TECHNICAL BRIEF:
SYMANTEC BACKUP EXEC™ 3600 APPLIANCE
TECHNICAL FEATURE BRIEF

Symantec Backup Exec™ 3600 Appliance Technical Feature Brief

Confidence in a connected world. Symantec.

Symantec Backup Exec™ 3600 Appliance Technical Feature Brief

Content

Introduction

This technical feature brief is intended to assist partners and customers as they implement data protection solutions based on the Symantec 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
- Microsoft Hyper-V® integration
- Built-in data deduplication
- Flexible recovery capabilities
- Example scenarios
- Hardware configuration
- Limitations and considerations

For step-by-step instructions on installing, configuring, and managing the Backup Exec 3600 Appliance, please refer to the Backup Exec 3600 Appliance Administrator's Guide.

Business value

There are several important problems associated with building, implementing, and supporting traditional server backup solutions. For many partners and customers, these problems make appliance-based solutions attractive. These problems include complexity, cost, and risk.

Complexity of a traditional backup solution

Building a traditional backup solution can involve many different parts and pieces. These parts and pieces include backup server hardware, the backup server operating system, backup software, backup software agents and options, and maintenance contracts. For some environments, it is also necessary to define and manage a backup storage strategy for remote offices, which can be complicated further if technical personnel resources are not available at remote offices.

In addition, as IT environments continue to adopt virtualization, another layer of complexity is needed to implement a backup solution that matches the needs of virtualized server resources.

Cost of a traditional backup solution

In addition to the problem of complexity, there are significant costs and time investments associated with creating a traditional backup solution. These might include backup software costs, backup software agent and option costs, backup server and storage hardware costs, costs associated with the time and effort needed to install the hardware and software components of the solution, as well as 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 all along the way. All in all, 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 made up 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**—Should the different components 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 parts of the backup solution.
- **Technical support time to resolution**—When dealing with a backup solution composed of hardware and software components from different vendors, troubleshooting and resolving problems can prove difficult. Vendors will each point the finger at another vendor, and issues can bounce back and forth before a solution is identified.

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.

Figure 1: The Backup Exec 3600 Appliance is a simple, cost-effective, and low-risk approach to data and application protection.

Complete virtual and physical protection in a single solution

The Backup Exec 3600 Appliance delivers complete data and application protection for growing VMware and Hyper-V virtual environments combined with protection of physical server environments, all using one consolidated appliance solution. Using the Backup Exec 3600

Appliance, customers and partners can protect all server resources in their environment and avoid the unnecessary costs and headaches associated with implementing and managing multiple backup solutions.

Figure 2: The Backup Exec 3600 Appliance is a simple, cost-effective, and low-risk approach to data and application protection.

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. Solutions such as this include several limitations, such as:

- Impact upon 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® Exchange, SQL®, and Active Directory®.
- Requiring the manual configuration of backup agents and policies for new virtual machines.
- Slow file-by-file backups that capture redundant data in each guest virtual machine over and over.
- Long restores of an entire guest virtual machine in order to recover a single file.

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

- Ability to perform direct backups of virtual environments without the need for a proxy or 'middleman' server.
- Support for image-level backups of virtual machines without having to take virtual machines offline.
- Best practice protection for virtual machines hosting Volume Shadow Copy Service (VSS) aware applications, ensuring application consistency.
- Automatic protection of new virtual machines added to a host since the last backup operation.
- All levels of recovery from a single-pass backup, including virtual machine-level, file-level, application-level, and granular application-level recovery.

