a single-pass, high-speed, backup of the virtual machine, you can recover the entire guest virtual machine, individual files/folders, entire applications or granular application objects
  - Restore data to the original or alternate location, even to a folder (e.g. D:\Recovery)
  - Upgrade Virtual Machines to hardware version 7 on restore
  - Convert a Virtual Machine originally provisioned as “Thick” to “Thin” on restore
- Improved Microsoft VSS Integration
  - Enables proper protection of applications, such as Exchange, SQL, or Active Directory, as part of the entire guest virtual machine, including application quiescence and log truncation
  - Combined with Granular Recovery Technology, support for individual item or database recovery from Exchange, SQL, or Active Directory

Complete Virtual and Physical Protection in a Single Solution

The enhanced Backup Exec 2010 VMware Agent delivers complete disk-to-disk-to-tape-based data protection for growing VMware virtual environments while protecting existing physical server environments through one flexible console. Backup Exec 2010 can quickly restore individual files and folders from a single image-level backup; eliminating the time and storage requirements of a second file-level backup.

- One agent delivers comprehensive data protection to an unlimited number of VMware virtual guest systems.
- Comprehensive backup support for both virtual systems and legacy physical systems in one backup solution, supporting disk and tape storage environments.
- Integration with VMware’s vStorage API to maximize backup and recovery performance
- Granular data recovery for VMware Infrastructures saves time and lowers cost
- Backup and restore virtual machine data over high-performance SAN transport modes

Backup Exec’s VMware agent offers the additional benefit of off-host backups, alleviating the burden of backup-related I/O operations from the hypervisor hosting production virtual machines and moving it to the Backup Exec media server. This represents another significant advantage of the Backup Exec VMware Agent when
compared to many legacy backup products that protect virtual machines as if they were standalone physical systems, forcing the hypervisor to take the full load of I/O operations for backup purposes. Backup Exec interacts with ESX servers through the vStorage API to capture snapshots at the virtual machine DataStore level.

**Underlying Principles**

**VMware vSphere Resource Discovery**

When configuring Backup Exec to protect VMware resources using the Backup Exec Agent for VMware, ESX hosts and their guest virtual machines can be discovered in one of two ways:

- Entering the ESX hostname or IP address into the Backup Exec interface
- Connecting to an available vCenter server for the discovery of multiple ESX hosts and their associated virtual machines

Backup Exec 2010 uses VMware Web Services for most communications with vCenter servers for ESX 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. In order to discover VMware resources through an available vCenter server, either Backup Exec itself or the Backup Exec Agent for Windows Servers (AWS) must be installed to the vCenter server.

**Backup Data Transport Modes**

When transporting backup data from an ESX host to the Backup Exec media server for storage, Backup Exec leverages integration with the VMware vStorage API, 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 the requested backup data can be transported from the ESX host to the Backup Exec media server. After a data request has been made by Backup Exec, the vStorage API returns a list that states what transport modes (SAN, NBD, HOTADD, etc) are supported and available. Based on this list, along with the list supplied by the user, a transport mode will be selected.

For SAN environments, it’s important to note that if Backup Exec is unable to access the SAN at the time of a backup or restore operation, it will revert to other available data paths (e.g. ethernet).

A transport mode is the physical data path leveraged for moving backup data from the source ESX server to the Backup Exec media server. The following transport modes are supported by Backup Exec 2010:

<table>
<thead>
<tr>
<th>Transport Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAN</td>
<td>Uses iSCSI or Fiber Channel shared storage for data transfers</td>
</tr>
<tr>
<td>NBD</td>
<td>Uses the LAN/ethernet for data transfers</td>
</tr>
<tr>
<td>NBDSSL</td>
<td>Uses the encrypted LAN/ethernet for data transfers</td>
</tr>
<tr>
<td>HOTADD</td>
<td>Uses a virtualized Backup Exec media server that exists as a virtual machine</td>
</tr>
</tbody>
</table>

Ultimately, transport mode selection is determined through a combination of Backup Exec and VMware. When selecting a transport mode, Backup Exec submits a prioritized list (preferred modes first) of the modes we would
Backup Exec 2010 R3 Agent for VMware Virtual Infrastructure: Technical Feature Brief

like to use for the backup job to VMware, and VMware decides what it will use based on the return call from the VMware API.

If incorrect or unexpected transport modes are being used for backup or recovery, it may be helpful to disable all transport modes except the desired transport mode as a troubleshooting step. This can be done under Options > Settings > VMware in the Backup Exec interface. If the job fails, review job logs for a better understanding of the root cause.

