

Backup Exec™ 2014 Technical White Paper

Convert-to-Virtual (P2V) and Backup-to-Virtual (B2V) Conversions

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	4
Business Value	5
Underlying Principles	8
Virtual Conversion Features	11
Data Deduplication	18
Licensing	20
Notes and Best Practices	21
For More Information	22



Introduction

This white paper is intended to assist technical personnel as they design and implement the Convert-to-Virtual (P2V) and Backup-to-Virtual (B2V) features of Backup Exec™ 2014 and make related decisions. The business value of Backup Exec™ 2014's virtual conversion technology will also be considered in this white paper.

This white paper will explore the following topics related to the Convert-to-Virtual (P2V) and Backup-to-Virtual (B2V) technology found within Backup Exec™ 2014:

- Business Value
- Underlying Principles
- Virtual Conversion Features
- Data Deduplication
- Licensing
- Notes and Best Practices

Note: For step-by-step instructions for installing and managing Backup Exec™ 2014's virtual conversion features, please refer to the *Backup Exec™ 2014 Administrator's Guide* available here: [TECH205797](#).



Business Value

Modern Business is Driven by Servers

Modern businesses are based upon servers – powerful computing systems that host and manage business-critical applications and data. Servers are the lifeblood of business today, without which businesses could not function at a very basic level in our modern industry. Some examples of critical applications found on these servers are Microsoft Exchange, SQL, and Active Directory.

Because servers host business-critical applications and priceless customer and corporate data assets, managing and protecting servers is the primary concern of IT professionals across the globe.

Virtualization Technology

Over the last decade, one of the most disruptive and widely adopted IT technologies affecting modern businesses is virtualization. Virtualization breaks the legacy one-to-one relationship between server hardware and server operating systems, allowing businesses to save costs, consolidate resources, and enjoy a great deal of flexibility in how hardware and software assets are applied within an organization. Virtualization technology offers IT professionals new and unique tools to help solve the continuing problems of data protection and disaster recovery.

Virtualization technology offers benefits to organizations of all sizes. Although not all organizations plan to become fully virtualized, and although the virtualization use cases do vary somewhat from organization to organization, most have adopted, are adopting, or plan to adopt virtualization technology in one way or another.

Barriers to Adopting Virtualization

One of the primary problems businesses still struggle with is how to effectively adopt virtualization technology within their organization. Early adopters of virtualization realized that, as with any significant IT project, moving legacy physical servers to a virtualized platform is something that must be implemented in a manner that does not impact the organization's ability to continue with business as usual. A staged approach to adopting virtualization was quickly identified as a best practice.

However, although virtualization abstracts the operating system from the physical hardware layer of a server by inserting itself between the two, the virtualization layer is still seen as, and treated by, the operating system as hardware. Simply moving the operating environment from a physical server into a virtual machine using 'brute force' would simply result in an inoperable server, as the virtual hardware would not be recognized properly. The need for migration tools to help streamline this process of moving or converting physical servers into virtual machines was born.

Leveraging Virtualization Technology for Disaster Recovery

Many organizations realized that not all servers are good candidates for virtualization. High performance and high usage servers, such as mail servers, in some situations may still operate optimally on standalone hardware over the long term. Even in these situations however, virtualization technology still offers benefits, such as the ability to leverage virtual duplicates of physical servers as a way to quickly recover a server in the event of a disaster, allowing business operations to continue while the original server problem is repaired.

Convert-to-Virtual, Backup-to-Virtual, and Point-in-Time Conversions with Backup Exec 2014

Backup Exec™ 2014 continues to invest in virtualization technology. Features included in the Backup Exec™ 2014 product help administrators solve the problem of moving physical servers to a virtual environment and also give administrators unique tools for leveraging virtualization technology for disaster recovery. These features are the ability to perform automated conversions of physical servers to a virtual machine replica,



perform automated conversions of physical servers – using existing backup sets – to a virtual machine replica, and perform “ad hoc” or on-demand conversions of physical server backups to a virtual machine replica.

Virtual Conversion Features in Backup Exec 2014

Convert-to-virtual	✓
Backup-to-virtual	✓
Point-in-time (Ad Hoc) conversion	✓

Convert to Virtual (P2V)

The Backup Exec™ 2014 P2V feature allows administrators to configure backup definitions for physical servers that protect the server by both storing backup data to the Backup Exec server and creating a virtual machine replica of the server on an available VMware or Hyper-V host.

For backup definitions configured with a P2V task, the backup operation and the virtual machine replica operation occur in parallel.