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

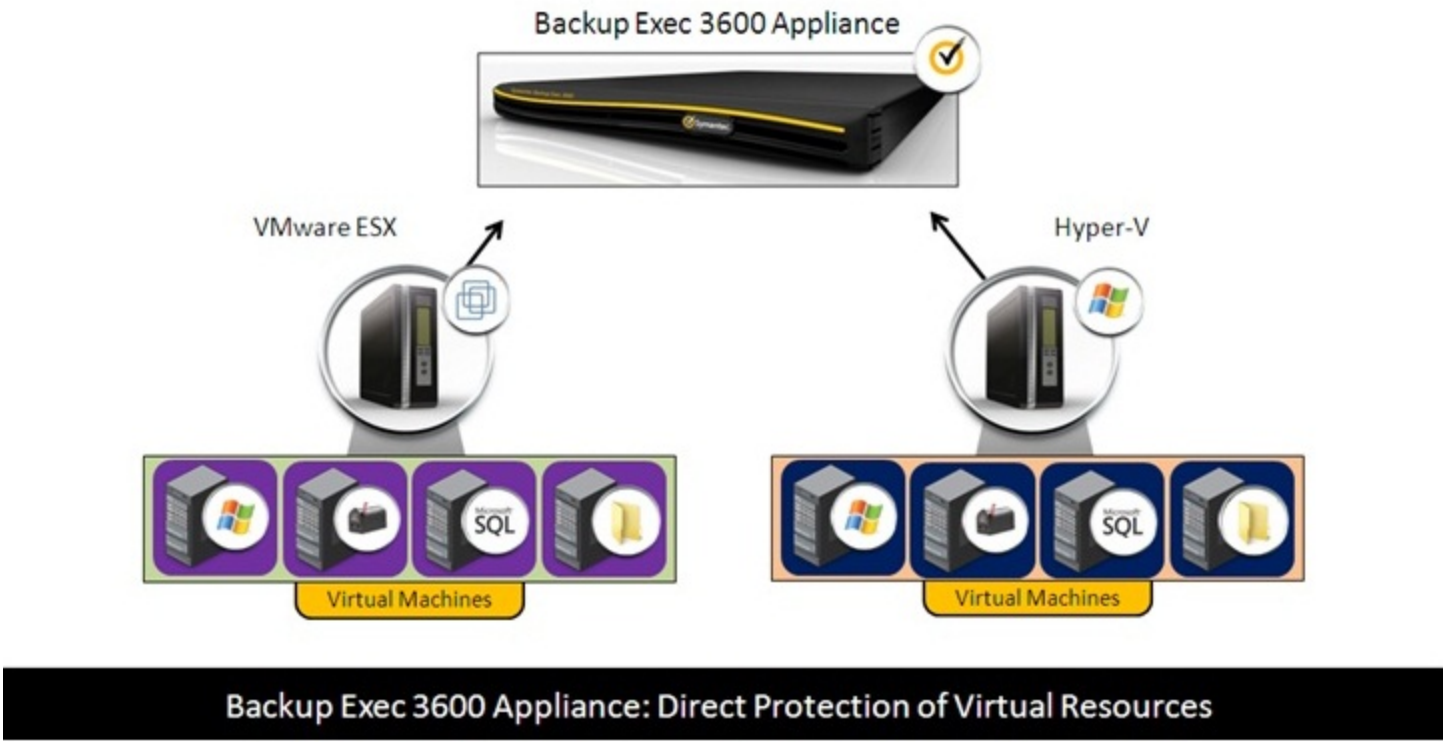

Figure 3: The Backup Exec 3600 Appliance offers direct backup protection of virtual resources; no proxy server is required.

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

Underlying principles

General

The Backup Exec 3600 Appliance is a 1U server system that comes with Backup Exec software pre-installed. The Backup Exec 3600 Appliance is designed to be a complete data and application backup solution for small and midsize environments, and includes the ability to directly protect both physical and virtual servers in an environment.

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

Included software

The Backup Exec 3600 Appliance includes the latest software, Symantec Backup Exec™ 2010 R3.

The operating system included on the Backup Exec 3600 Appliance is Windows® Storage Server 2008 R2 and has been hardened to ensure optimal security and stability in production environments.

Both core software components of the Backup Exec 3600 Appliance, Backup Exec 2010 R3, and Windows Storage Server 2008 R2, are update-enabled. Critical patches and hot fixes will be automatically downloaded and installed according to the configuration settings applied by the administrator during initial setup. 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 called the Agent for Windows® Servers or the Agent for Linux® and UNIX® Servers. With either agent, communication with the Backup Exec 3600 Appliance travels over the Local Area Network (LAN) infrastructure to receive backup job instructions from the Backup Exec 3600 Appliance and to transmit backups of protected data and application elements on the protected server back to the Backup Exec 3600 Appliance for storage.

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

The communication path between the Agent for Windows Servers or the Agent for Linux and UNIX Servers and the Backup Exec 3600 Appliance is encrypted using Transport Security Layer/Secure Sockets Layer (TSL/SSL) encryption technology, and requires a trust relationship between the agent and the Backup Exec 3600 Appliance.