Also ensure SAN/LUNs are visible and accessible from the Backup Exec media server with read and write access. If not, the backup job will fail (if only SAN mode is selected). The inability of the Backup Exec media server to access the SAN/LUNs is one of the possible reasons why Backup Exec would switch back to the LAN for data transport instead of the SAN.

Transport Mode Options

Users can select one or more transport modes from a list of supported modes and adjust which modes are tried first (move up/move down in screenshot below).

The transport mode options are located in the Backup Exec interface under Options > Settings > VMware:

![Transport Mode Options Screenshot](image)

VMware vStorage API

The Backup Exec VMware Agent fully integrates the latest version of VMware’s vStorage API’s for Data Protection and provides a number of new capabilities, including:
Backup Exec 2010 R3 Agent for VMware Virtual Infrastructure: Technical Feature Brief

- Improved overall backup and restore performance, particularly in SAN-based environments
- Changed-block tracking for fast block-level Incremental/Differential backup
  - Requires vSphere 4.x
  - Requires Hardware Version 7-“formatted” virtual machines
- Backup and recovery support of both thin and thick-provisioned virtual disks
- Template virtual machine backup
- SAN-based backup and restore of virtual machines.

The Backup Exec VMware Agent supports the protection of existing ESX 3.5 Update 2 (and later) guest virtual machines and vSphere 4.0 (including vSphere 4.0 Update1) and vSphere 4.1. You can even mix ESX 3.5 and vSphere 4.0 backups together in the same backup job without the need to modify any additional settings.

The vStorage API provides all of the capabilities of VCB as well as a number of new capabilities. It also eliminates many of the shortcomings of the original VCB technology. Symantec has worked closely with VMware to integrate the vStorage API into Backup Exec 2010 to ensure it meets the needs of our customers.

Proxy Server Elimination

vStorage API’s for Data Protection eliminate the need for a separate VCB “Proxy Server”. Symantec and VMware have worked closely together to ensure that performance impacts during backup are minimal. Customers utilizing vStorage API’s for Data Protection in Backup Exec 2010 can expect a significant performance improvement over VCB in both CPU and I/O impacts during backups. Typical CPU utilization during backup with vStorage API’s for Data Protection ranges between 1-4% throughout the duration of the backup while maintaining constant I/O rates. Backups are based on temporary snapshots, which are low-impact and low in disk-space consumption.
Compression and Encryption

Whether or not it's possible to utilize compression and/or encryption features of Backup Exec when protecting VMware resources with the VMware Agent depends on the backup device to which data is being stored and whether or not the backup jobs are GRT-enabled.

GRT-enabled backup jobs stored to backup-to-disk devices cannot be encrypted or compressed since they are stored in native (VMMDK) format. If backup jobs are stored to tape devices or do not have GRT enabled, they can be compressed or encrypted, or both.

Licensing Considerations

Another advantage of Backup Exec’s VMware Agent when compared to other solutions in the market is its simplified licensing system. A single VMware Agent allows for full file and image-level protection of all guest virtual machines on a single hypervisor host (ESX server). There is no need to worry about how many virtual machines an ESX server is hosting or how many CPU cores the ESX server contains. One license of the VMware Agent offers full file-level and image-level protection of an ESX server and all virtual machines that it hosts.

Application agents, which enable the proper protection of key applications as well as granular recovery of those applications, are licensed separately.

Here is an example VMware environment protected by Backup Exec:
The above environment includes a Backup Exec media server, a VMware ESX server, and four guest virtual machines. The four guest virtual machines above can be described as follows (from left to right):

- Linux server
- Windows server hosting Microsoft Exchange
- Windows file server
- Windows server hosting Microsoft SQL

This environment would require the following Backup Exec licenses in order to be both fully protected and fully in compliance with license requirements:

<table>
<thead>
<tr>
<th>Backup Exec Component</th>
<th>Required Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Exec Server</td>
<td>1</td>
</tr>
<tr>
<td>Agent for VMware Virtual Infrastructure</td>
<td>1</td>
</tr>
<tr>
<td>Agent for Microsoft Exchange</td>
<td>1</td>
</tr>
<tr>
<td>Agent for Microsoft SQL</td>
<td>1</td>
</tr>
<tr>
<td>Agent for Windows Servers</td>
<td>0</td>
</tr>
<tr>
<td>Agent for Linux/Unix Servers</td>
<td>0</td>
</tr>
</tbody>
</table>

In this example environment, the Backup Exec Server license and the VMware Agent license are required to protect the VMware ESX server. With these two licenses, full off-host protection of all guest virtual machines is possible including file/folder granular recovery and full image-level virtual machine recovery.

