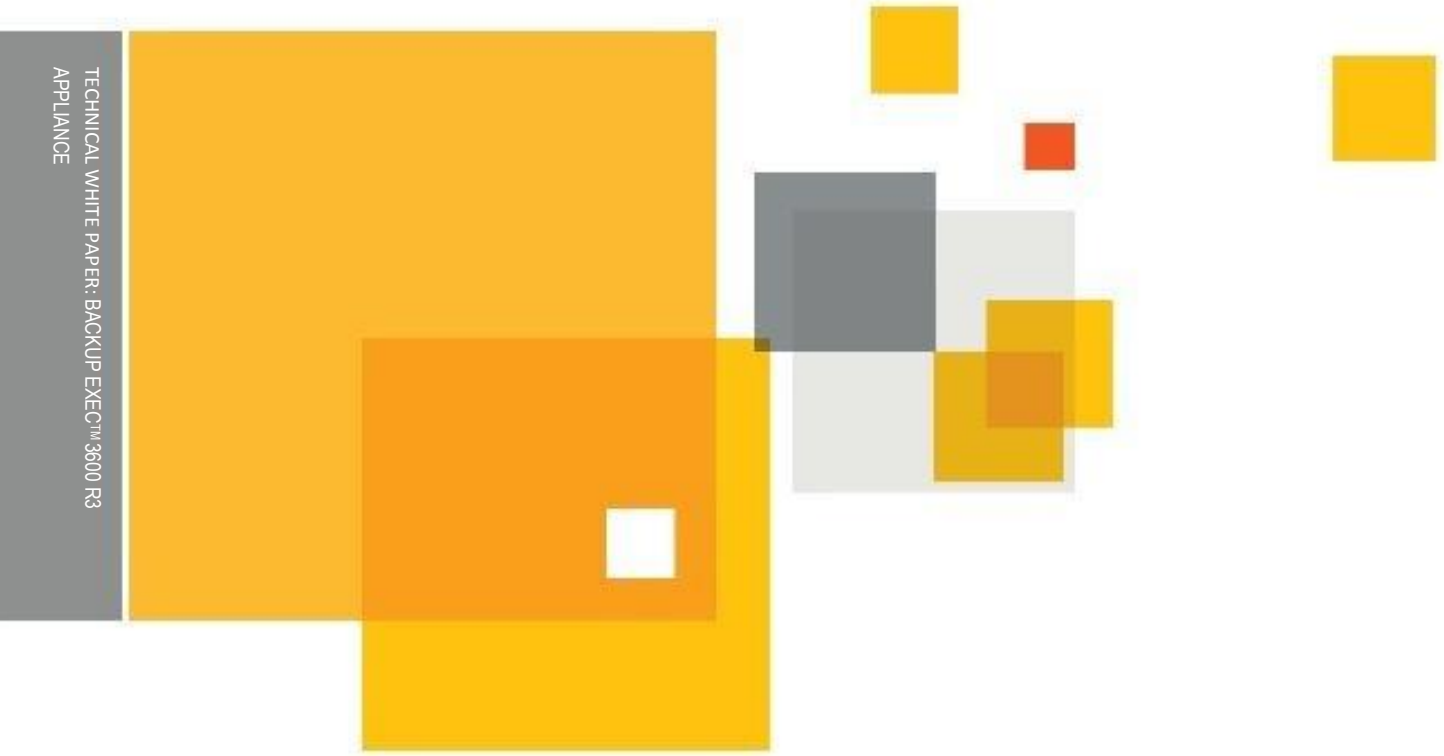

Backup Exec™ 2014 Technical White Paper

Backup Exec™ 3600 R3 Appliance

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 10
VMware Integration 14
Hyper-V Integration 17
Virtual Conversion Features 19
Built-in Data Deduplication 21
Recovery Capabilities 24
Monitoring and Management 29
Example Appliance Scenarios 32
Hardware Configuration 35
Licensing Overview 38
Notes and Considerations 39
For More Information 42

Introduction

This technical white paper is intended to assist partners and customers as they implement data protection solutions based on the Backup Exec™ 3600 Appliance. This brief will explore the following topics as they relate to the Backup Exec™ 3600 Appliance product:

- Business Value
- Underlying Principles
- VMware Integration
- Hyper-V Integration
- Virtual Conversion Features
- Built-in Data Deduplication
- Recovery Capabilities
- Monitoring and Management
- Example Appliance Scenarios
- Hardware Configuration
- Licensing Overview
- Notes and Considerations

Note: For step-by-step instructions for installing and managing the Backup Exec™ 3600 Appliance, refer to the *Backup Exec™ 3600 Administrator's Guide* available here: DOC4613.

Business Value

In today's complex world of information technology and data protection, there are many challenges and considerations associated with building, implementing, and supporting a backup solution. These challenges often lead to delayed projects, overspent budgets, and sometimes even failure. For these and many other factors, organizations are seeking a simple appliance-based solution to reduce complexity, cost, and associated risks.

Complexity of a Traditional Backup Solution

Building a traditional backup solution involves the acquisition and assembly of multiple component parts, such as a server, an operating system, storage devices and media, backup software, and of course multiple warranty and maintenance contracts. As a result, the traditional backup solution can include a very high level of complexity.

For some environments, it is also necessary to define and manage a backup strategy for remote offices, which can be further complicated if technical personnel are not available at remote offices to manage backup processes. In addition, as IT environments continue to adopt virtualization, yet another layer of complexity is the need to implement a backup solution that matches the needs of both physical and virtualized server resources.

Cost of a Traditional Backup Solution

In addition to the challenges and complexity, there are significant costs and time investments associated with creating a traditional backup solution. These include the following:

- Backup software costs
- Backup software agent and option costs
- Backup server and storage hardware costs
- Hardware and software installation and configuration costs
- Costs associated with managing removable media at remote offices

In some environments, costs are unnecessarily compounded if separate backup solutions are implemented for physical and virtual resources.

In addition to these visible costs, there are hidden costs along the way. As such, the combined monetary and time cost of implementing a traditional backup solution can be significant.

Risks of a Traditional Backup Solution

Finally, there's the additional problem of risk that comes from constructing a backup solution comprised of software and hardware components from different vendors. These risks include:

- **Hardware and Software Component Compatibility**

  Solutions built using different hardware and software components from different vendors may or may not work together properly.

- **Backup Performance**

  Presuming the different components of the backup solution function together, performance may not be optimal. In order to achieve acceptable performance, it may be necessary to troubleshoot, reconfigure, or even replace one or more components of the backup solution.

- **Technical Support Time to Resolution**

  When dealing with a backup solution comprised of hardware and software components from different vendors, troubleshooting and resolving problems can prove difficult. Different vendors will point fingers at each other while the issue is investigated, costing the customer time and money.

The Backup Exec™ 3600 Appliance

The Backup Exec™ 3600 Appliance mitigates the problems of complexity, cost, and risk associated with traditional backup solutions by delivering a combined hardware and software solution in a single package.

SIMPLE: One vendor for hardware, software, licensing and support

COST EFFECTIVE: Unlimited use of included Backup Exec™ agents and options

LOW RISK: All-in-one solution with reliable compatibility and performance

Figure 1: Symantec Backup Exec™ 3600 Appliance Advantages

Complete Virtual and Physical Protection in a Single Solution

The Backup Exec™ 3600 Appliance delivers complete data and application protection for both virtual and physical server resources, including optimized support for the latest VMware and Hyper-V platforms. For VMware environments, the Backup Exec™ 3600 Appliance includes deep integration with the VMware vStorage API, ensuring VMware virtual machines are protected using the latest technology available.

Figure 2: Complete Physical and Virtual Protection

Using the Backup Exec™ 3600 Appliance, customers and partners can protect both physical and virtual server resources in their environment and avoid the unnecessary costs and headaches associated with implementing and managing separate backup solutions for each.

Designed for Virtual Environments

Partners and customers who want to protect their VMware or Hyper-V virtual environments understand the frustration and time involved with legacy backup technologies that are not designed specifically for protecting virtual environments. Legacy solutions such as these include several limitations, such as:

- Impacting virtual environment performance when processing backups inside virtual machines
- Requiring the shutdown of guest virtual machines in order to protect them completely
- Requiring separate backups for virtualized applications, such as Microsoft SQL, Active Directory, SharePoint, and Exchange
- Requiring the manual configuration of backup agents and policies for new virtual machines
- Requiring slow file-by-file backups that capture redundant data in each guest virtual machine over and over
- Requiring long restores of an entire guest virtual machine in order to recover a single file

The Backup Exec™ 3600 Appliance includes features and technologies specifically designed for modern virtualized environments, including the VMware vSphere platform and the Microsoft Hyper-V platform. These technologies enable the Backup Exec™ 3600 Appliance to offer features such as the following:

Virtual Protection Features	
Direct backups of virtual environments (no proxy server)	✓
Image-level backups of virtual machines while they remain online	✓
Differential and incremental backup support (change block tracking)	✓
Block Optimization	✓
VSS integration, ensuring application consistency	✓
Automatic discovery and protection of new virtual machines	✓
Optimized data deduplication of VMDK and VHD/X files	✓

Virtual Recovery Features	
Full virtual machine recovery	✓
VMDK and VHD/X file recovery	✓
Application recovery	✓
Granular application recovery	✓
Granular file and folder recovery	✓
Redirected recovery	✓

The Backup Exec™ 3600 Appliance is ready, right out of the box, to properly and completely protect both VMware vSphere and Microsoft Hyper-V virtual infrastructures.

Figure 3: Direct Backup of Virtual Resources

The Backup Exec™ 3600 Appliance represents an effective, easy-to-buy, and easy-to-use data and application protection solution for small and medium-sized customers who are partially or fully virtualized.

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 Principles

General

The Backup Exec™ 3600 R3 Appliance is a 1U server system that arrives from the factory with Backup Exec™ 2014 software pre-installed. The Backup Exec™ 3600 Appliance is designed to be a complete data and application backup solution for small and medium-sized environments, and includes the ability to directly protect both physical and virtual servers without the need for a proxy server.

The Backup Exec™ 3600 Appliance has been rigorously and thoroughly tested by Symantec to ensure optimal compatibility and performance.

Included Software

Backup Exec™ 2014

The Backup Exec™ software included on the Backup Exec™ 3600 R3 Appliance is based upon Backup Exec™ 2014. Both the core Backup Exec™ software, as well as the agent software required to protect physical servers, are included in the Backup Exec™ 3600 Appliance.

Windows Storage Server 2008 R2

The operating system included on the Backup Exec™ 3600 Appliance is Windows Storage Server 2008 R2. The Windows Storage Server 2008 R2 operating system ensures optimal security and stability in production environments.

Update Enabled

Both primary software components of the Backup Exec™ 3600 Appliance, Backup Exec™ 2014 and Windows Storage Server 2008 R2, are update-enabled. Critical patches and hot fixes are automatically downoaded, and the administrator controls the schedule by which they are installed. This self-update capability ensures that the appliance remains secure and functional in an ever-evolving security environment.

Physical Server Backup Methods

For physical servers protected by the Backup Exec™ 3600 Appliance, backup data is always captured through a local agent on the physical server called the Agent for Windows (for Windows servers), the Agent for Linux (for Linux servers), or the Agent for Mac (for Macintosh servers). Communication with the Backup Exec™ 3600 Appliance occurs over the LAN infrastructure, enabling physical client servers to receive backup job instructions and to transmit backup data to the Backup Exec™ 3600 Appliance for storage.