Virtual machine backup methods

For virtual infrastructures, such as vSphere environments or Hyper-V environments, partners and customers have the option to protect virtual machines using host-based backup methods which capture image-level backups of virtual machines associated with the virtual host, or to protect virtual machines using the same agent-based backup method used to protect physical servers. In most cases image-level backups are optimal. Image-level and agent-based backups can be mixed and matched to meet the needs of an environment. For example, a partner or customer may choose to protect all Windows-based virtual machines using image-level backups while protecting Linux-based virtual machines using agent-based backups.

Although the Backup Exec 3600 Appliance fully supports image-based backups of vSphere and 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 the ability to automatically discover applications inside of the virtual machine, perform application granular recovery operations for virtual machines hosting applications such as Exchange, SQL, and Active Directory, and to restore granular file-level elements directly back to the virtual machines from which they were generated.

Hyper-V backups

Image-level backups of Hyper-V virtual machines

When protecting virtual machines on a Hyper-V host using the Agent for Hyper-V, which performs image-level backups, the Backup Exec Agent for Windows Servers 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. As such, the communication between the Agent for Windows Servers 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 for Windows Servers on the Hyper-V host and the Backup Exec 3600 Appliance.

Agent-based backups of Hyper-V virtual machines

When protecting virtual machines on a Hyper-V host without using the Agent for Hyper-V, which is done using an agent within the virtual machines themselves, the same TSL/SSL encryption is used and the same trust relationship is required between the agents on each virtual machine and the Backup Exec 3600 Appliance.

VMware backups

Image-level backups of vSphere virtual machines

When protecting virtual machines on a vSphere host using the Agent for VMware Virtual Infrastructures, which captures image-level backups, backups are captured via integration with the VMware vStorage™ Application Programming Interface (API) and communication with the vSphere host. No Backup Exec agent is installed to the vSphere host itself. To ensure security in these configurations, it is recommended that SSL be enabled on the vSphere host to ensure communication traffic between the vSphere host and the Backup Exec 3600 Appliance remains secure.

Agent-based backups of vSphere virtual machines

When protecting virtual machines on a vSphere host without using the Agent for VMware Virtual Infrastructures, which is done using an agent within the virtual machines themselves, TSL/SSL encryption is used and a trust relationship is again required between the Agent for Windows Servers on each virtual machine and the Backup Exec 3600 Appliance.

Secondary copies of backup data

All backup data is stored to the local physical disk array of the Backup Exec 3600 Appliance, which has a maximum capacity of 5.5 TB. In addition, secondary copies of backup data can be transferred to other locations for additional layers of protection and disaster recovery. Example locations to which secondary copies of backup data can be transferred include:

- Local USB (Backup to disk folder (B2D) and RDX)
- Remote Backup Exec Media Server
- Remote Backup Exec 3600 Appliance
- Remote Network Attached Storage (NAS) Device with B2D
- Nirvanix™ Cloud Storage

It's important to note that the Backup Exec 3600 Appliance does not support direct-attached tape devices or Storage Attached Network (SAN) shared tape devices. If transferring backup data to tape is a requirement for an environment, this can be achieved by connecting the Backup Exec 3600 Appliance to a remote Backup Exec Media Server with access to a tape device.

By offering flexible and state-of-the-art protection for both physical and virtual infrastructures, a high level of data security, and flexible choices for copying data to removable device, off-site, or cloud destinations, the Backup Exec 3600 Appliance is well-suited to meet the data and application protection requirements of most small and midsize IT environments.