The Agent for Microsoft Exchange and the Agent for Microsoft SQL enable advanced application protection and recovery capabilities within Backup Exec for the applications they are designed to protect. This includes proper
application quiescence and log truncation at the time of backup, as well as full application recovery and granular application recovery capabilities. In order to unlock these advanced application protection capabilities in this example environment, one license for the Agent for Microsoft Exchange and one license for the Agent for Microsoft SQL must also be purchased.

File/folder and full image-level virtual machine recovery capabilities for all virtual machines on a single ESX server are included with the VMware Agent license.

It is not necessary to install the Backup Exec Agent for Windows Servers into protected virtual machines for file/folder and full image-level virtual machine recovery. Backup data is generated at the host level through the vStorage API, and is not gathered by the Backup Exec Agent for Windows Servers. However, if for other reasons it is desired to install the Backup Exec Agent for Windows Servers into one or more guest virtual machines on a protected hypervisor (for example, in order to recover files and folders directly back to the virtual machine), this is included in the host license.

Other options that unlock additional Backup Exec capabilities, such as the Deduplication Option, are licensed separately and are not included in the VMware Agent license.

Agent for VMware and Other Backup Exec Agents and Options

VMware Agent and Application Protection Agents

It is important that Backup Exec Database or Application Agents continue to be licensed and installed inside of guest virtual machines. Backup Exec 2010 introduces a new industry-first technology for virtualized applications using its patented Granular Recovery Technology (GRT) in combination with the Agent for VMware Virtual Infrastructure.

This new virtualized application GRT capability removes the need for separate regular database- or application-level backups of virtualized applications, such as:

- Microsoft SQL Server (2005-2008 R2)
- Microsoft Exchange Server (2003-2010 SP1)
  - Note: Exchange 2010 Distributed Availability Groups are not supported for virtualized application GRT restores
- Microsoft Active Directory (2003-2008 R2)

The Backup Exec 2010 VMware Agent can interact with these applications when the Backup Exec Agent for Windows Servers is installed inside of the guest virtual machines hosting these applications and the appropriate Backup Exec Agent for SQL, Exchange, or Active Directory is licensed at the associated media server. This combination allows for the following capabilities to be enabled:

- **Virtualized Application Discovery** - The Backup Exec Agent for Windows Servers facilitates the discovery of any virtualized applications inside of a guest virtual machine without the need to browse the virtual machine and select the application resource specifically. The agent also collects application metadata at the time of backup.

  Without installing the Backup Exec Agent for Windows Servers into the guest virtual machine, the entire VM will be backed up at the image level without specific intelligence about the application hosted inside.
Backup Exec 2010 R3 Agent for VMware Virtual Infrastructure: Technical Feature Brief

- **Granular Application Object Recovery** - When the appropriate application agent has been licensed at the media server, the Backup Exec Agent for Windows Servers—which has been installed into the guest virtual machine that hosts the application—enables the granular recovery of associated application objects as well as point-in-time recovery of the application itself. All of these advanced recovery options are possible from a single pass, off-host backup of the virtual machine using the Backup Exec Agent for VMware. No additional SQL, Exchange, or Active Directory backup needs to be performed.

**Application Quiescence and Log Truncation** - Key Microsoft applications and databases require regular log truncation, database maintenance, consistency checks, and other maintenance-related tasks that are performed only as part of a regular Backup Exec database or application agent-level backup.

If these separate Database Agent-level backups are not performed regularly, application log files could continue to accumulate, eventually fill the entire disk, and cause application or database failure.

Applications that utilize the Microsoft Volume Shadow Copy Service (VSS) framework on Windows 2003 and 2008 systems can be protected as part of a normal image-level backup of the entire guest virtual machine with the Backup Exec Agent VMware Agent. There are two options for obtaining a VSS “Requestor/Provider” for your Windows guest virtual machines running Windows 2003 or later:

- A generic version can be obtained as part of ESX 3.5 Update 2 from VMware and is automatically installed as part of the normal VMware Tools installation.
- (Recommended) A VSS provider that is specific to Backup Exec can be installed inside of the guest virtual machine to replace the default VMware version by simply installing the Backup Exec Agent for Windows Servers inside of the guest virtual machine.