The agent component that is deployed to physical server resources also enables direct recovery of file or application objects back to the original resource from which they were captured.

Virtual Machine Backup Methods

For virtual infrastructures, such as VMware vSphere environments or Microsoft Hyper-V environments, partners and customers have the option to protect virtual machines using either of the following two methods:

- **Image-level Backups**

  The Backup Exec™ 3600 Appliance interacts with the vitual host to capture image-level backups of the protected virtual machines. In most cases, image-level backups are optimal when protecting virtual environments.

- **Agent-based Backups**

  The Backup Exec™ 3600 Appliance protects virtual machines in the same manner that it protects physical servers, through a remote software agent installed to the virtual machine.

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

Note: Although the Backup Exec™ 3600 Appliance fully supports image-based backups of VMware vSphere and Microsoft Hyper-V virtual machines, additional functionality can be enabled by also installing the appropriate Backup Exec™ agent to each virtual machine that is being protected by the Backup Exec™ 3600 Appliance. This agent works hand-in-hand with the image-level backup operation to enable advanced features, such as the following:

- Automatic discovery of applications inside of a virtual machine
- Granular recovery of application objects for Exchange, SQL, SharePoint, and Active Directory
- Direct recovery of granular file-level elements back to the virtual machines from which they were generated

Hyper-V Backups

When protecting virtual machines on a Hyper-V host using the Agent for VMware and Hyper-V, the Backup Exec™ Agent for Windows is installed to the Hyper-V host. This agent is used to transmit image-level backup data of virtual machines over the LAN to the Backup Exec™ 3600 Appliance for storage.

When protecting virtual machines on a Hyper-V host without using the Agent for VMware and Hyper-V, the agent-based backup method is used. When using agent-based backups, the appropriate Backup Exec™ agent captures and transmits backup data to the Backup Exec™ 3600 Appliance.

VMware Backups

When protecting virtual machines on a VMware ESX/i host using the Agent for VMware and Hyper-V, image-level backups are captured via integration with the VMware vStorage API. No Backup Exec™ agent is installed to the ESX/i host server itself.

When protecting virtual machines on a VMware ESX/i host without using the Agent for VMware and Hyper-V, the agent-based backup method is used. When using agent-based backups, the appropriate Backup Exec™ agent captures and transmits backup data to the Backup Exec™ 3600 Appliance.

Communication Security

Physical Server Communication Security

The communication path between Backup Exec™ Agents and the Backup Exec™ 3600 Appliance is encrypted using TSL/SSL encryption technology, and requires a trust relationship between the Backup Exec™ Agents and the Backup Exec™ 3600 Appliance.

Hyper-V Virtual Machine Communication Security

For Hyper-V environments, the Agent for Windows is installed to each Hyper-V host. The communication path between the Agent for Windows on the Hyper-V host and the Backup Exec™ 3600 Appliance is encrypted using TSL/SSL encryption technology, and requires a trust relationship between the agent and the Backup Exec™ 3600 Appliance.

VMware Virtual Machine Communication Security

For VMware environments, backups are captured usng integration with the VMware vStorage API. No Backup Exec™ Agent is installed to the VMware ESX/i host itself. To ensure security in these configurations, it is

recommended that SSL be enabled on the ESX/i host to ensure communication traffic between the ESX/i host and the Backup Exec™ 3600 Appliance remains secure.

Communication Security and Other Virtual Platforms

For virtual infrastructures based on platforms other than VMware and Hyper-V, virtual machines are protected using agent-based backups, and requires an agent to be installed locally to each virtual machine. In essence, virtual machines on platforms other than VMware and Hyper-V are protected as if they were standalone physical servers.

The communication path between the Backup Exec™ Agents and the Backup Exec™ 3600 Appliance is encrypted using TSL/SSL encryption technology, and requires a trust relationship between the agent and the Backup Exec™ 3600 Appliance.

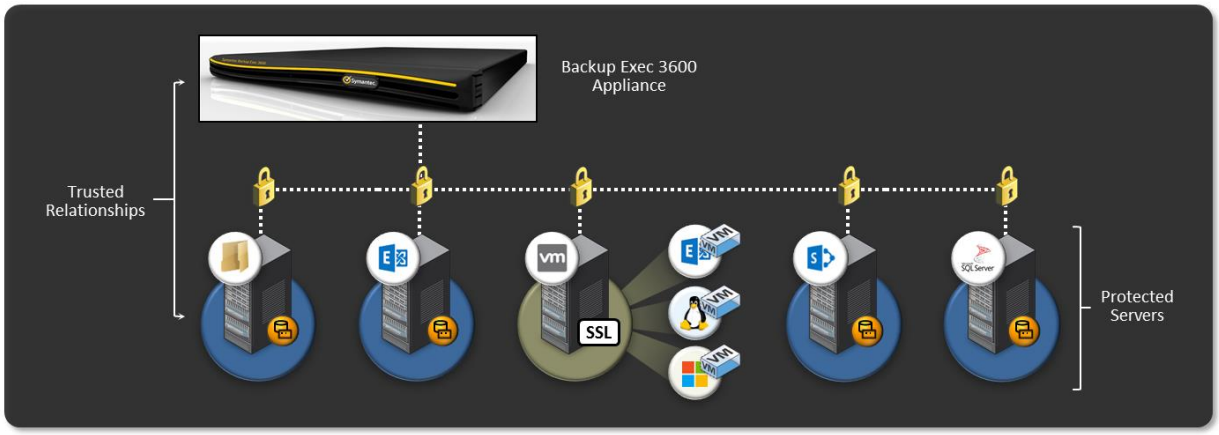

Figure 4: Communication Security Diagram

Secondary Copies of Backup Data

The primary storage device of the Backup Exec™ 3600 Appliance is the 5.5 TB disk array within the appliance itself. The disk array within the appliance has a capacity of 5.5 TB. Because the disk array within the Backup Exec™ 3600 Appliance is enabled for data deduplication, the 5.5 TB capacity of the disk array will protect a much larger amount of front-end data.

In addition, secondary storage devices and locations can be leveraged for storing secondary copies of backup data for additional layers of protection and disaster recovery, or for primary backup storage. Example devices and locations supported by the Backup Exec™ 3600 Appliance include the following:

Backup Exec™ 3600 Appliance Supported Secondary Storage Devices	
Locally Attached Disk Devices (USB)	✓
Locally Attached Tape Drives and Libraries (SAS)	✓
Remote Backup Exec™ Servers or 3600 Appliances	✓
Remote Network Storage Devices (NAS)	✓
Riverbed Whitewater Appliance (CIFS target) with Amazon S3	✓

Note: For additional details on secondary storage devices supported by the Backup Exec™ 3600 Appliance, please refer to the compatibility lists for the Backup Exec™ 3600 Appliance available here: TECH205797.

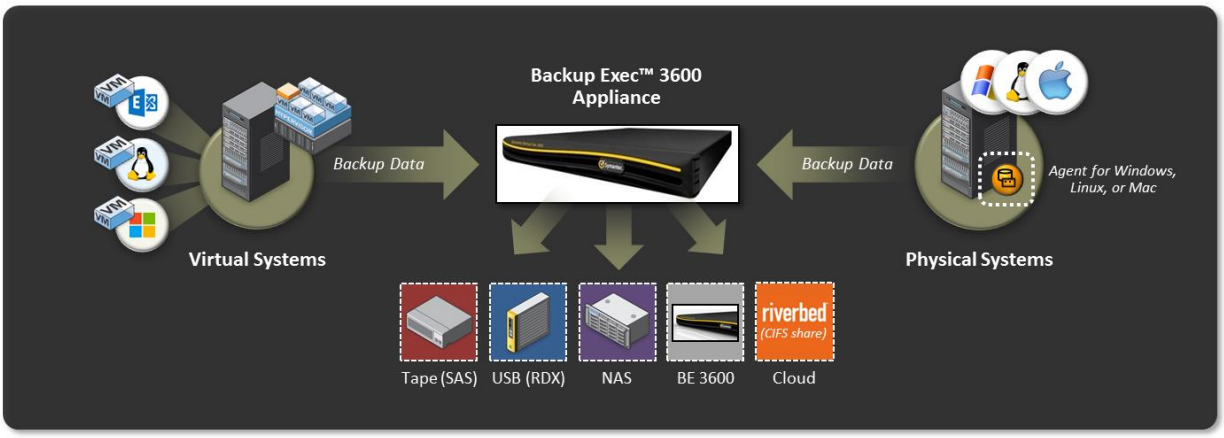

Figure 5: Backup Exec™ 3600 Appliance Secondary Storage Devices

By offering flexible and state-of-the-art protection for both physical and virtual infrastructures, as well as providing a high level of data security with flexible choices for backup data storage, the Backup Exec™ 3600 Appliance is well-suited to meet the data and application protection requirements of almost any small and medium-sized IT environment.

VMware Integration

The Backup Exec™ 3600 Appliance includes technology specifically designed and optimized for VMware environments. This optimization allows the Backup Exec™ 3600 Appliance to properly protect VMware virtual machine resources through integration with the VMware platform and the vStorage set of APIs.

Backup Technology Optimized for VMware

Integration with the vSphere platform through the vStorage API enables the Backup Exec™ 3600 Appliance to support the following features:

VMware Protection Features	
Direct backups of virtual environments (no proxy server)	✓
Image-level backups of virtual machines while they remain online	✓
Differential and incremental backup support (change block tracking)	✓
Block Optimization	✓
VSS integration, ensuring application consistency	✓
Automatic discovery and protection of new virtual machines	✓
Optimized data deduplication of VMDK files	✓

VMware Recovery Features	
Full virtual machine recovery	✓
VMDK file recovery	✓
Application recovery	✓
Granular application recovery	✓
Granular file and folder recovery	✓
Redirected recovery	✓

Best-practices for Application Protection

The Backup Exec™ 3600 Appliance includes features to ensure that applications such as Exchange, SQL, SharePoint, and Active Directory are properly protected according to Microsoft best practice recommendations. These features include the following:

- Enhanced VSS integration ensures applications are protected according to Microsoft best practices.
- Consistent application protection through the placement of applications into a consistent or 'backup ready' state before backup.
- Log truncation of key applications ensures proper application maintenance and the prevention of storage saturation by ever-growing transaction logs.

Administrators using the Backup Exec™ 3600 Appliance to protect virtualized, VSS-aware application servers can be confident that these applications are being protected properly and will recover successfully in the event of a disaster.

Non-VSS Compliant Virtual Machines and Applications

Some platforms and applications that are not VSS-compliant cannot be properly protected using VSS methods. If these virtual machines are protected using the Agent for VMware and Hyper-V capabilities of the Backup

Exec™ 3600 Appliance, they will be momentarily placed in a suspended or offline state while the virtual machine snapshot is captured.

When non-VSS-compliant virtual machines are momentarily placed in a suspended or offline state to capture backups, they are not placed in a consistent or "backup ready" state, nor are application logs truncated. Rather, they are protected in a "crash consistent" manner. While most recovery operations from crash-consistent backups are successful, Symantec does not recommend this approach.

Administrators using the Backup Exec™ 3600 Appliance and the Agent for VMware and Hyper-V to protect VMware environments that include one or more virtual machines that are not VSS-compliant should consider using the standard Backup Exec™ Agent for Windows or Agent for Linux to protect these virtual machines. Using the Backup Exec™ Agent for Windows or the Agent for Linux to protect non-VSS-compliant virtual machines helps ensure the virtual machines themselves, as well as the applications they contain, are backed up properly.