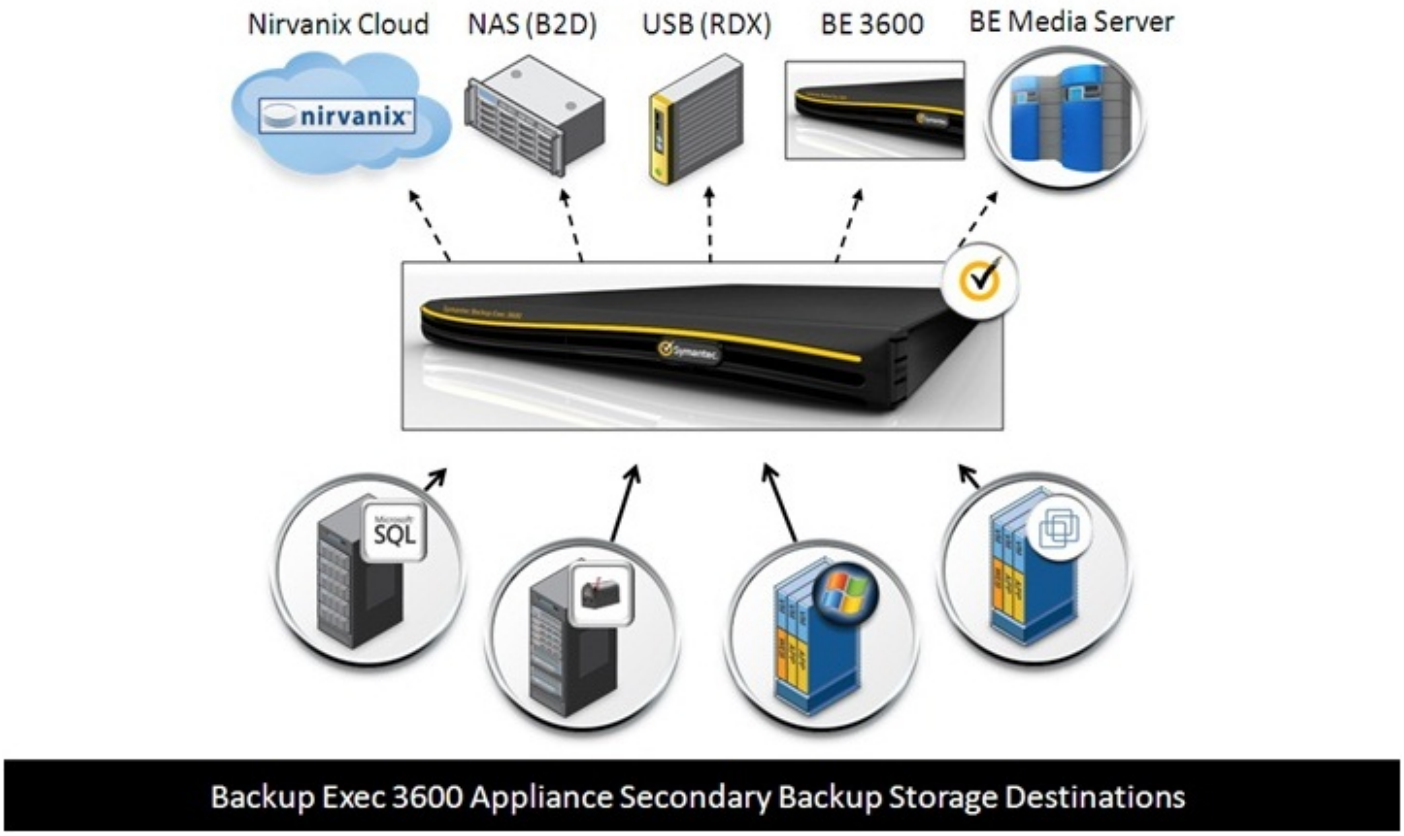

Figure 4: In addition to containing 5.5 TB of deduplication-enabled storage, the Backup Exec 3600 Appliance supports a number of secondary backup destinations

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:

- Proxy-less backup; no proxy server is required to protect VMware virtual machines using the Backup Exec 3600 Appliance.
- The Backup Exec 3600 Appliance includes VMware block-optimization support, which allows the empty space within VMware virtual machine disk (VMDK) files to be ignored, reducing backup sizes and increasing backup performance.
- Differential and incremental backup support allows the Backup Exec 3600 Appliance to capture only the delta changes in a backup operation, further reducing storage requirements and increasing backup speeds.
- Dynamic inclusion enables the automatic protection of new virtual machines added to the VMware environment since the last backup operation.

Best-practice application protection

The Backup Exec 3600 Appliance includes features ensuring that applications such as Exchange, SQL, 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.

Non-VSS compliant virtual machines and applications

Platforms and applications that are not VSS-compliant, such as Linux, cannot be properly protected using VSS. If these virtual machines are protected using the Agent for VMware 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, this approach is not recommended by Symantec.