Backup Exec 2010 will automatically detect the presence of the VMware Tools version and replace it with the correct Backup Exec version. Please see your Backup Exec 2010 Administrator’s Guide for more details on how to install the Backup Exec Remote Agent for Windows Servers.

Application transaction logs are an important element to protecting your virtualized applications. Backup Exec 2010 provides new capabilities to assist you in the proper protection of your virtualized applications and their transaction logs. For this reason, it is recommended that the Backup Exec Agent for Windows Servers (also known as the Backup Exec Remote Agent) be installed inside of the guest virtual machine with the appropriate Backup Exec Agent (SQL, Exchange, or Active Directory) license key installed on the Backup Exec 2010 server.

Exchange and Active Directory transaction logs will be properly truncated automatically as part of your normal backups of the guest virtual machine. SQL installations inside of guest virtual machines will still require a separate log-level backup to properly truncate the transaction log of SQL.
VSS Provider Considerations

Each VSS Requestor/Provider from either VMware or Symantec should be installed separately, and never on the same system at the same time. Please uninstall the Backup Exec Agent for Windows Servers if you are reinstalling the VSS provider version that VMware Tools provide.

Non-VSS Compliant Applications

Applications that are installed in Windows or Linux guest virtual machines that are not VSS-compliant, such as Lotus Domino, Oracle, SAP, and DB2 cannot be properly quiesced using the VMware or Backup Exec VSS Requestor/Provider. Image-level backups of these virtual machines will contain “crash consistent” backups of the virtual machines, as well as the applications they contain. To ensure these applications are protected properly, it is recommended that the associated Backup Exec Database or Application Agents be used inside of the guest virtual machine to protect these applications in the standard fashion.

VMware Agent and the Deduplication Option

The Backup Exec Agent for VMware can be used in conjunction with the Deduplication Option to realize additional backup data storage savings. The technology used to deduplicate VMDK files has been significantly improved in Backup Exec 2010 R3.

When used together, VMDK copies gathered from VMware virtual machines by Backup Exec are broken into blocks of variable sizes. These blocks are fingerprinted and identified as either unique or non-unique. Unique blocks are stored and their fingerprints are added to the database while non-unique blocks are skipped. This method of deduplication is known as variable-length segmenting.

Backup Exec 2010 R3 now includes a VMware stream handler designed specifically for backups of VMware virtual machines. The new technology operates invisibly to Backup Exec, meaning no additional management or configuration adjustments are required on the part of the administrator. The VMware stream handler enables variable-length segmenting of VMDK files during deduplication calculations, rather than fixed-length segmenting used in previous versions of Backup Exec. This results in better storage savings across all VMware backups when using the Backup Exec Agent for VMware in conjunction with the Backup Exec Deduplication Option.

Using the Deduplication Option with the Backup Exec VMware Agent will result in significant storage savings in addition to the savings achieved by leveraging the block-level differential and incremental backup methods for VMware backups that are supported in Backup Exec 2010.

There are two deduplication methods that can be used when combining the Backup Exec 2010 Agent for VMware with the Deduplication Option: Server-side deduplication and client-side deduplication.

Server-side Deduplication

The server-side deduplication method uses a process where all backup data is transferred to the media server before deduplication calculations are made. Once backup data has arrived at the media server, blocks are fingerprinted and identified as unique or non-unique, and either kept or skipped respectively. This method of deduplication is optimal for environments where the protected ESX hosts and the Backup Exec media server are located in a SAN environment, allowing for high-speed data transfers.

Using server-side deduplication allows Backup Exec to leverage its integration with the vStorage API to capture efficient, off-host backups that alleviate a significant portion of backup I/O from the ESX host and transfer it to...
the media server, allowing the ESX host to dedicate the bulk of its computing resources to the production machines it is hosting, allowing them to run at optimal performance.

For these reasons, using server-side deduplication along with the VMware Agent is considered optimal for most environments.

**Client-side Deduplication**

The client-side deduplication method uses a process whereby deduplication “crunching”, meaning the identification of unique and non-unique blocks and the skipping of non-unique blocks, happens at the virtual machine level. The advantage of using this method is that only the unique blocks of data are transferred to the Backup Exec media server, greatly reducing the data traffic impact on the selected transport mode. This can be particularly desirable when the LAN is used as the transport mode to move data from the protected virtual machines to the Backup Exec media server.