VMware Storage Distributed Resource Scheduling

The Backup Exec™ 3600 Appliance and the Agent for VMware and Hyper-V support several new features offered in the latest release of the VMware vSphere platform, vSphere 5.0. This includes support for virtual machines using hardware version 8 as well as support for the new Storage Distributed Resource Scheduling (SDRS) feature.

The SDRS capabilities of vSphere 5.0 allow virtual administrators to simplify management of datastores through the introduction of datastore clusters, also referred to as 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 operation. This feature works hand in hand with other VMware technologies, such as vMotion.

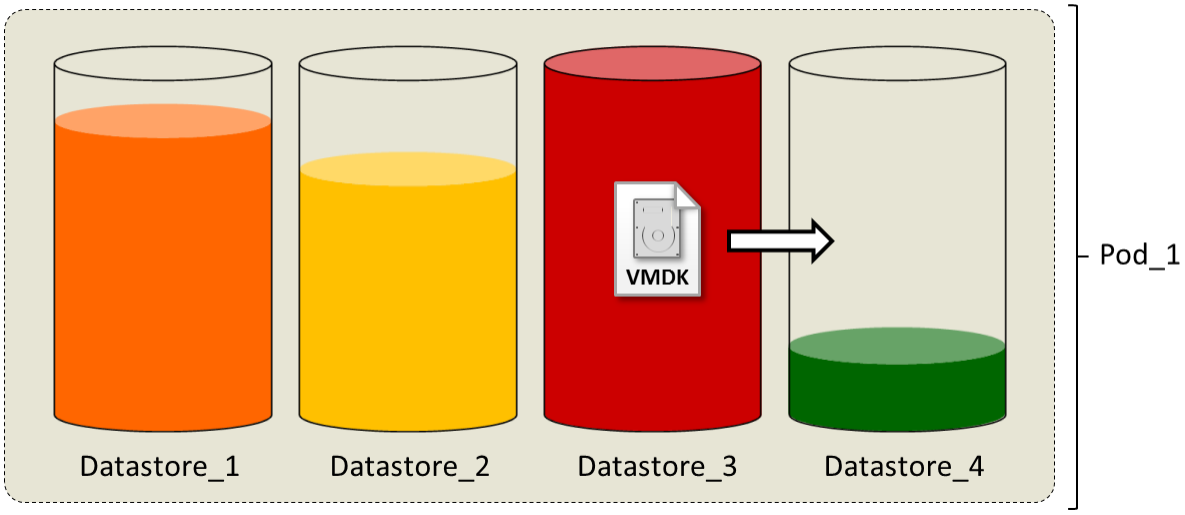

Figure 6: VMware Storage Distributed Resource Scheduling Diagram

The Backup Exec™ 3600 Appliance and the Agent for VMware and Hyper-V fully support virtual machines that are located within a datastore cluster and that are enabled for SDRS.

If a virtual machine is actively involved in a backup or recovery operation controlled by the Backup Exec™ 3600 Appliance at the time an SDRS event occurs, the Backup Exec™ 3600 Appliance places a temporary lock on the virtual machine. This action delays the SDRS event until after the backup or recovery operation has completed and the associated virtual machine snapshot has been removed. Once the operation is complete, the virtual

machine is unlocked and the SDRS event proceeds normally. The Backup Exec™ 3600 Appliance does not remove SDRS attributes from a virtual machine during backup or restore operations.

In addition, new restore features have been added allowing administrators to restore virtual machines to the cluster level or to specific datastores within a cluster.

Hyper-V Integration

The Backup Exec™ 3600 Appliance includes technology specifically designed and optimized for Hyper-V environments. This optimization allows the Backup Exec™ 3600 Appliance to properly protect Hyper-V resources through integration with the Microsoft Hyper-V platform and VSS.

Backup Technology Optimized for Hyper-V

Integration with the Microsoft Hyper-V platform enables the Backup Exec™ 3600 Appliance to support the following features:

Hyper-V Protection Features	
Direct backups of virtual environments (no proxy server)	✓
Image-level backups of virtual machines while they remain online	✓
Differential and incremental backup support (change block tracking)	✓
Block Optimization	✓
VSS integration, ensuring application consistency	✓
Automatic discovery and protection of new virtual machines	✓
Optimized data deduplication of VHD/X files	✓

Hyper-V Recovery Features	
Full virtual machine recovery	✓
VHD/X file recovery	✓
Application recovery	✓
Granular application recovery	✓
Granular file and folder recovery	✓
Redirected recovery	✓

Best Practices for Application Protection

The Hyper-V protection capabilities of the Backup Exec™ 3600 Appliance provide best practice protection for application servers such as Exchange, SQL, SharePoint, and Active Directory that have been virtualized on the Hyper-V platform. This includes the following:

- Online backups of guest virtual machines that host Microsoft applications, such as Exchange and Active Directory, which utilize the Microsoft VSS framework; virtual machines are not taken offline during this process, and normal operations continue.
- Backup processes leverage VSS to capture a consistent snapshot of the virtual machine and any VSS-aware applications that it is hosting.
- Automatic truncation of transaction logs for Exchange and Active Directory.

Note: In order for online backups of guest virtual machines to be possible, Hyper-V Integration Services must be installed to guest virtual machines.

Non-VSS Compliant Virtual Machines and Applications

Some platforms and applications that are not VSS-compliant cannot be properly protected using VSS methods. If these virtual machines are protected using the Agent for VMware and Hyper-V capabilities of the Backup Exec™ 3600 Appliance, they will be momentarily placed in a suspended or offline state while the virtual machine snapshot is captured.

When non-VSS-compliant virtual machines are taken offline in order to capture backups, they are not placed in a consistent or "backup ready" state, nor are application logs truncated. Rather, they are protected in a "crash consistent" manner.

Administrators using the Backup Exec™ 3600 Appliance to protect Hyper-V environments with the Agent for VMware and Hyper-V that include one or more virtual machines that are not VSS-compliant should consider using the standard Backup Exec™ Agent for Windows or Agent for Linux to protect these virtual machines. Using the Backup Exec™ Agent for Windows or the Agent for Linux to protect non-VSS-compliant virtual machines helps ensure the virtual machines themselves, as well as the applications they contain, are backed up properly.

Cluster Shared Volumes

Microsoft introduced a new technology for their Windows 2008 Server platforms called Cluster Shared Volumes. A Cluster Shared Volume is an NTFS volume that can be accessed by all the nodes in a cluster at the same time. This new clustering technology from Microsoft allows virtual machines to migrate or fail over to other nodes in the cluster independently, without affecting other virtual machines that are stored on the same LUN.

The Backup Exec™ 3600 Appliance and the Agent for VMware and Hyper-V support the protection of Cluster Shared Volume nodes, as well as highly available virtual machines in a Cluster Shared Volume configuration. The Backup Exec™ 3600 Appliance and the Agent for VMware and Hyper-V fully support the Live Migration of virtual machines between Hyper-V hosts.

Virtual Conversion Features

The Backup Exec™ 3600 Appliance includes capabilities that allow administrators to create virtual replicas of protected physical servers.

Simplified Disaster Recovery

The core technology that enables the new virtual conversion features within the Backup Exec™ 3600 Appliance is called Simplified Disaster Recovery, or SDR. This technology ensures that key system-level elements of a server are captured and stored as part of a backup operation. When a virtual conversion operation is performed, this system-level information is used to ensure the converted server is complete and will function properly as a virtual machine.

In the Backup Exec™ 3600 Appliance, the SDR feature is enabled by default for every new backup policy that is created. When backups are enabled for SDR, virtual conversion features become available for the associated server, such as the following:

Virtual Conversion Features Enabled by Simplified Disaster Recovery	
Physical to Virtual	✓
Backup to Virtual	✓
Point in Time (Ad Hoc)	✓

Note: For additional details on platforms that are supported for Simplified Didaster Recovery protection, please refer to the *Software Compatibility List (SCL)* for the Backup Exec™ 3600 Appliance available here: TECH205797.

Physical to Virtual Conversions

When the Backup Exec™ 3600 Appliance is used to perform a physical-to-virtual conversion task against a physical client server, the Backup Exec™ Agent for Windows that is installed to the physicel client server transmits two data streams in parallel. The first data stream is a backup stream that is sent to the Backup Exec™ 3600 Appliance. The other is a conversion stream that is sent to the targeted ESX or Hyper-V host on the network.

Because these data streams are transmitted in parallel, a physical-to-virtual conversion task can only be defined alongside a backup task in a Backup Exec™ 3600 Appliance protection policy, and cannot be standalone. As such, when defining a physical-to-virtual conversion task a separate schedule is not created; the physical-to-virtual conversion task uses, and runs in parallel with, the full backup schedule.

Backup to Virtual

For Backup Exec™ 3600 Appliance protection policies configured with a Backup to Virtual stage, the Backup Exec™ Agent for Windows that is installed on the standalone physical system transmits the backup stream and virtual converstion streams serially, or separately. Backup-to-virtual tasks do not run in parallel to backup tasks, and backup-to-virtual 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 protection policy. When multiple full backup stages are a part of a protection policy, the backup-to-virtual task can be linked to any of the full backups or to always source the most recent full backup.

Point-in-time Conversions

The Backup Exec™ 3600 Appliance 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 protection policy; they are executed as “one off” virtual conversions and can source any full, SDR-enabled backup set on the BE 3600 Appliance storage array.

Note: For more information about the virtual conversion capabilities found in the Backup Exec™ 3600 Appliance, please refer to additional white paper documents available on these topics and the *Backup Exec™ 3600 Administrator’s Guide* available here: DOC4613.

Built-in Data Deduplication

The Backup Exec™ 3600 Appliance includes data deduplication technology that greatly increases its backup data storage efficiency.

Data Deduplication Technology

As backup data is captured from protected physical and virtual resources and stored to the disk array in the Backup Exec™ 3600 Appliance, the data is scanned to determine what 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. Unique and non-unique blocks are identified through a process known as fingerprinting.

The calculation of data block fingerprints, through which unique and non-unique blocks are identified, can occur at the client level, or at the Backup Exec™ 3600 Appliance itself. When fingerprint calculations are performed by the Backup Exec™ 3600 Appliance itself, it is referred to as server or server-level deduplication. Which deduplication 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 and server deduplication methods can be mixed and matched according to the needs of an administrator. For example, an administrator could decide to have all VMware backups leverage server deduplication, and have all physical client backups leverage client deduplication.

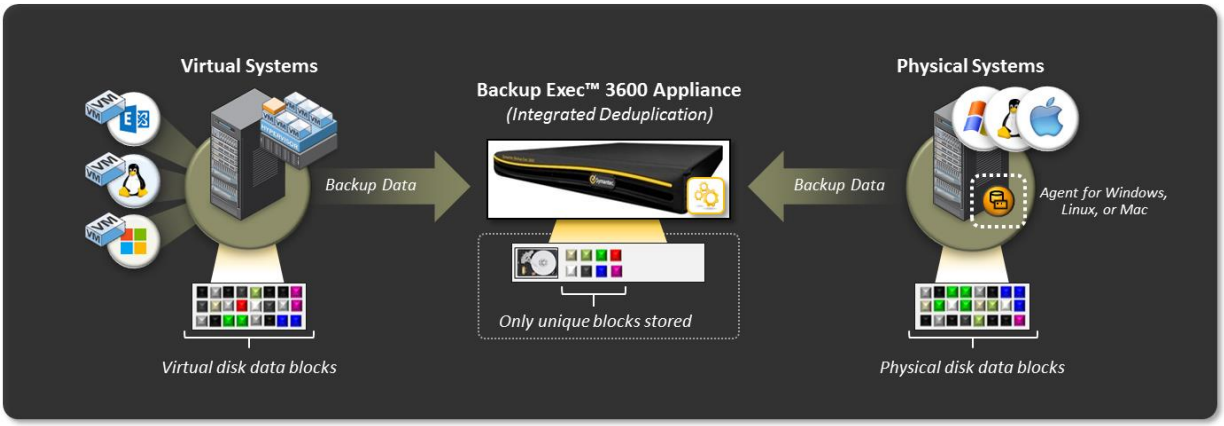

Figure 7: Backup Exec™ 3600 Appliance Data Deduplication

This powerful data deduplication technology is built into the Backup Exec™ 3600 Appliance and does not require any additional purchase.