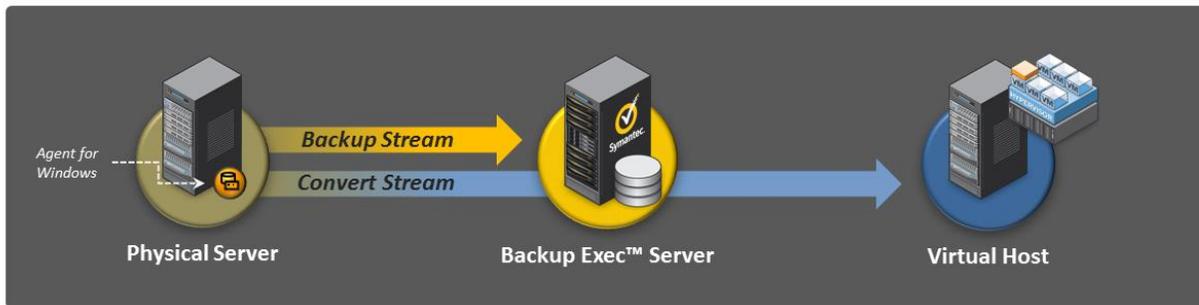


Figure 1: P2V Diagram

Backup to Virtual (B2V)

A Backup Exec™ 2014 backup definition configured with a B2V task is similar to a backup definition configured with a P2V task; however, B2V jobs run the backup and virtual machine replica operations serially, meaning the backup operation runs first, and the virtual replica portion runs immediately afterwards or on a different schedule.

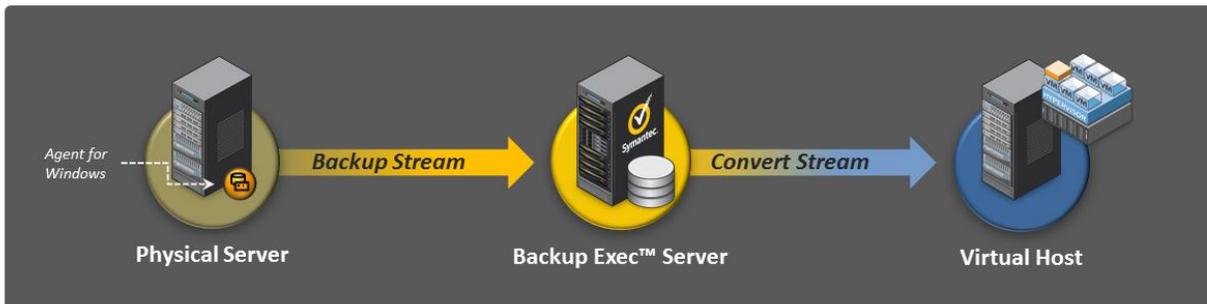


Figure 2: B2V Diagram

Point-in-Time Virtual Conversions

Another method of creating a virtual machine replica of physical servers using Backup Exec™ 2014 is the ad hoc or Point-in-Time method. This method is not scheduled, and is not directly associated with any particular



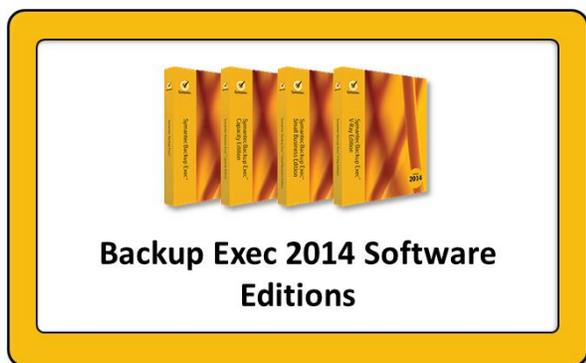
backup definition. It simply enables an administrator to create a virtual machine replica, on demand, of any physical machine that has been backed up to a Backup Exec server using an SDR-enabled backup.

The P2V, B2V, and Point-in-Time conversion features of Backup Exec™ 2014 can be used by administrators to move physical servers to a virtual environment permanently for migration purposes, or temporarily for testing or quick failover.

Symantec Backup Exec

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

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



Unified Virtual and Physical Protection in a Single Solution



Underlying Principles

Simplified Disaster Recovery (SDR)

The core technology that enables the Convert-to-Virtual (P2V) and Backup-to-Virtual (B2V) capabilities within Backup Exec™ 2014 is called Simplified Disaster Recovery (SDR). This technology ensures that key system-level elements of a server are captured and stored as part of a backup operation. When a P2V or B2V operation is performed, this system-level information is used to ensure the converted server is complete and will function properly as a virtual machine. Some of these critical system components include:

- System volume
- Boot volume
- Services volumes
- System state components

In Backup Exec™ 2014, the SDR feature is enabled by default for every new backup job that is created. It is represented within the Backup Exec™ 2014 user interface as a part of the backup selections screen through a ribbon titled “Simplified Disaster Recovery” as shown in the figure below:

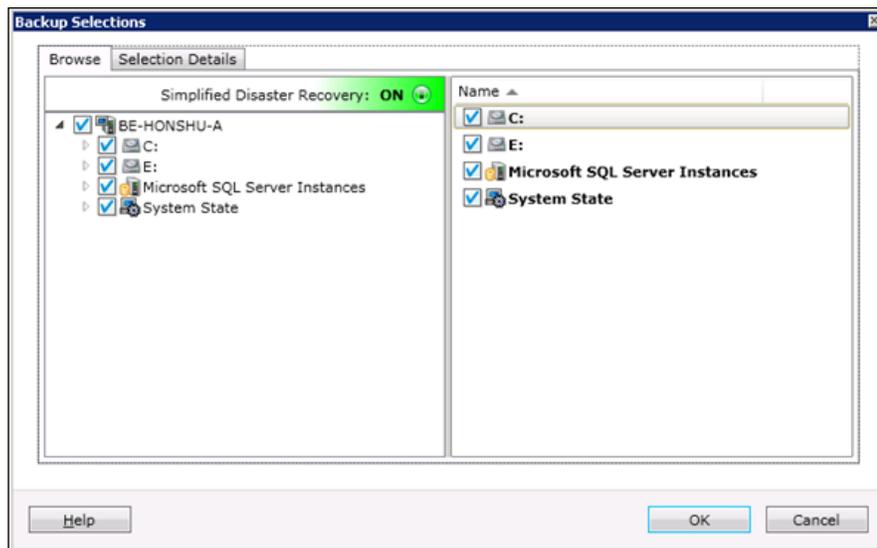


Figure 3: Simplified Disaster Recovery Ribbon

Administrators can disable SDR by unselecting elements of the server that are required to restore the server from a bare metal state, such as the “C:\” volume, certain sub-elements of the “C:\” volume, or “System State” elements.

In addition to enabling P2V and B2V operations, SDR enables other recovery features supported by Backup Exec™ 2014, such as the following:

Additional Recovery Features by Simplified Disaster Recovery	
Bare Metal Recovery	✓
Dissimilar Hardware Recovery	✓
Online Server Recovery	✓

This technical white paper will focus exclusively on the P2V and B2V features of Backup Exec™ 2014.



Whenever a backup job is modified such that the SDR feature is disabled, all corresponding recovery features that rely upon SDR are not available from those backups.

Recovery Features Enabled by Simplified Disaster Recovery	
Bare Metal Recovery	✓
Dissimilar Hardware Recovery	✓
Online Server Recovery	✓
Physical to Virtual Conversions (P2V)	✓
Backup to Virtual (B2V)	✓
Point in Time (Ad Hoc) Conversion	✓

Microsoft Volume Shadow Copy Service (VSS) Integration

In accordance with Microsoft best practices, the methods used by Backup Exec™ 2014 to capture SDR-enabled backups integrate with the Microsoft Volume Shadow Copy Service (VSS) to ensure that backups are both complete and consistent.

Complete Backups

Through integration with VSS, the backups captured by Backup Exec™ 2014 include all selected elements, even if they are components of the active operating system or are considered to be in an “open” state. This includes all selected operating system elements, such as the registry, and system state components.

Consistent Backups

This same integration also ensures that the backups captured are in a consistent state, and have been properly placed into a “quiet” mode at the time the snapshot is captured. This ensures that the operating system will boot and operate properly after a bare metal or dissimilar hardware restore operation.

DR File

Each backup set captured by a backup job that is enabled for SDR includes a disaster recovery or ‘DR’ file (file with the .DR extension). This file contains key metadata leveraged during bare metal and dissimilar hardware restore processes to recreate a physical server’s configuration from bare metal.

Applicable Backup Methods

Agent-based Backups of Physical Servers

The virtual conversion features of Backup Exec™ 2014 apply only to agent-based backups, meaning backups captured through the Agent for Windows installed to the protected server. This means that the virtual conversion capabilities of Backup Exec™ 2014 are generally limited to standalone physical servers with a local install of the Agent for Windows, and are backed up through the Agent for Windows using the agent-based backup approach.

Agent-based Backups of Physical Application Servers

Standalone physical application servers hosting applications such as Exchange, SQL, SharePoint, and Active Directory, and which are licensed for the Agent for Applications and Databases, also use agent-based backups captured through a local installation of the Agent for Windows. As a result, these standalone physical application servers can also be protected with Simplified Disaster Recovery backups and converted to virtual



using convert-to-virtual, backup-to-virtual, and point-in-time conversion methods. No additional Agent for Windows license or Agent for Windows backups are required to enable this functionality.