It’s important to keep in mind that when using client-side deduplication, backups are captured and transported to the Backup Exec media server by locally installed Backup Exec agents and are not captured at the image or virtual machine level. The off-host method of protecting VMware virtual machines, which alleviates significant backup I/O burden from the ESX host, is not utilized. In essence, the virtual machines are protected in the same way as physical machines.

**Flexible Deduplication Choices**

Different deduplication methods can be mixed and matched to better service the configuration needs of Backup Exec customers.

Configurations are not restricted to a single deduplication method for a particular environment or even for a particular ESX server. Some virtual machines on a single ESX host can be configured to be backed up with client-side deduplication while the rest of the virtual machines use vStorage API backups and server-side deduplication. Some ESX hosts can be backed up with server-side deduplication while others use client-side deduplication, all managed by the same Backup Exec media server.
Backup Exec Management Plug-in for VMware

Overview

In early 2011, Symantec released the Backup Exec Management Plug-in for VMware. This management plug-in is offered at no charge and is available for download from the Backup Exec Technical Support web portal. The Backup Exec Management Plug-in for VMware allows administrators of virtual environments that are protected by Backup Exec and the VMware Agent to utilize the vSphere client application to do basic status monitoring tasks without having to visit the Backup Exec media server, such as the following:

- Monitor Backup Exec backup jobs that protect VMware virtual machines
- View the backup status of protected virtual machines
- View information regarding past backups as well as scheduled future backups

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

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

This new management plug-in requires Backup Exec 2010 (or later) and VMware vSphere 4.0 components (or later).
Login

Users of the Backup Exec Management Plug-in for VMware will be required to log into the associated Backup Exec 2010 media server. This can be done by specifying either the media server’s hostname or IP address. The credentials should represent a user that is a member of the Backup Exec Operators group.

Monitoring

In the plug-in display, the administrator is able to view all the Backup Exec backup jobs that protect virtual machines in the VMware environment. Because virtual machines can be a part of more than one backup job, some virtual machine names may be listed more than once.

The number of total virtual machines being protected by Backup Exec for the selected ESX host is also shown. This allows administrators to have a clearer view of the total number of virtual machines that are currently protected by Backup Exec.

It is possible for an administrator to exclude one or more virtual machines from particular backup jobs right from the plug-in interface. This will not exclude the virtual machine from all backups; only from the associated backup job. To exclude the virtual machine from additional backup jobs, this operation must be performed for each listed backup job for that particular virtual machine.

Additional views are also offered, such as a view that shows unprotected virtual machines or virtual machines that are protected by a different media server.
Performance Recommendations

SAN-based Backup Guidance

Configuring SAN-based backups with Backup Exec 2010 and the VMware Agent is relatively simple after following some basic guidelines:

- For performance reasons, it is recommended that only one Backup Exec media server be zoned to see a set of VMFS LUNs at one time.
- Zone the LUNs that contain the VMFS data store such that the Backup Exec 2010 media server can see and access them.
- On the Backup Exec 2010 media 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 LUN’s should appear in Windows Disk Administrator (on the Backup Exec media 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 ESX Server to the Backup Exec storage location (i.e. Tape or Disk). These components are:

- ESX server system resources: CPU (GHz)
- ESX system disk I/O capabilities (Gbps)
- Network type (Fiber Channel 1/2/4/8GB, iSCSI, 1/10GB Ethernet, etc)
- Backup Exec 2010 media server system resources

General 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 physical machine.
- Size the ESX server and Backup Exec 2010 CPU to support 10 MHz of CPU available per 1 MB/second of data throughput in and out of the ESX server.
- The internal bus of the Backup Proxy 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.

For more information, see Backup Exec Technote [http://seer.entsupport.symantec.com/docs/346047.htm](http://seer.entsupport.symantec.com/docs/346047.htm)

Recommended Number of Virtual Machines to Protect with a Single Media Server

There is no limit to the number of guest virtual machines that a single Backup Exec 2010 media server can protect. This is highly dependent on the number of guest virtual machines, the size of the VMDK files for each guest virtual machine, and the physical backup infrastructure.
Backup Job Recommendations

It is recommended that a seven-day rotation be used with Incremental and Differential backups, where a Full backup is run on the 7th day to avoid long Incremental/Differential backup chains.