Deduplication calculations are made against all backup streams that are sent to the Backup Exec™ 3600 Appliance and stored in the deduplication storage folder, whether they are generated from physical resources, virtual resources, or both.

Optimized Data Deduplication for Virtual Backups

The data deduplication technology within the Backup Exec™ 3600 Appliance includes specific optimizations for backups of virtual machines. This includes backups of VMware virtual machines as well as Hyper-V virtual machines.

Intelligent Deduplication of Virtual Disk Files

Virtual disk files are the core data components of a virtual machine. VMware virtual disks are VMDK files, and Hyper-V virtual disks are VHD or VHDX files. The virtual disk file is analogous to the hard drive or hard drive

array found in physical server systems. Although virtual disk files represent data stored in a proprietary format (VMDK format for VMware and VHD or VHDX format for Hyper-V), the Backup Exec™ 3600 Appliance includes intelligence that allows it to understand and interpret file structures within VMware and Hyper-V virtual disk files and efficiently deduplicate them. This is made possible through components known as stream handlers. Stream handlers operate invisibly to the backup process and require no additional configuration or management on the part of the administrator.

Stream Handler Technology

As deduplication-enabled backups of VMware or Hyper-V virtual machines are processed by the Backup Exec™ 3600 Appliance, variable-length segmenting is used. This is made possible by the virtual disk stream handlers that are included in the Backup Exec™ 3600 Appliance. As a result of this technology, data changes within a virtual disk file that occur over time result in fewer unique blocks being identified during the deduplication fingerprinting process. This results in greater storage efficiency.

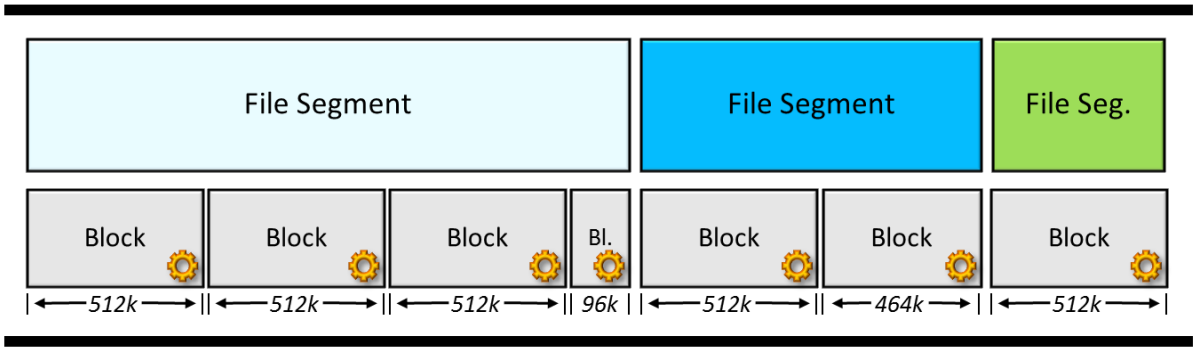

Figure 8: Virtual Disk Stream Handler Technology

This advanced deduplication technology is particularly effective when multiple virtual machines are protected by a Backup Exec™ 3600 Appliance.

The virtual disk stream handlers described above are built into the Backup Exec™ 3600 Appliance and operate invisibly without requiring any additional knowledge or administration. When deduplication is enabled, the stream handler technology that increases the effectiveness of deduplication for VMware and Hyper-V backups is always active.

Backup Exec™ Partner Toolkit

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

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

Business Value

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

- **Performance Analyzer** - The Performance Analyzer Tool will assess the readiness of one or more server systems to act as a Backup Exec™ server. Each server's hardware and software configuration is analyzed for performance inhibitors, including any disk and tape backup devices attached to that server.
- **Deduplication Assessment Tool** - The Deduplication Assessment Tool will directly demonstrate the value of Backup Exec's deduplication technology to partners and end users by scanning one or more servers in an environment and offering deduplication ratio and backup storage savings estimates.
- **Front-end Capacity Analyzer** - The Front-end Capacity Analysis Tool will easily and quickly identify the amount of front-end data in an environment and greatly streamlines the process of selling the Backup Exec™ Capacity Edition, which is licensed against the amount of front-end data in an environment.

Ease of Use

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

Platform and Application Support

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

Recovery Capabilities

The Backup Exec™ 3600 Appliance supports a wide range of recovery options for both physical and virtual machine backups. Each of these recovery options is possible from a single-pass backup operation; no additional or separate backup operation is required to achieve additional levels of restore granularity.

Virtual Server Recovery Options

The Backup Exec™ 3600 Appliance supports a full range of powerful recovery options for protected VMware and Hyper-V virtual machines. These include:

Virtual Recovery Features (VMware and Hyper-V)	
Full virtual machine recovery	✓
VMDK and VHD/X file recovery	✓
Application recovery	✓
Granular application recovery	✓
Granular file and folder recovery	✓
Redirected recovery	✓

The Backup Exec™ 3600 Appliance represents the latest in backup technology with features and capabilities integrated with, and designed specifically for, VMware and Hyper-V virtual environments.

Full Virtual Machine Recovery

When protecting VMware or Hyper-V virtual machines using the Backup Exec™ 3600 Appliance, full virtual machine recovery is supported. Virtual machines can be recovered back to their original virtual host, or redirected to an alternate virtual host. Additional features are also included, such as the option to automatically power off the target virtual machine that is being restored, and the option to automatically power on the restored virtual machine once the recovery process is complete.

Full virtual machine recovery includes all files associated with the virtual machine. This includes the core virtual disk file (VMDK or VHD), as well as other files that make up the virtual machine on disk.

VMDK and VHD/X File Recovery

The Backup Exec™ 3600 Appliance also allows administrators to easily recover individual file elements of a virtual machine, such as individual virtual disk files. Virtual disk files can be recovered as flat files, restored to an existing virtual machine on the original virtual host, or redirected to an alternate location or virtual host.

Application Recovery

For VMware and Hyper-V virtual machines hosting Exchange, SQL, SharePoint, and Active Directory, full recovery at the application level is also supported by the Backup Exec™ 3600 Appliance. This allows administrators to recover a full application instance if a full virtual machine recovery is not necessary or desired.

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

To enable application-level recovery, the Backup Exec™ Agent for Windows must be installed to the guest virtual machine before backup. The Agent for Applications and Databases, which enables advanced support for Exchange, SQL, SharePoint, Active Directory, and other applications, is included with the Backup Exec™ 3600 Appliance.

Granular Application Recovery

One of the key software capabilities of the Backup Exec™ 3600 Appliance is the Agent for VMware and Hyper-V. The Agent for VMware and Hyper-V, when combined with the Agent for Applications and Databases, enables administrators to recover granular application objects from single-pass backups of VMware and Hyper-V guest virtual machines. Both the Agent for VMware and Hyper-V and the Agent for Applications and Databases are included with the Backup Exec™ 3600 Appliance. Granular application objects that can be recovered include Exchange mailboxes, emails, attachments, and calendar items, Active Directory objects such as user and computer objects, SharePoint documents and other objects, and SQL databases.

A separate database-level or object-level backup is not required to enable granular application recovery for virtual machine backups.

Note: To enable granular application recovery, the Backup Exec™ Agent for Windows must be installed to the guest virtual machine before backup.

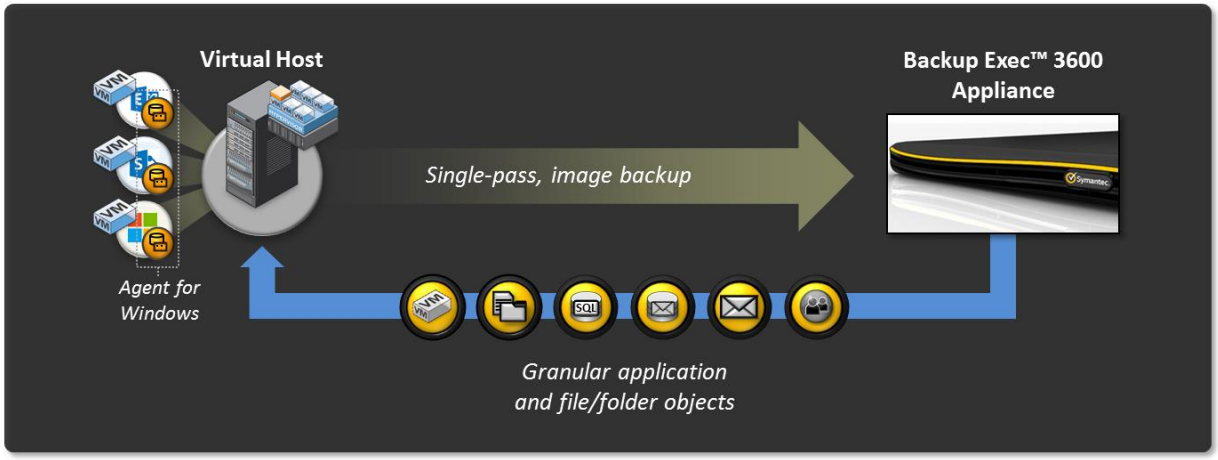

Figure 9: Granular Recovery of Virtualized Applications

Granular File and Folder Recovery

Granular file and folder recovery is possible from single-pass, image-level backups of VMware and Hyper-V guest virtual machines. It is not necessary to have the Backup Exec™ Agent for Windows installed to the guest virtual machine for granular file and folder recovery to be possible. However, having the Backup Exec™ Agent for Windows installed to the guest virtual machine is required to recover files and folders *directly back* to the source virtual machine.

Optionally, files and folders can be recovered to an alternate location and moved back to the original guest virtual machine using other methods.

Redirected Recovery

Data from VMware and Hyper-V virtual machines or virtual disk files can be restored to their original locations or to alternate virtual hosts. Granular recovery operations of Windows virtual machines can also be redirected to a different virtual machine than where the data was backed up, if the Agent for Windows is present on the destination virtual machine.

Note: For additional details on recovery options for VMware and Hyper-V environments, or for step-by-step instructions for performing a recovery, please consult the *Backup Exec™ 3600 Administrator's Guide* available here: DOC4613.

Physical Server Disaster Recovery Options

The Backup Exec™ 3600 Appliance supports advanced disaster recovery capabilities for the physical servers it is being used to protect. This includes the following:

Physical Server Disaster Recovery Options	
Bare Metal Recovery*	✓
Dissimilar Hardware Recovery*	✓

*Windows servers only.

Note: For additional details on supported platforms for bare metal and dissimilar recovery operations, please consult the Backup Exec™ compatibility lists available here: TECH205797.

Simplified Disaster Recovery technology enables the Backup Exec™ 3600 Appliance to provide advanced bare metal and dissimilar hardware recovery for the physical servers that it protects.