Virtual Machine Backups

In most cases, VMware and Hyper-V virtual machines – even if they contain a local installation of the Agent for Windows – are not backed up through an agent-based process. In VMware and Hyper-V environments, it is optimal to protect virtual machines through host-based snapshot methods using the Agent for VMware and Hyper-V, rather than through a locally installed Agent for Windows. Host-based snapshot backups do not utilize SDR technology and as such the features enabled by SDR, such as P2V and B2V, are not available.

The Backup Exec™ 2014 Agent for VMware and Hyper-V offers the following recovery features for VMware and Hyper-V virtual machines:

Virtual Machine Recovery Features of the Agent for VMware and Hyper-V	
Full Virtual Machine Recovery	✓
Application Recovery	✓
Granular Application Recovery (requires Agent for Applications and Databases)	✓
Granular File and Folder Recovery (requires Agent for Applications and Databases)	✓
Redirected Recovery	✓

Note: For further details on the backup and recovery features available for VMware and Hyper-V virtual machines using the Agent for VMware and Hyper-V, please refer to the *Backup Exec™ 2014 Administrator's Guide* available here: [DOC5211](#).



Virtual Conversion Features

Overview

The virtual conversion features of Backup Exec™ 2014 are built from agent-based backups, generated by a locally installed Backup Exec Agent for Windows inside of a standalone physical server, and are transmitted to a Backup Exec server that is available on the network.

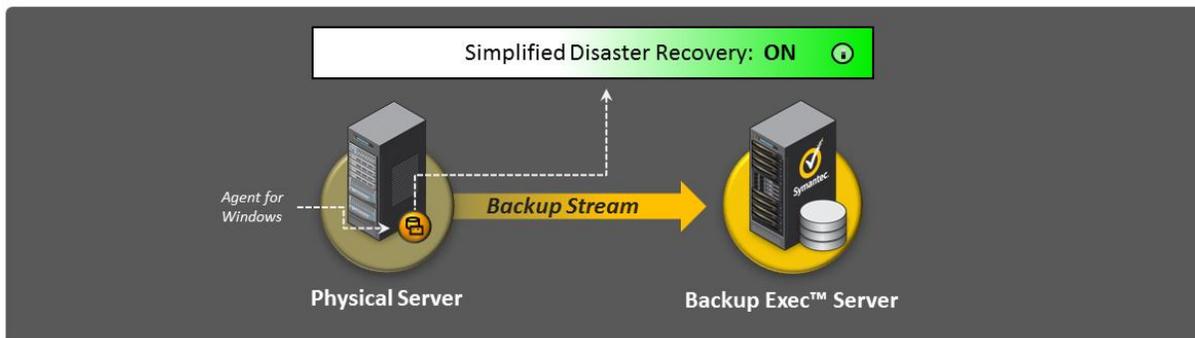


Figure 4: Agent-based Backup Enabled for Simplified Disaster Recovery

These agent-based backups must be SDR-enabled in order for virtual conversion features to be supported. By default, Backup Exec™ 2014 backups of standalone physical servers are enabled for SDR, which can be confirmed by the presence of the green “Simplified Disaster Recovery” ribbon in the backup selection portion of the user interface.

Backup Exec™ 2014 offers three options for converting agent-based backups of standalone physical servers to a virtual machine replica. These options are:

Virtual Conversion Features in Backup Exec 2014	
Convert-to-virtual (P2V)	✓
Backup-to-virtual (B2V)	✓
Point-in-time (Ad Hoc) conversion	✓

Each of these conversion methods, along with their differences and core use cases, is described in greater detail below.

Convert to Virtual (P2V)

Selecting a P2V Operation

An administrator can select a P2V operation from the list of pre-defined definition types within the Backup Exec™ 2014 user interface.

Parallel Data Streams

When Backup Exec™ 2014 is used to perform a P2V task against a standalone physical system, the Agent for Windows that is installed on the standalone physical system transmits two data streams in parallel. The first is a backup stream that is sent to a Backup Exec server on the network and is stored to a disk storage device managed by that Backup Exec server. The other is a conversion stream to an ESX or Hyper-V server on the network.