Administrators using the Backup Exec 3600 Appliance and the Agent for VMware 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 Servers or Agent for Linux and UNIX Servers to protect non-VSS compliant virtual machines. Using the Backup Exec Agent for Windows Servers or the Agent for Linux and UNIX Servers to protect non-VSS-compliant virtual machines helps ensure the virtual machines themselves, as well as the applications they contain, are backed up properly.

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 Hyper-V platform and VSS.

VSS-compliant application protection

The Agent for Hyper-V protection capabilities of the Backup Exec 3600 Appliance provide best practice protection for virtualized application servers such as Exchange, SQL, and Active Directory. 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, normal operations continue.
- VSS-aware applications are protected as part of a normal image-level backup of the entire guest virtual machine.
- Backup process leverages VSS to capture a consistent snapshot of the virtual machine and the VSS-aware applications that it hosts.
- Automatic truncation of transaction logs for Exchange and Active Directory.

Notes: In order for online backups of guest virtual machines to be possible, Hyper-V Integration Services must be installed to guest virtual machines. Also, SQL installations inside of guest virtual machines will still require a separate log-level backup to properly truncate the transaction log of SQL.

Non-VSS compliant virtual machines and applications

Platforms and applications that are not VSS-compliant, such as Linux, cannot be properly protected using VSS. If these virtual machines are protected using the 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 Microsoft Hyper-V that include one or more virtual machines that are not VSS-compliant should consider using the standard Backup Exec Agent for Windows Servers or Agent for Linux and UNIX Servers to protect non-VSS compliant virtual machines. Using the Backup Exec Agent for Windows Servers or the Agent for Linux and UNIX Servers 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

A new technology introduced by Microsoft for their Windows 2008 Server platforms is Cluster Shared Volumes. A Cluster Shared Volume is an New Technology File System (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 Logical Unit Number (LUN).

The Backup Exec 3600 Appliance and the Hyper-V Agent support the protection of Cluster Shared Volume nodes, as well as highly available virtual machines in a Cluster Shared Volume configuration.

When virtual machines are configured for high availability, they are moved to a new location in the backup selection list. Highly available virtual machines appear under the name of the Hyper-V cluster, in the Highly Available Hyper-V machines node. Non-clustered virtual machines remain in the Hyper-V node. When you make a backup selection of Hyper-V virtual machines, the Backup Exec 3600 Appliance checks for any high-availability virtual machines in the environment. If highly available virtual machines are discovered, Backup Exec reminds you to select those virtual machines for backup.

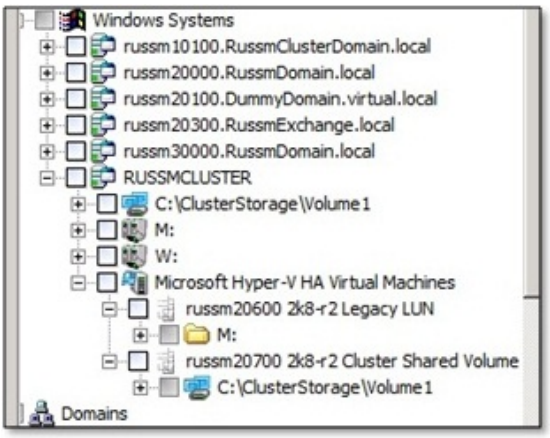

Figure 5: Virtual machines configured for high availability are moved to a different location in the backup selection list.

The Backup Exec 3600 Appliance and the Agent for Hyper-V fully support Live Migration between Hyper-V hosts.

Built-in data deduplication

Data deduplication technology

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

As backup data is captured from protected physical and virtual resources and stored to the disk array in the Backup Exec 3600, 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 can occur at the client 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 and appliance-level calculation methods can be mixed and matched according to the needs of an administrator. For example, an administrator could decide to have all VMware backups captured using the Agent for VMware Virtual Infrastructure and deduplicated at the appliance level, and have all physical backups deduplicated at the client level.