Simplified Disaster Recovery

Simplified Disaster Recovery (SDR) technology ensures that key system-level elements of a server are captured and stored as part of a backup operation. For environments protected by the Backup Exec™ 3600 Appliance, the SDR feature is enabled by default for every new physical server backup policy that is created.

Simplified Disaster Recovery Disk

The Backup Exec™ 3600 Appliance's recovery disk is the tool used by administrators to perform bare metal and dissimilar hardware recovery operations of physical servers being protected by the Backup Exec™ 3600 Appliance. The recovery disk is based on the powerful Microsoft WinPE operating system, and includes a robust driver database leveraged for both runtime tasks and dissimilar hardware recovery operations.

Creating a Simplified Disaster Recovery Disk for Appliance Environments

It is important to create a Simplified Disaster Recovery Disk for environments protected by the Backup Exec™ 3600 Appliance. When creating a Simplified Disaster Recovery Disk, necessary Microsoft components for creating the recovery disk are downloaded. In addition, this process includes the ability to add additional drivers to the recovery disk ensuring that all key hardware components in the environment are supported.

Note: Procedures for creating a Simplified Disaster Recovery Disk can be found in the *Backup Exec™ 3600 Administrator's Guide*, available here: DOC4613.

Recovery Disk Language Support

The Simplified Disaster Recovery Disk supports all languages supported by the Backup Exec™ 3600 Appliance. During the recovery disk boot process, a language selection screen is displayed from which the administrator can select a language version to use:

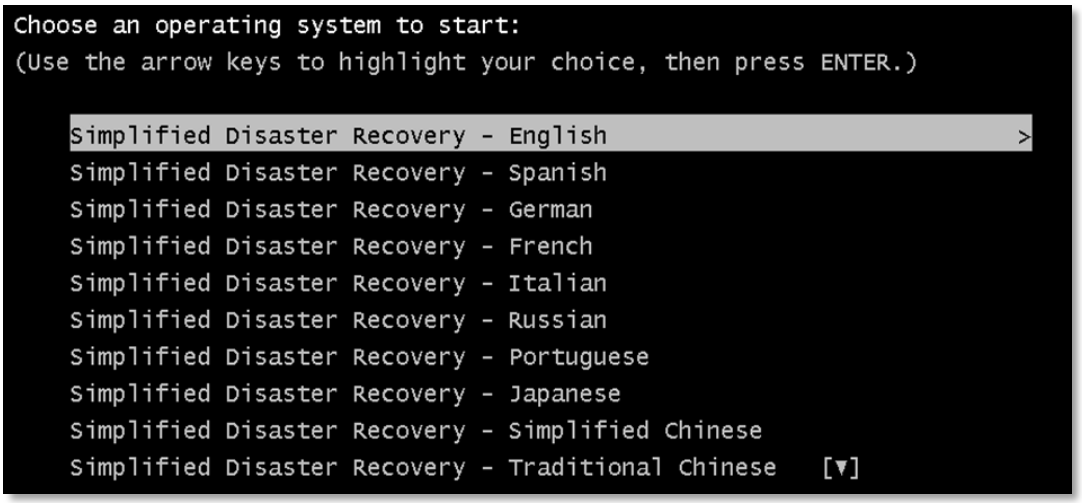

Figure 10: Recovery Disk Language Selection Menu

After a language has been selected, the recovery disk boot process continues and the corresponding language-version of the recovery environment is loaded.

Bare Metal Recovery

During a bare metal or dissimilar hardware recovery operation, the user first boots the server to be restored with the Simplified Disaster Recovery Disk. After the recovery environment has been loaded and the recovery wizard has been started, the user connects to the parent Backup Exec™ 3600 Appliance and identifies the backup set that needs to be restored. The server being recovered is then reconstructed using the data contained in the selected backup set. This includes the process of formatting and partitioning the disk system, restoring basic disk boot components, and recovering the file contents of the server including the operating system and data files.

The bare metal recovery process returns the server to a consistent and functional point in time associated with the selected backup set. The bare metal restore capability of the Backup Exec™ 3600 Appliance automates, simplifies, and significantly speeds up the process of recovering a server from a bare metal state.

Dissimilar Hardware Recovery

The dissimilar hardware recovery feature enables administrators to perform a bare metal recovery of a backup set to a new server with a different hardware configuration. The process of configuring a recovered server for new or dissimilar hardware is fully automated and occurs during a bare metal restore event when a new hardware configuration is detected. The dissimilar hardware recovery process leverages the built-in driver database that comes with the recovery disk. Administrators can add additional drivers to this driver database using the recovery disk customization feature.

Additional Physical Server Recovery Options

In addition to the advanced disaster recovery features supported by the Backup Exec™ 3600 Appliance for the physical servers it is protecting, other non-disaster recovery capabilities are also supported. This includes the following:

Non-disaster Physical Server Recovery Options	
Application recovery	✓
Granular application recovery	✓

File and folder recovery	✓
Redirected recovery	✓

These recovery operations are performed through the connection between the Agent for Windows or Agent for Linux installed to physical servers, and the Backup Exec™ 3600 Appliance.

Note: For additional details on recovery options for physical server environments, or for step-by-step instructions for performing a recovery, please consult the *Backup Exec™ 3600 Administrator's Guid*e available here: DOC4613.

Application Recovery

The Backup Exec™ 3600 Appliance supports the protection and recovery of a wide array of applications and databases, including the ability to perform a full recovery of an application instance. Recovery operations for applications hosted on physical servers are performed through the Backup Exec™ user interface available on the Backup Exec™ 3600 Appliance, and benefit from key features in the Backup Exec™ 2014 user experience. This includes a guided, contextual, and streamlined recovery process.

Granular Application Recovery

The Backup Exec™ 3600 Appliance supports the recovery of granular application objects from a wide array of applications and databases hosted on physical servers. This includes Exchange, SharePoint, SQL, and Active Directory, and many others. Granular recovery is supported after a single pass backup of supported applications. Additional backups in order to achieve granular recovery are not required. Granular recovery operations for applications hosted on physical servers are performed through the Backup Exec™ user interface that is available on the Backup Exec™ 3600 Appliance, and benefit from key features in the Backup Exec™ 2014 user experience. This includes a guided, contextual, and streamlined recovery process.

File and Folder Recovery

Granular file and folder recovery of physical servers is also fully supported by the Backup Exec™ 3600 Appliance. This support applies to a broad range of server platforms, such as Windows, Linux, and Macintosh. Granular file and folder recovery operations are also streamlined by the guided, contextual recovery features of the Backup Exec™ 2014 user experience.

Redirected Recovery

The Backup Exec™ 3600 Appliance also supports redirected recovery of application and file or folder data captured from protected physical servers. Redirected recovery refers to the recovery of data to a server or location that is different from where the data was originally captured for backup purposes.

As with other physical server recovery methods – excluding bare metal recovery operations, which are performed using the Simplified Disaster Recovery Disk – redirected recoveries also benefit from the guided, contextual recovery features of the Backup Exec™ 2014 user experience.

Note: For a comprehensive list of applications, databases, and operating system platforms supported for recovery by the Backup Exec™ 3600 Appliance, please refer to the *Software Compatibility List* (SCL) available here: TECH205797.

Note: For more information on performing the different methods of recovery supported by the Backup Exec™ 3600 Appliance, please refer to the *Backup Exec™ 3600 Administrator's Guide* available here: DOC4613.

Monitoring and Management

The Backup Exec™ 3600 Appliance does not support the direct attachment of a monitor, keyboard, or mouse for local administration purposes. Symantec provides the following remote management capabilities for the Backup Exec™ 3600 Appliance to meet the needs of administrators:

- Appliance Web User Interface
- PowerShell Interface

Appliance Web User Interface

The Backup Exec™ 3600 Appliance includes a web interface that can be used for initial setup and configuration of the appliance, as well as on-going monitoring, and management tasks. Three primary tabs in the Web User Interface expose the monitoring and management tasks available to the administrator.