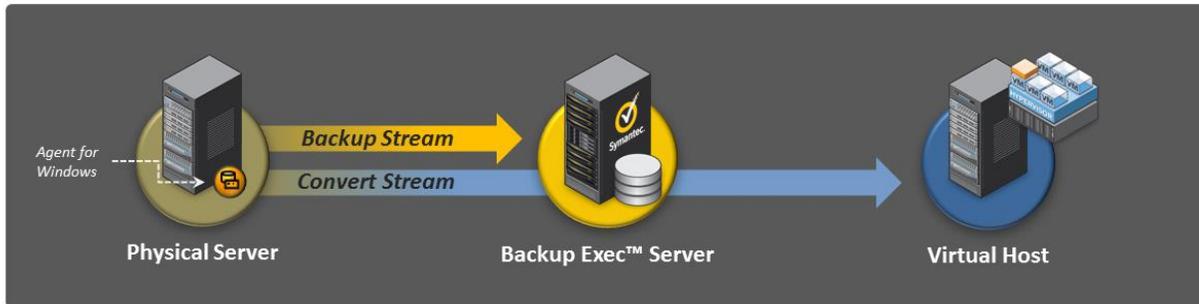


Figure 5: P2V Diagram

Because these data streams are transmitted in parallel, a P2V task can only be defined alongside a backup task in a Backup Exec backup definition, and cannot be standalone. As such, when defining a P2V task a schedule is not created; the P2V task uses – and runs in parallel with – the backup schedule.

Disk Storage Device Required

The backup stream must target a disk storage device managed by the Backup Exec server. Both disk storage devices as well as deduplication disk storage devices are supported. Standard backup options for the backup task, such as backup type, schedule, encryption settings, etc, are supported.

Performance Factors

Because the backup and P2V streams run in parallel in a backup definition configured with a P2V stage, performance will generally match that of the slowest of the two data streams. For example, if the backup stream is capable of running at 10,000 MB/minute, but the P2V stream is only capable of running at 2000 MB/minute, the entire parallel process will run at 2000 MB/minute.

Backup Stream is Primary Task

Backup Exec considers the backup stream to be the primary task in backup definitions that are configured with a P2V stage. This means the following:

- If the P2V stream fails, the backup stream will continue if possible
- If the backup stage fails, the entire job will fail, including the P2V stage

VMware Virtualization Environment Options

The administrator must specify a VMware vSphere host that will receive the virtual machine replica created by the P2V task. In addition, the administrator must provide authentication credentials in order to successfully connect to the target host.

The administrator must also specify a storage location for the virtual machine replica, including the target data center, datastore or cluster, host or cluster, virtual machine folder, and resource pool.



Virtualization environment options

ESX / vCenter server name: vt-vc01

Logon account: System Logon Account

Data center: TEST-DC

Datastore or Datastore cluster: SCLR7_HROAX4-5_VTEAM_VTESXCLS1TB-2

Host or cluster: vt-esx01.hro.rnd.veritas.com

Virtual machine folder: P2VTest

Resource pool: Resources

Figure 6: VMware Virtualization Environment Options

VMware Virtual Machine Options – Server Configuration

The administrator is also able to configure virtual memory and virtual CPU settings for the virtual machine replica depending upon the available VMware host resources.

Virtual machine options

Virtual machine name: VM-SYMANTEC-7C2981

Overwrite the virtual machine if it already exists

Full path of VMware Tools ISO image: \\lk-build-2.hro.rnd.veritas.com\G:\DriversIso\Vmware\windows.iso

Server configuration

System configuration	Source physical machine	Destination virtual machine
Physical RAM (MB)	2047	2047
CPU Count	4	4

Figure 7: VMware Virtual Machine Options – Server Configuration

VMware Virtual Machine Options – Disk Configuration

Finally, the administrator can configure the disk configuration for the virtual machine replica. This includes the ability to specify whether the virtual disk files will be provisioned as thick or thin.

Virtual machine options

Virtual machine name: VM-SYMANTEC-7C2981

Overwrite the virtual machine if it already exists

Full path of VMware Tools ISO image: \\lk-build-2.hro.rnd.veritas.com\G:\DriversIso\Vmware\windows.iso

Server configuration

Name	Disk type	Disk size	Disk controller	Virtual disk name	Path of virtual disk
Disk 0 (Boot, System)	Thin	233 GB	IDE (0:0)	VM-SYMANTEC-7C2981	[SCLR7_HROAX4-5_VTEAM_... - Available MB: 1086207(<da
Disk 1	Thin	466 GB	IDE (0:1)	VM-SYMANTEC-7C2981_1	[SCLR7_HROAX4-5_VTEAM_... - Available MB: 1086207(<da

Figure 8: VMware Virtual Machine Options – Disk Configuration



Conversion options for Microsoft Hyper-V environments are similar to the options available for VMware vSphere environments, with a few differences. The Microsoft Hyper-V virtual machine options are shown below:

Hyper-V Virtualization Environment Options

The administrator must specify a Hyper-V host that will receive the virtual machine replica created by the P2V task, along with a destination path to which the virtual machine files will be physically stored. In addition, the administrator must provide authentication credentials in order to successfully connect to the target host.