Configuration Examples

Example 1: Backup Exec Protecting a Single VMware ESX Server

- A standalone ESX server is discovered by hostname or IP address
- The Backup Exec media server gathers virtual machine snapshot data through the vStorage API to perform off-host backups of VMware virtual machines

Example 2: Backup Exec Protecting Multiple ESX Servers Managed Through vCenter

- The ESX servers and guest virtual machines are discovered by Backup Exec using VMware Web Services method calls to the vCenter server
- The Backup Exec media server is either installed to the vCenter server, or Backup Exec is installed on a standalone server and the Backup Exec Agent for Windows Servers is installed to vCenter server
- The Backup Exec media server gathers virtual machine snapshots from datastores directly through vStorage API and performs off-host backups to a targeted storage device
Current Limitations

Virtual Machines Configured With RDM Physical Compatibility Mode Disks

The Backup Exec VMware Agent cannot protect RDM (Raw Device Mapping) Physical Compatibility Mode disks.

There are two types of RDM disks; virtual mode and physical compatibility mode. Physical compatibility mode (i.e. persistent-independent) bypasses the ESX storage infrastructure (VMFS file system) and cannot have a snapshot taken by vStorage APIs for Data Protection. Physical compatibility mode RDM disks in this configuration are skipped automatically during backup job processing and logged by Backup Exec as unprotected.

In order to protect virtual machines configured with physical compatibility mode RDM disks, Backup Exec Remote Agents can be installed in the guest virtual machines to back up their data using traditional backup methods.

Virtual Machines Configured With GPT Disks

The Backup Exec VMware Agent can be used to back up and recover virtual machines that are configured with GPT disks at the image level. This includes full, differential, and incremental backup methods. However, granular file/folder recovery and granular application recovery from virtual machines configured with GPT disks is not currently supported using the Backup Exec VMware Agent.

For configurations where a need exists to protect virtual machines configured with GPT disks and take advantage of granular recovery capabilities, install the Backup Exec Agent for Windows Servers to the virtual machine configured with GPT disks and protect it in the standard fashion.

Virtual Machines Configured With vSphere 4.0 Fault Tolerance
The Backup Exec 2010 VMware Agent cannot be used to protect vSphere 4.0 Fault Tolerant virtual machines.

Once a virtual machine has Fault Tolerance enabled, snapshots are no longer supported on that virtual machine. The Backup Exec 2010 Agent for VMware uses snap-based backups via the vStorage API 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 2010 VMware Agent 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 Servers to that virtual machine and protect it as you would a standalone physical machine.

**Virtual Machines Located On NFS Storage**

Due to limitations in the VMware vStorage API, Backup Exec 2010 VMware Agent is unable to determine used vs. unused blocks of VMDK files associated with virtual machines located on NFS storage. This results in backups of virtual machines on NFS storage captured by the Backup Exec Agent for VMware to be full backups, including both used and unused blocks of VMDK files.

A workaround is available for using the VMware Agent to capture GRT-enabled backups of Windows virtual machines located on NFS storage. The following registry key can be used to allow the Backup Exec Agent for VMware to bypass the VMware vStorage API when calculating used vs. unused blocks of a VMDK file, resulting in unused blocks in VMDK files being successfully ignored during backups:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Backup Exec For Windows\Backup Exec\Engine\VMware Agent\ NTFS Used Sector Tracking Preferred=1
```

Another workaround for protecting VMware virtual machines located on NFS storage is to install the Backup Exec Agent for Windows Servers to the virtual machines and protect them in the standard fashion.

**For More Information**

<table>
<thead>
<tr>
<th>Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.backupexec.com">www.backupexec.com</a></td>
<td>Backup Exec Website</td>
</tr>
<tr>
<td><a href="http://support.veritas.com/docs/304175">http://support.veritas.com/docs/304175</a></td>
<td>Backup Exec in Large Environments</td>
</tr>
<tr>
<td><a href="http://www.symantec.com/business/products/datasheets.jsp?pcid=2244&amp;pvid=57_1">www.symantec.com/business/products/datasheets.jsp?pcid=2244&amp;pvid=57_1</a></td>
<td>Backup Exec Datasheets &amp; Solution Briefs</td>
</tr>
<tr>
<td><a href="http://www.backupexec.com/compatibility">www.backupexec.com/compatibility</a></td>
<td>Compatibility Documents</td>
</tr>
<tr>
<td><a href="http://www.backupexec.com/configurator">www.backupexec.com/configurator</a></td>
<td>BE Product Configurator</td>
</tr>
<tr>
<td><a href="http://www.backupexec.com/skugenerator">www.backupexec.com/skugenerator</a></td>
<td>SKU Generator and BEST Tool</td>
</tr>
</tbody>
</table>