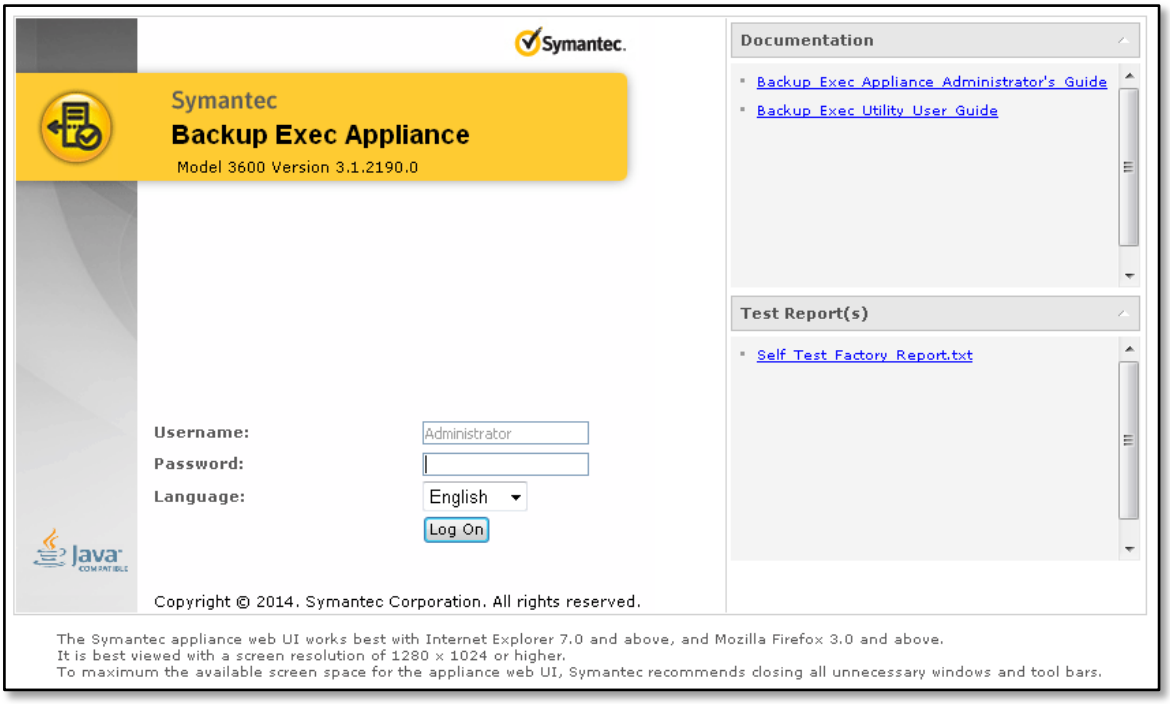

Figure 11: Backup Exec™ 3600 Appliance Web UI - Log On Screen

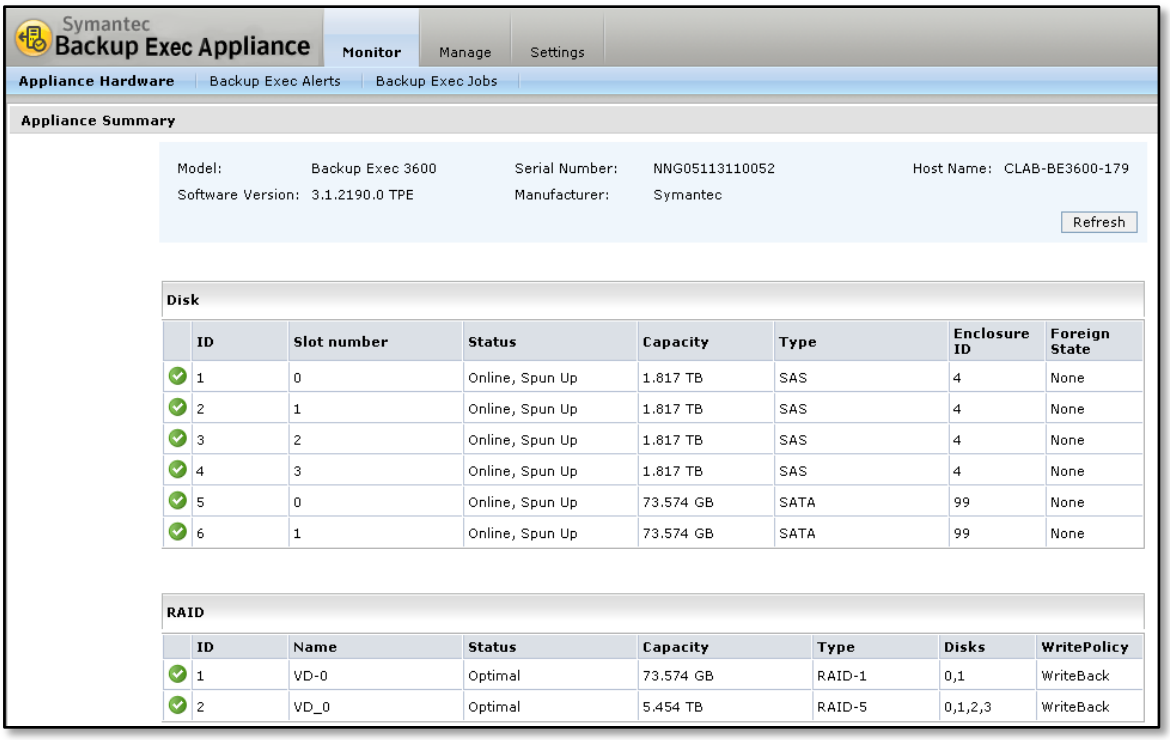

Figure 12: Backup Exec™ 3600 Appliance Web UI - Monitor Tab Screenshot

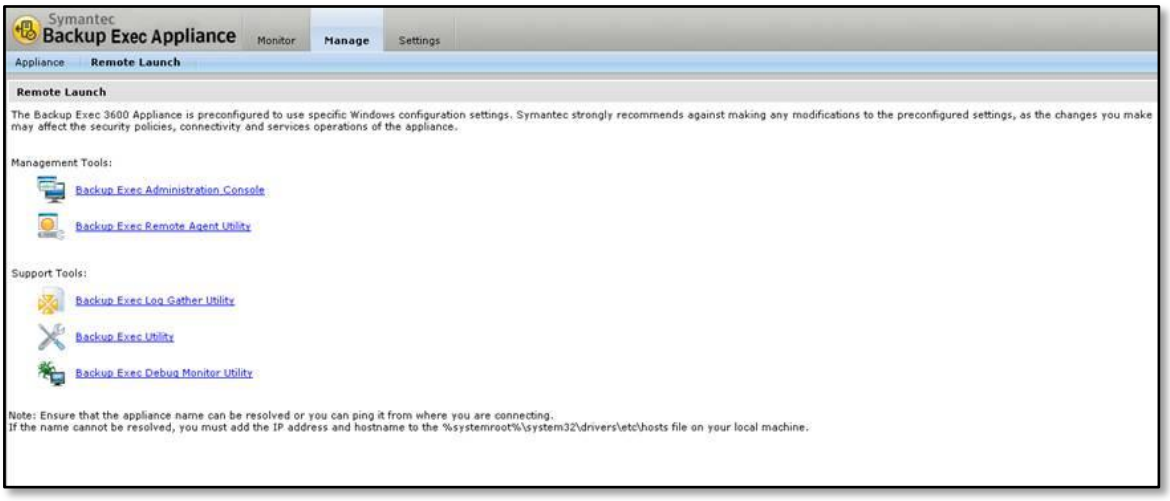

Figure 13: Backup Exec™ 3600 Appliance Web UI - Manage Tab Screenshot

As described by the screenshots above, the Web User Interface can be used to remotely launch the full Backup Exec™ console, giving the administrator full access to the backup and recovery functions of the appliance solution, powered by Backup Exec™ 2014.

The Web User Interface also allows the administrator to manage software updates for the Backup Exec™ 3600 Appliance. This includes software updates for the Windows Storage Server 2008 R2 platform as well as for Backup Exec™ 2014 itself.

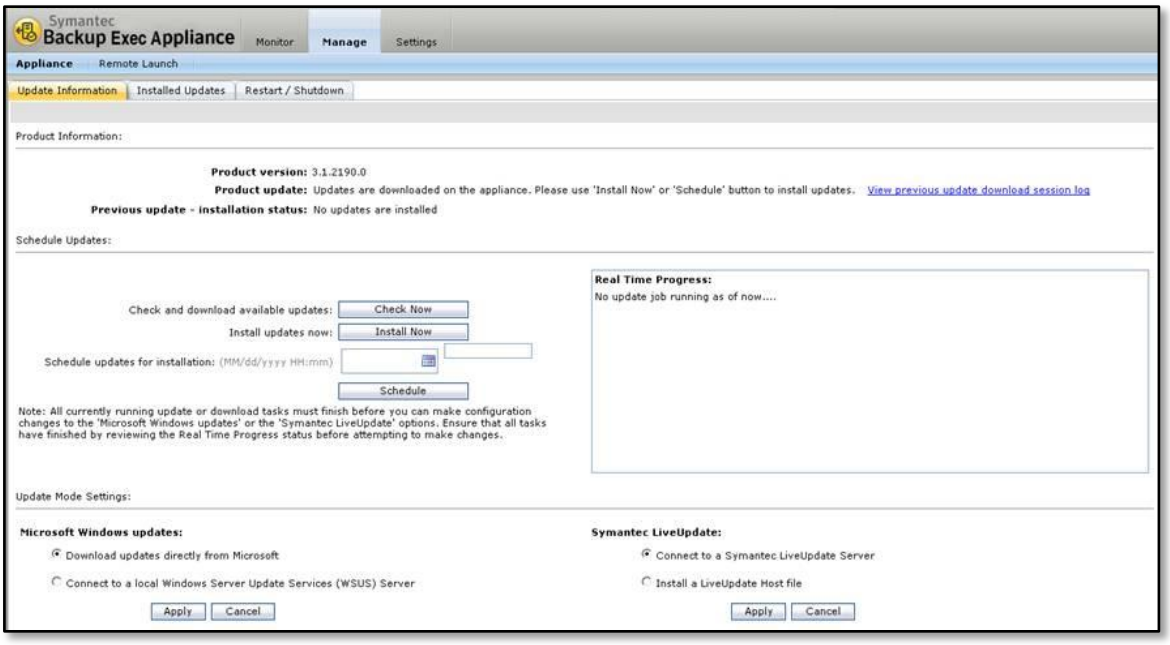

Figure 14: Backup Exec™ 3600 Appliance Web UI - Manage Tab Screenshot

The Web User Interface supports Internet Explorer and Mozilla Firefox web browsers.

PowerShell Interface

In addition, the Backup Exec™ 3600 Appliance includes the Microsoft Windows PowerShell interface for command line monitoring and management operations. The PowerShell interface supports a broad range of predefined parameters that can be leveraged by administrators that have management processes better suited to command line operations.

Note: For more information about the remote management capabilities of the Backup Exec™ 3600 Appliance, please refer to the *Backup Exec™ 3600 Aministrator's Guide* available here: DOC4613.

Example Appliance Scenarios

Single Site

A common scenario for the Backup Exec™ 3600 Appliance involves the protection of a single site. In this scenario, the appliance replaces the traditional backup server, which is commonly constructed of hardware and software components from different vendors that have been manually combined to form a backup server.

In this scenario, the appliance is deployed into the single site environment and configured to protect physical and virtual server resources in the environment. Backup policies are constructed and assigned to the protected server resources, and backup data sets are copied, per the defined schedule, to the disk storage system of the appliance.

From there, backup data is copied offsite. This is accomplished either by copying backup sets to removable USB media (RDX) or tape media, or by copying backup sets to a remote resource, such as a network storage location or to the cloud through integration with the Riverbed SteelStore Appliance (accessed via a CIFS share).

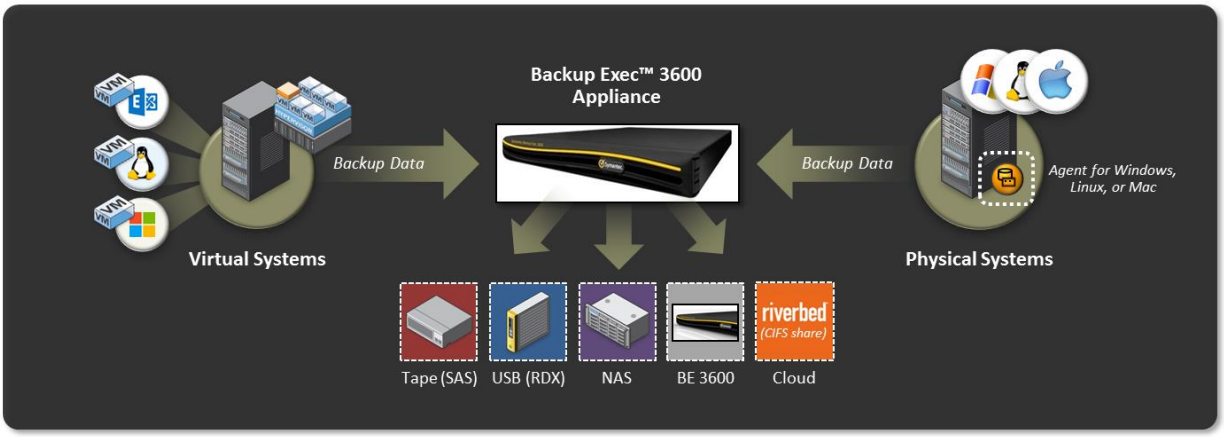

Figure 15: Single Site Appliance Scenario

Virtual Machine Protection

Another important scenario for the Backup Exec™ 3600 Appliance involves the protection of virtual infrastructures. With built-in support for VMware and Hyper-V environments and optimized virtual backup deduplication technology (no additional purchase necessary), the Backup Exec™ 3600 Appliance is a nice fit for environments that are partially or fully virtualized.

The Backup Exec™ 3600 Appliance can act as a single, all-in-one data and application protection solution for both partially and fully virtualized environments.