Figure 9: Hyper-V Virtualization Environment Options

Hyper-V Virtual Machine Options – Server Configuration

The administrator is also able to configure virtual memory and virtual CPU settings for the virtual machine replica depending upon the available Hyper-V host resources.

System configuration	Source physical machine	Destination virtual machine
Physical RAM (MB)	2047	2047
CPU Count	4	4

Figure 10: Hyper-V Virtual Machine Options – Server Configuration

Hyper-V Virtual Machine Options – Disk Configuration

Finally, the administrator can configure the disk configuration for the virtual machine replica. This includes the ability to specify whether the virtual disk files will be provisioned as fixed or dynamically expanding.

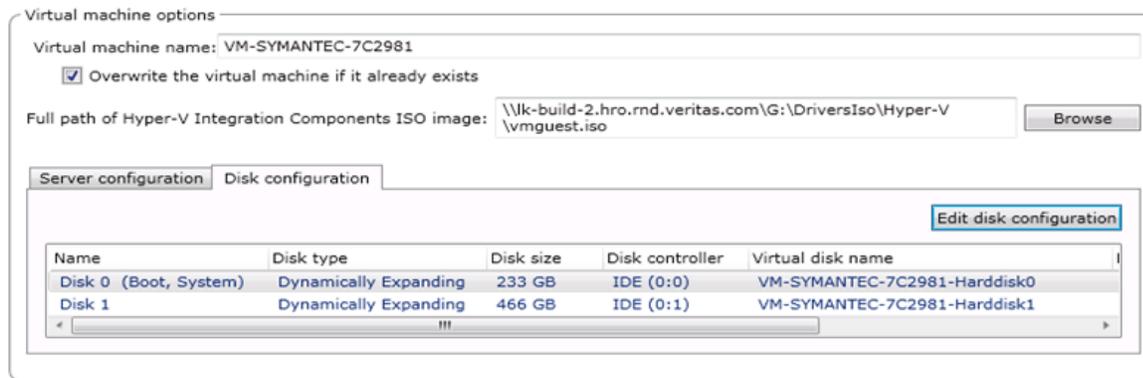


Figure 11: Hyper-V Virtual Machine Options – Disk Configuration

Backup to Virtual (B2V)

Selecting a B2V Operation

An administrator can select a B2V operation from the list of pre-defined definition types within the Backup Exec™ 2014 user interface.

Serial Data Streams

For Backup Exec™ 2014 backup definitions that are configured with a B2V stage, the backup stream and B2V stream are processed serially, or one after the other. This means that B2V tasks do not necessarily have to occur immediately after backup tasks. They can be scheduled to run on a different schedule, or to run immediately after a full backup task in a backup definition.

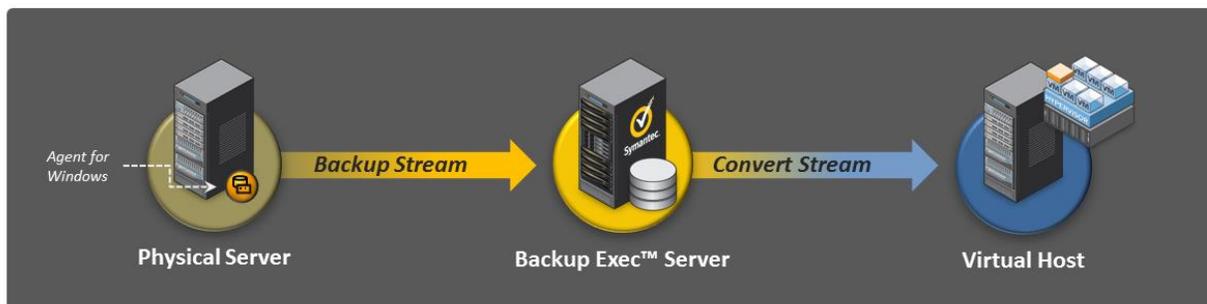


Figure 12: B2V Diagram

When multiple backup stages are a part of a backup definition, the B2V task can be linked to any of the backups or to always source the most recent backup.

Disk Storage Device Required

The backup task to which a B2V task is linked must target a disk device managed by the Backup Exec server. Both disk storage devices and deduplication disk storage devices are supported. Standard backup options for the backup task, such as backup type, schedule, encryption settings, etc, are supported.

Virtualization Environment Options

For B2V tasks, both VMware vSphere and Microsoft Hyper-V virtualization environment options, such as specifying a virtual host and managing virtual machine settings, are the same as for convert-to-virtual tasks.

Performance Factors



Because the B2V task runs independently of standard backup tasks, there is no performance link between the two operation types. With hardware being equal, a B2V operation should result in performance similar to a standard backup operation.