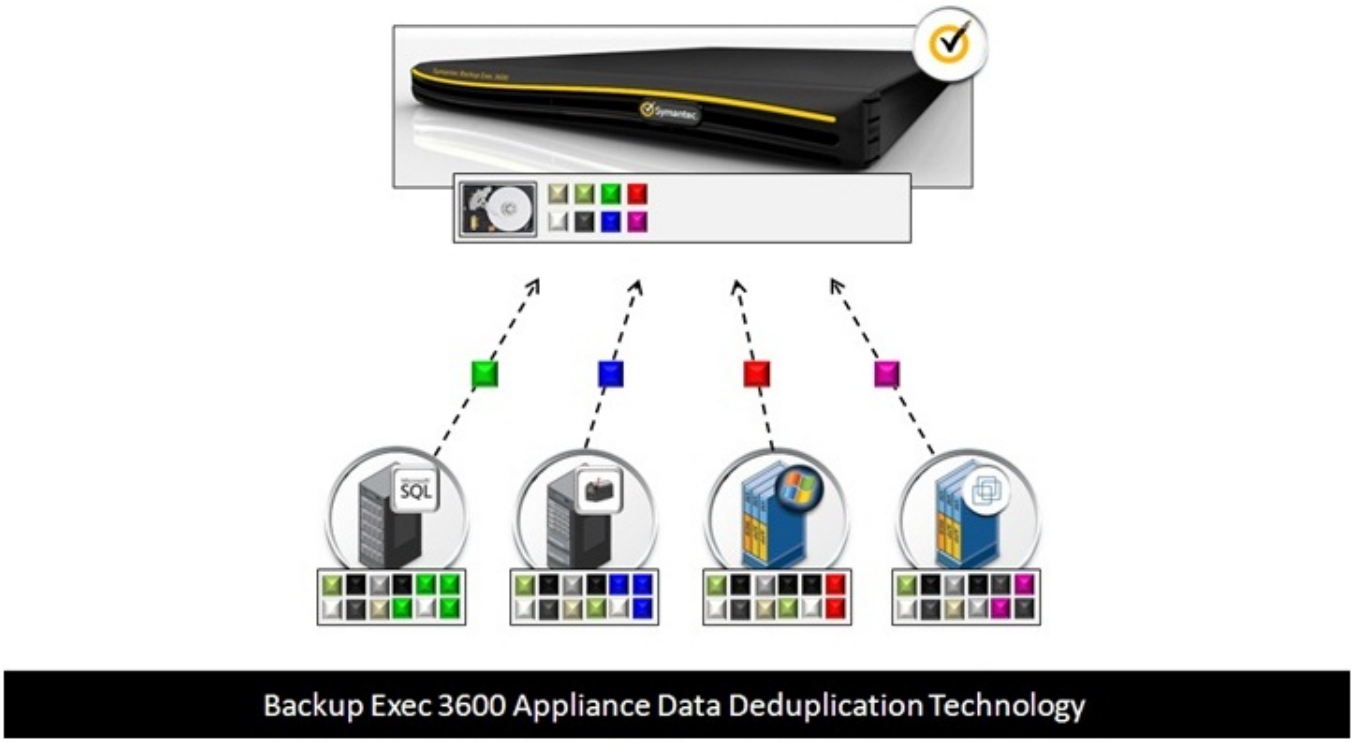

Figure 6: The Backup Exec 3600 Appliance includes data deduplication technology that greatly increases its backup data storage efficiency.

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 or virtual resources.

Optimized data deduplication for VMware backups

The data deduplication technology within the Backup Exec 3600 Appliance includes specific optimization for backups of VMware virtual machines.

The core data component of a VMware virtual machine is the VMDK file, known commonly as the virtual disk. The VMDK file is analogous to the hard drive or hard drive array found in physical server systems. Although VMDK files are stored in a proprietary VMware file format (VMDK), the Backup Exec 3600 Appliance includes specific intelligence that allows it to understand and interpret file structures within VMDK files and efficiently deduplicate them. This is made possible through a component known as a VMDK stream handler, which operates invisibly to the backup process.

As deduplication-enabled backups of VMware virtual machines are processed by the Backup Exec 3600 Appliance, blocks are aligned to file extent boundaries as they occur within a VMDK file. This deduplication method is known as variable-length segmenting, and is made possible by the VMDK stream handler included in the Backup Exec 3600 Appliance. The result of this technology is that data changes within a VMDK file that occur over time as a virtual machine performs normal operations result in fewer unique blocks being identified during the deduplication fingerprinting process. This results in less backup data being stored and a smaller storage footprint.