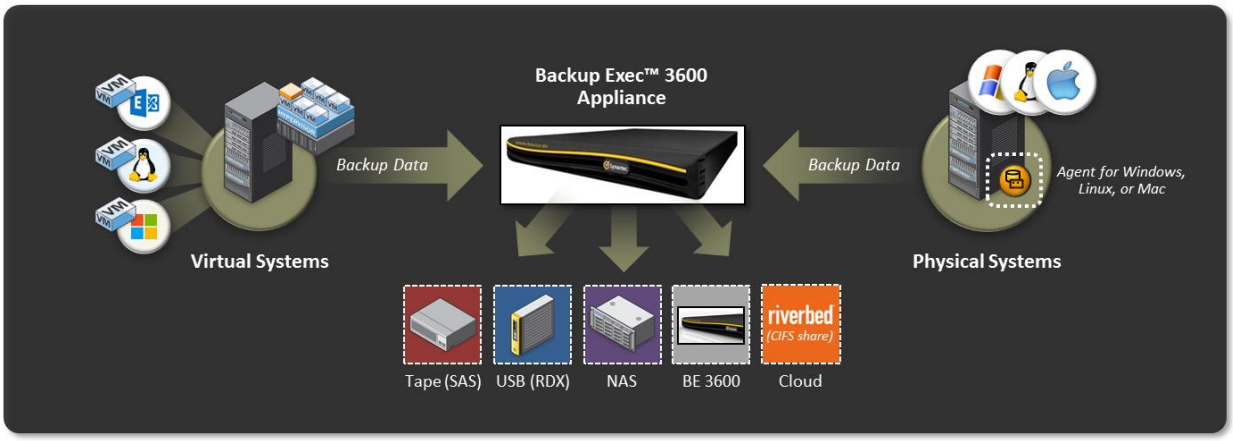

Figure 16: Virtual Server Backup Scenario

Sister Site or Disaster Recovery Site Scenario

Another scenario for the Backup Exec™ 3600 Appliance is the sister site or disaster recovery site scenario. In this example, a Backup Exec™ 3600 Appliance is configured at each site. Backup data sets are captured at each site from protected physical and virtual servers and stored to the disk system of the appliance at that site. These backup sets are also copied or duplicated between each Backup Exec™ 3600 Appliance, ensuring that each appliance contains the complete set of backup data from both sites.

In this scenario, backup data is transferred in deduplicated or compressed form, reducing bandwidth requirements and speeding up the data movement process. This is also known as Optimized Duplication.

In this scenario, one of the Backup Exec™ 3600 Appliances must be promoted to the role of Central Administration Server (CAS), to ensure that catalogs and device sharing methods are managed properly. Another advantage of a CAS is that the operations of both appliances can be controlled and operated from a single location and console.

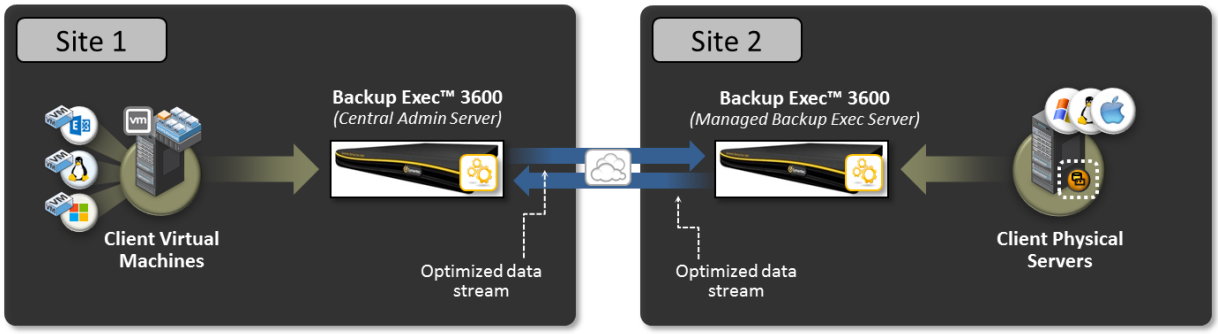

Figure 17: Appliance Sister Site Scenario

Optimized Duplication

To perform optimized duplication between a Backup Exec™ 3600 appliance promoted to a CAS and a managed Backup Exec™ 3600 appliance, the following WAN requirements must be met:

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

Remote Office Scenario

Another key scenario supported by the Backup Exec™ 3600 Appliance involves the protection of remote office environments.

Distributed organizations with server infrastructures at remote sites struggle to properly protect and back up these remote locations, which commonly includes the problem of managing tape media at remote sites. A great way for customers to solve this problem is to implement a Backup Exec™ 3600 Appliance at each of their remote sites. At each remote site, backup data is stored to the Backup Exec™ 3600 Appliance. From there, backup sets are copied 'up stream' to a centralized Backup Exec™ server. This allows for disaster recovery protection of the remote sites without having to manage tape media at those locations.

In this scenario, a CAS must be present. In most cases, the Backup Exec™ server at the central data center would play the role of CAS.

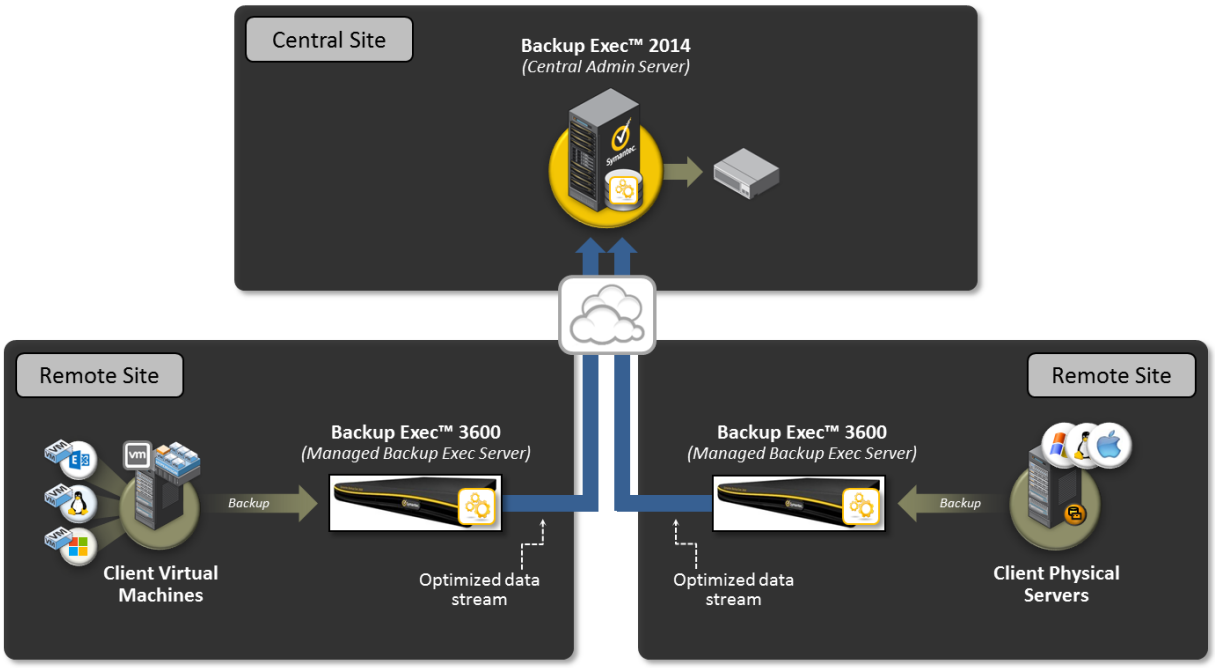

Figure 18: Remote Office Appliance Scenario

In both the sister site and remote office scenarios, backup data is transferred in deduplicated or compressed form, reducing bandwidth requirements and speeding up the data movement process. This is also known as Optimized Duplication.

When large amounts of backup data need to be replicated to another appliance or 'up stream' to a Backup Exec™ server, it may be beneficial to 'seed' the target appliance or server with a bulk of the initial data that needs to be copied. This seeding process will allow each WAN duplication event to only transfer the delta changes.

Hardware Configuration

The hardware configuration of the Backup Exec™ 3600 Appliance was designed with small and midsize organizations in mind. This includes storage, processor, and memory resources with the power needed to provide a high level of performance and sufficient storage capacity to meet the requirements of most small and midsize organizations.

Hardware Configuration Overview

The Backup Exec™ 3600 Appliance is 1U high. The specific hardware configuration details of the Backup Exec™ 3600 Appliance are listed below:

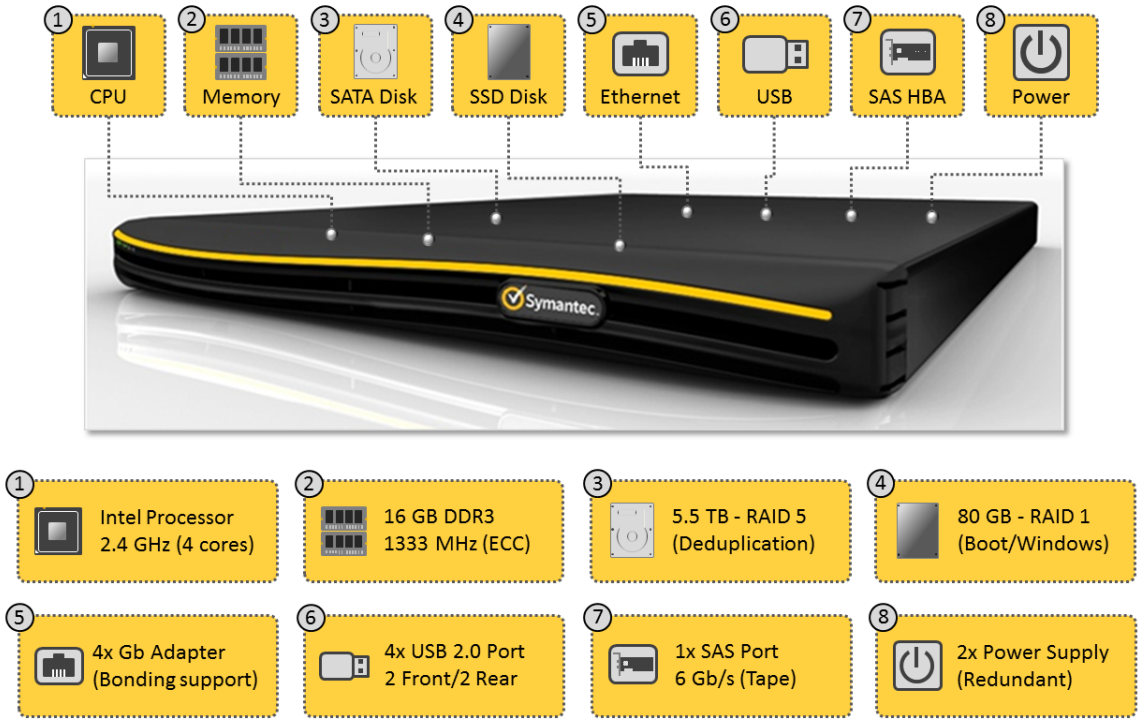

Figure 19: Backup Exec™ 3600 Appliance Hardware Configuration

The disk configuration of the Backup Exec™ 3600 Appliance is composed of two controllers, one SATA controller and one SAS controller.

SSD Disk Configuration

The SATA controller includes an array of two 80 GB solid state (SSD) disks in a RAID 1 configuration with a capacity of 80 GB. The SSD disk array is used for the Windows Storage Server 2008 R2 operating system, and core components of Backup Exec™ 2014.

SATA Disk Configuration

The SATA controller includes an array of four 2 TB SATA disks in a RAID 5 configuration with a usable capacity of 5.5 TB. The SATA disk array is used for housing the Backup Exec™ database, Backup Exec™ logs, Backup Exec™ catalogs, and the deduplication store (backup data).