Point-in-Time Conversions

Backup Exec™ 2014 also supports ad hoc, or Point-in-Time, virtual conversions. As with other conversion types, point-in-time conversions can target VMware vSphere or Microsoft Hyper-V virtual servers. Point-in-Time conversions are always “run now” events, and as such have no scheduling mechanism.

Because Point-in-Time conversions are not scheduled, they are not defined as part of a backup definition. Point-in-Time conversions are executed as “one off” virtual conversions.

General Notes for P2V and B2V Conversions

Supported Virtual Servers

The conversion stream must target a VMware vSphere or Microsoft Hyper-V virtual server that is available on the network. This includes support for Windows 2012 Hyper-V servers and VMware vSphere 5.5 hosts.

It's important to note that the conversion stream results in a full virtual machine replica on the target virtual server, and not just a virtual disk file.

When conversion streams target a Windows 2012 Hyper-V server, the resulting virtual machines will use .VHDX virtual disk files instead of .VHD virtual disk files.

Note: For the latest information on supported operating system platforms and virtual platforms, please refer to the Backup Exec compatibility lists available here: [TECH175581](#).

Access to Associated Virtual Tools ISO Image Required

Virtual conversion tasks require access to an ISO image of the associated virtual tools component for the target virtual server. For example, if the conversion operation is targeting a Hyper-V host, a path to a Hyper-V Integration Services ISO image is required. If the conversion operation is targeting a VMware host, a path to a VMware Tools ISO image is required. The path to the appropriate ISO image is entered in the ‘Virtual Machine Options’ section of the virtual conversion task.

One Virtual Conversion Task Type per Backup definition

Backup Exec™ 2014 supports only one virtual conversion task type per backup definition. This means that at a maximum, a backup definition can be configured with one P2V task and one B2V task. Point-in-Time conversions are standalone and are not associated with any particular backup definition.

One Virtual Machine Replica Maintained per Conversion Task

Backup Exec™ 2014 supports only one virtual machine replica per conversion task. This applies to both P2V and B2V tasks. Virtual machine replicas created from Point-in-Time conversions are standalone and not associated with any particular backup definition.

In order to automatically maintain more than one virtual machine replica for a protected physical server, one or more *additional* backup definitions, each containing an SDR-enabled backup and a virtual conversion task, must be configured for the protected physical server.

“Overwrite the Virtual Machine If It Already Exists” Option



If the option to “Overwrite the virtual machine if it already exists” is *not* selected, subsequent runs of the virtual conversion task in the backup definition will fail if the virtual machine already exists. Please note that this only affects the virtual conversion task, and does not affect backup tasks in the same backup definition.

The option to “Overwrite the virtual machine if it already exists” is selected by default.

Virtual Hardware Considerations

During a conversion operation, a form of dissimilar hardware restore is used to inject virtual device drivers into the virtual machine’s virtual disk file to ensure that the resulting virtual machine boots and operates normally. This virtual driver insertion process is fully automated and requires no user intervention or administration.

The administrator is required to enter the path to the appropriate virtual tools ISO image in the “Virtual Machine Options” section of the virtual conversion task.



Data Deduplication

Integrated Data Deduplication

Backup Exec™ 2014 includes integrated, block-level deduplication technology that dramatically reduces backup storage requirements. This includes advanced stream handler technologies for VMware and Hyper-V virtual disks, which greatly increase the storage optimization benefits of deduplication for VMware and Hyper-V backups. The stream handler for the latest Hyper-V virtual disk format (VHDX) is a new feature in Backup Exec™ 2014.

Data Deduplication Overview

As backup data is captured from protected servers and stored to the deduplication disk storage device on a Backup Exec server, the data is scanned to determine which blocks are unique and need to be stored and which blocks are non-unique and can be skipped. Only unique data blocks are stored to disk, while non-unique blocks are skipped. Unique and non-unique blocks are identified through a process known as fingerprinting.

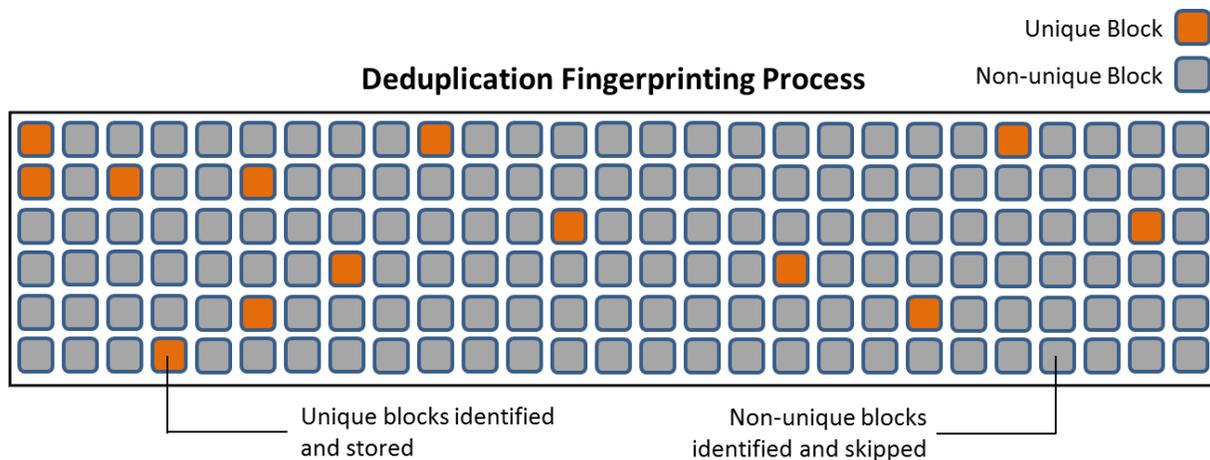


Figure 13: Data Deduplication Fingerprinting Process Diagram

The calculation of data block fingerprints can occur at the client level, the server level, or at the appliance level. Which calculation method is most efficient for a given backup operation depends on the backup environment topology, whether the client is physical or virtual, and other factors. Client-level, server-level, and appliance-level deduplication methods can be mixed and matched according to the needs of an administrator.

Data Deduplication and Virtual Conversions

The data deduplication features of Backup Exec™ 2014 apply to all backup data stored to the Backup Exec deduplication disk storage device. If a backup definition stores backup data to the deduplication disk storage device, it is deduplicated, and benefits from the storage optimization benefits of data deduplication technology.

Backup Stream Deduplicated, Convert Stream Not Deduplicated

Backup Exec™ 2014 backup definitions that include P2V or B2V tasks generate two data streams. One data stream is sent to the Backup Exec server as backup data, and the other is sent to a virtual host as a virtual machine replica. The backup data stream will fully benefit from deduplication technology if it is targeted to the Backup Exec deduplication disk storage device. The virtual machine replica stream that is transmitted to a VMware or Hyper-V host as part of a P2V or B2V task is not stored to the Backup Exec deduplication disk



storage device, and does not receive any storage optimization benefit from Backup Exec's deduplication technology.

Client-side Deduplication and P2V Tasks

As explained previously, backup definitions that are configured with a P2V task generate two data streams. One data stream is sent to the Backup Exec server as backup data, and the other is sent to a virtual host as a virtual machine replica. When the same backup definition is enabled for client-side deduplication, the backup stream consists only of the unique data blocks present since the last backup operation. However, the conversion stream is still a full conversion. Because both streams originate from the protected server, performance will only be as fast as the full conversion stream being sent to the virtual host in the form of a full virtual machine replica.



Licensing

Virtual Conversion Features Included

The P2V, B2V, and Point-in-Time conversion capabilities of Backup Exec™ 2014 are included in the core product and are not purchased or licensed separately. Any individual server that is licensed for protection by a Backup Exec server, such as a server that is licensed for the Agent for Windows or the Agent for Applications and Databases, is eligible for virtual conversion tasks.



Notes and Best Practices

Basic Disks Only

In Backup Exec™ 2014, virtual conversion tasks are supported only for physical servers configured with basic disks. Dynamic disk configurations are not supported for virtual conversion tasks.

File System Support

In Backup Exec™ 2014, virtual conversion tasks are supported only for physical servers configured with NTFS or FAT32 volumes. Other file system types, such as Linux file systems, are not supported for virtual conversion tasks.

System Support

In Backup Exec™ 2014, virtual conversion tasks are not supported for GPT volumes. Only MBR volumes are supported.

Clusters

In Backup Exec™ 2014, virtual conversion tasks are not supported for physical servers configured in a cluster configuration.



For More Information

Link	Description
http://www.symantec.com/connect/blogs/new-backup-exec-partner-toolkit-v10	Backup Exec Partner Toolkit
www.symantec.com/business/backup-exec-for-windows-servers	BE Family Landing Page
www.symantec.com/business/products/whitepapers.jsp?pcid=pcat_business_cont&pvid=57_1	BE White Papers
www.symantec.com/business/products/datasheets.jsp?pcid=2244&pvid=57_1	BE Datasheets, Feature Briefs
TECH205797	BE Compatibility Docs
www.backupexec.com/configurator	BE Product Configurator
www.backupexec.com/skugenerator	BE SKU Generator and BEST Tool



About Symantec

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

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

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

Symantec helps organizations secure and manage their information-driven world with [data backup and recovery software](#).

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