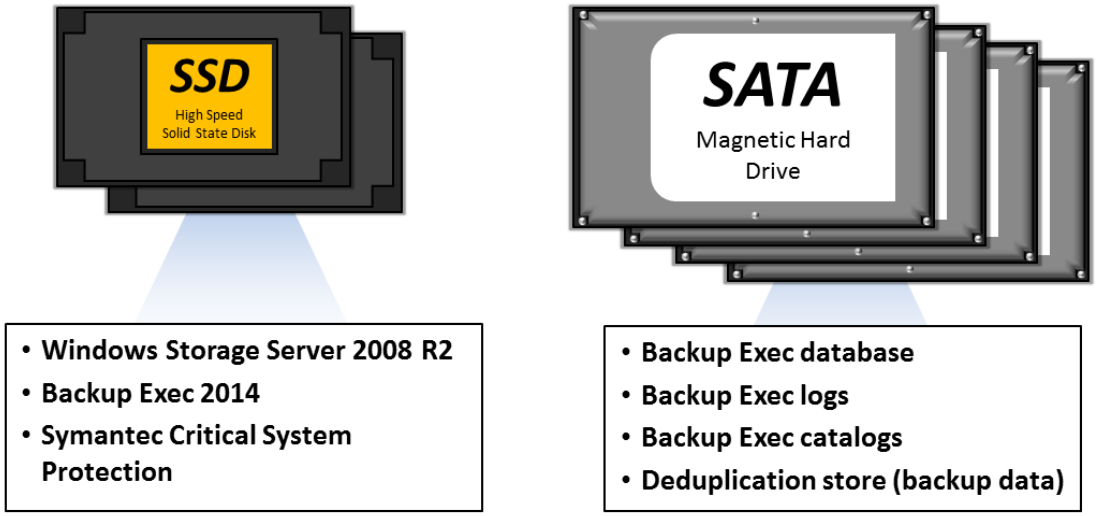

Figure 20: Backup Exec™ 3600 Appliance Disk Configuration

SAS HBA Controller

The Backup Exec™ 3600 Appliance includes an LSI 9212-4i4e SAS HBA to enable the copying of backup sets from the internal disk storage array to external tape devices, or for backing up directly to tape.

Note: A list of supported tape devices that can be used in conjunction with the Backup Exec™ 3600 Appliance can be found in the *Backup Exec™ 2014 Hardware Compatibility List* (HCL), available here: TECH205797.

It is possible to tune the SAS HBA controller for performance purposes. Increasing tape drive block and buffer sizes above the defaults can result in improved performance in some configurations.

Network Controller

With the Backup Exec™ 3600 Appliance, a total of four network ports are available for administrator use. They are as follows:

Network Port	Type	Usage
ETH0 (NIC1)	Public	Setup and configuration. Also available for backup data transport.
ETH1 (NIC2)	Public	Available for backup data transport.
ETH2 (NIC3)	Public	Available for backup data transport.
ETH3 (NIC4)	Public	Available for backup data transport.
ETH4 (NIC5)	*Reserved*	*RMM port – technical support only*

The availability of four network ports allows the administrator to enable network redundancy or to connect the appliance to multiple networks.

Note: Additional details on the hardware configuration of the Backup Exec™ 3600 Appliance can be found at the following location: http://www.symantec.com/business/support/index?page=landing&key=60491.

Warranty and Hardware Replacement

The Backup Exec™ 3600 Appliance comes with one year or three years of advance system replacement in addition to a three-year end user hardware warranty. Hardware warranty service is delivered through an

advanced replacement program. Customer-replaceable parts such as hard drives and power supplies are shipped overnight. If it is determined that there is an issue with a non-replaceable part, a replacement appliance will be shipped overnight. All hardware warranty support is initiated through Symantec Technical Support.

Licensing Overview

The Backup Exec™ 3600 Appliance includes unlimited use of most agents and options in the Backup Exec™ technology family. This includes key agents, such as the Agent for VMware and Hyper-V, as well as key options, such as the Deduplication Option. This licensing approach greatly simplifies the buying experience associated with the Backup Exec™ 3600 Appliance and provides a great deal of flexibility, enabling the Backup Exec™ 3600 Appliance to meet the data and application protection needs of almost any small or medium-sized customer.

Two Backup Exec™ 3600 Appliance License Editions

There are two license edtions of the Backup Exec™ 3600 Appliance. The first, known as the Total Protection Edition (Backup Exec™ 3600T), includes almost the entire line of Backup Exec™ software technologies, with only a few exceptions. The second, known as the Essential Protection Edition (Backup Exec™ 3600E), includes a slightly reduced set of Backup Exec™ software technologies, but still includes all key elements needed to protect most customer environments, such as the Agent for Applications and Databases, the Agent for VMware and Hyper-V, and the Deduplication Option.

The chart below describes the Backup Exec™ software technologies that are either included or optional in each of the two license editions of the Backup Exec™ 3600 Appliance:

Backup Exec 3600 Appliance Editions			
3600 Essential Protection Edition		**3600 Total Protection Edition**	
Included Licenses	**Optional Licenses**	**Included Licenses**	**Optional Licenses**
Agent for Windows	Enterprise Server Option	Agent for Windows	VTL Unlimited Drive Option
Agent for Linux	NDMP Option	Agent for Linux	
Agent for Mac	Remote Media Agent for Linux	Agent for Mac	
Agent for VMware and Hyper-V	Library Expansion Option*	Agent for VMware and Hyper-V	
Agent for Applications/DBs	VTL Unlimited Drive Option	Agent for Applications/DBs	
Deduplication Option		Remote Media Agent for Linux	
		Enterprise Server Option	
		Deduplication Option	
		Library Expansion Option*	
		NDMP Option	

***Library Expansion Option:** The Essential Protection Edition includes support for a single tape drive library. The Total Protection Edition includes support for up to 10 drives.

Figure 21: Backup Exec™ 3600 Appliance Edition Licensing Overview

Note: The Exchange and File System Archiving Options are not supported with either edition of the Backup Exec™ 3600 Appliance.

The agents and options that are included with either license edition of the Backup Exec™ 3600 Appliance allow for the protection of any number of physical and virtual server resources, limited only by the available storage capacity of the deduplication-enabled storage space on the appliance.

Notes and Considerations

General

Disk Capacity

The Backup Exec™ 3600 Appliance does not support disk expansion. For a particular appliance, the user is limited to the 5.5 TB of deduplication-enabled backup storage included within the appliance solution.

Should the storage requirements of an environment surpass the 5.5 TB of storage available on a single Backup Exec™ 3600 Appliance, additional appliance units or additional Backup Exec™ software on third-party server hardware can be added to the environment.

Backup Transport

The Backup Exec™ 3600 Appliance does not include Fibre or iSCSI SAN capability. Backups of SAN-connected servers will travel over the LAN transport path. Four Ethernet ports are available for backup data transport. NIC teaming/bonding is supported.

VMware Notes and Limitations

Virtual Machines Configured with RDM Physical Compatibility Mode Disks

The Backup Exec™ 3600 Appliance cannot protect VMware virtual machines with RDM (Raw Device Mapping) Physical Compatibility Mode disks using image-based (vStorage) backup methods.

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.

Virtual Machines Configured with Fault Tolerance

The Backup Exec™ 3600 Appliance cannot be used to protect VMware Fault Tolerant virtual machines using image-based (vStorage) backup methods.

Once a virtual machine has Fault Tolerance enabled, snapshots are no longer supported on that virtual machine. The Backup Exec™ 3600 Appliance uses snap-based backups via the vStorage API to protect VMware virtual machines, and therefore cannot protect virtual machines with Fault Tolerance enabled using this method.

The only way to back up a virtual machine that is enabled with Fault Tolerance using the Backup Exec™ 3600 Appliance and image-based backups 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 to that virtual machine and protect it as you would a standalone physical machine.

Hyper-V Notes and Limitations

Image-based Backup Requirements

The Backup Exec™ Agent for Windows must be installed to Hyper-V hosts in order to enable image-based protection of Hyper-V guest virtual machines using the Backup Exec™ 3600 Appliance.

Hyper-V Integration Services

Hyper-V Integration Services must be installed to Hyper-V guest virtual machines before online backup of Hyper-V

virtual machines will be possible using the Backup Exec™ 3600 Appliance.

Non-VSS Aware Platforms and Applications

Non-VSS aware platforms and applications, such as Linux, should be protected with the associated Backup Exec™ Agents and not using the image-based backup method.

VHDX Files

Hyper-V virtual machines using VHDX files with a *capacity* larger than 2TB (2040 GB) can be protected and recovered by the Backup Exec™ 3600 Appliance. However, they are not supported for granular recovery operations.

Hyper-V virtual machines using VHDX files with a logical sector size *other than* 512 bytes can be protected and recovered by the Backup Exec™ 3600 Appliance. However, they are not supported for granular recovery operations.

Disk Configuration Limitations

Online backups of certain disk configuration types are unsupported when using image-based backups. These include the following:

- *Remote iSCSI Disks* – Virtual machines utilizing remote iSCSI disks should be protected using the standard Agent for Windows and not the Agent for VMware and Hyper-V.
- *Storage Spaces* – Virtual machines utilizing Storage Spaces should be protected using the standard Agent for Windows and not the Agent for VMware and Hyper-V.
- *Shared Virtual Disks* – Virtual machines utilizing shared virtual disks should be protected using the standard Agent for Windows and not the Agent for VMware and Hyper-V.
- *Physical or Pass-through Disks* – Data residing on physical or pass-through disks cannot be protected using the Agent for VMware and Hyper-V and image-level backups.
- *Dynamic Disks* (http://technet.microsoft.com/en-us/library/cc757696(WS.10).aspx) – Virtual machines using Dynamic Disks can be protected using the Agent for VMware and Hyper-V. However, online backups of these virtual machines are unsupported. Granular recovery of Dynamic Disk volume backups captured through the Agent for VMware and Hyper-V is also unsupported.
- *FAT32 Volumes* - Virtual machines using FAT32-formatted VHDs can be protected using the Agent for VMware and Hyper-V. However, online backups of FAT32 volumes are not supported. Other features, such as granular recovery of FAT32 volumes, are supported via the Agent for VMware and Hyper-V.

For more information on these disk configuration types, please refer to the following Microsoft website: http://technet.microsoft.com/en-us/library/cc754747.aspx.

Windows 2012/R2 Notes and Limitations

Simplified Disaster Recovery

Simplified Disaster Recovery backups and related features, such as bare metal recover, dissimilar hardware recovery, and physical-to-virtual conversions, are supported for Windows 2012 servers.

Simplified Disaster Recovery backups and related features, such as bare metal recover, dissimilar hardware recovery, and physical-to-virtual conversions, are *not supported* for Windows 2012 R2 servers.

ReFS and Deduplication Volumes

Windows 2012 and Windows 2012 R2 servers using ReFS and Deduplication Volumes can be protected and recovered using the Backup Exec™ 3600 Appliance. However, granular recovery is not supported.

Windows 2012 R2 Active Directory Servers

Windows 2012 R2 Active Directory servers can be protected and recovered using the Backup Exec™ 3600 Appliance. However, granular recovery is not supported.

For More Information

Link	Description
www.symantec.com/business/support/index?page=landing&key=60491	**BE 3600 Appliance Support Landing Page**
www.symantec.com/business/backup-exec-for-windows-servers	**Backup Exec™ Family Landing Page**
http://www.symantec.com/connect/articles/backup-exec-partner-toolkit-documentation-resources	**Backup Exec™ Partner Toolkit**
www.symantec.com/business/products/whitepapers.jsp?pcid=pcat_business_cont&pvid=57_1	**White Papers, Datasheets, Solution Briefs**
http://support.veritas.com/docs/304175	**Using Backup Exec™ in Large Environments**
www.backupexec.com/compatibility	**Compatibility Documentation**
www.backupexec.com/skugenerator	**SKU Generator and BEST Tool**
https://partnernet.symantec.com/Partnercontent/Login.jsp	**Symantec PartnerNet Portal**

About Symantec

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

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

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

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