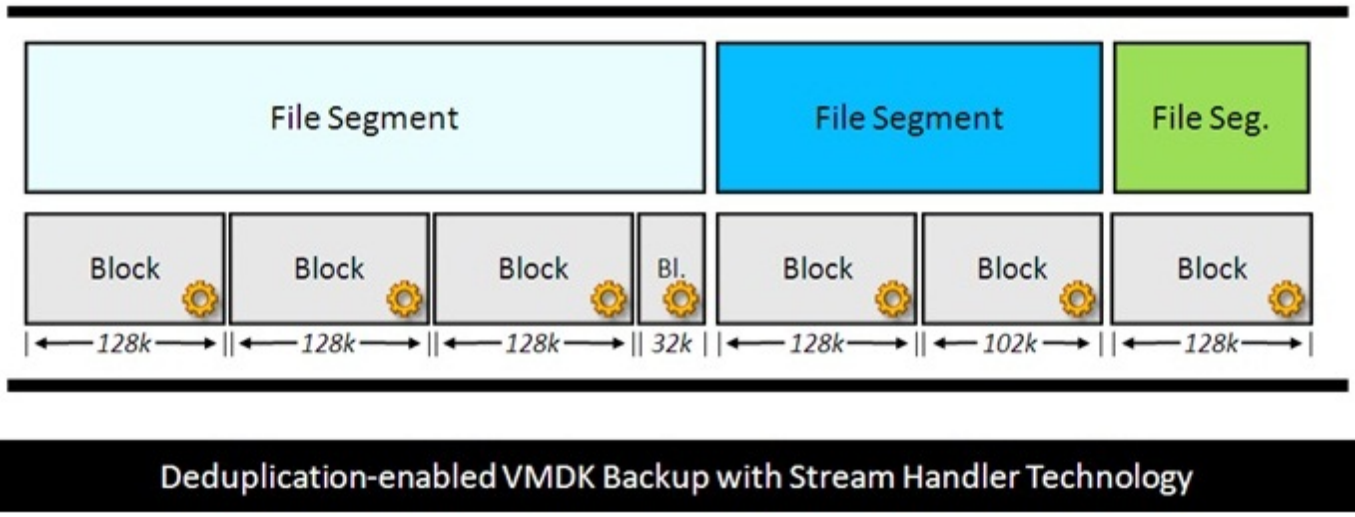

Figure 7: The data deduplication technology within the Backup Exec 3600 Appliance includes specific optimization for backups of VMware virtual machines.

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

Flexible 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 a certain level 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:

- Full virtual machine recovery
- VMDK/Virtual Hark Disk (VHD) 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 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, redirected to an alternate virtual host, or recovered to a local

directory on the Backup Exec 3600 Appliance. Additional features are also included, such as the option to automatically power off the target virtual machine 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.

Application recovery

For VMware and Hyper-V guest virtual machines hosting Exchange, SQL, 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, 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 applicable Backup Exec application agent must be licensed at the media server and the Backup Exec Agent for Windows Servers must be installed to the guest virtual machine that hosts the application before backup.

Granular application recovery

The VMware and Hyper-V Agents included with the Backup Exec 3600 Appliance enable administrators to recover granular application objects from single-pass backups of VMware and Hyper-V guest virtual machines. This includes Exchange mailboxes, emails, attachments, and calendar items, Active Directory objects such as user and computer objects, and SQL databases.

A separate database-level or object-level backup is **not** required to enable granular application recovery.

To enable granular application recovery, the Backup Exec Agent for Windows Servers must be installed to the guest virtual machine that hosts the application before backup.

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 Servers installed to the guest virtual machine in order for granular files and folder recovery to be possible. However, having the Backup Exec Agent for Windows Servers installed to the guest virtual machine is required in order to recover files and folders directly back to the source virtual machine.

Optionally, files and folders can be recovered to a local directory on the media server, and moved back to the original guest virtual machine using other methods.

Redirected recovery

Recovery operations of 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 an alternate virtual machine different from the original from which the backup was captured, if the Agent for Windows Servers is present on the target virtual machine.

For granular file/folder recovery from a backup of a VMware or Hyper-V virtual machine when the Agent for Windows Servers is not present on the target virtual machine to which a file or folder needs to be recovered, a work around is to restore the file/folder data to a local directory on the Backup Exec 3600 Appliance, and then transfer the restored data to the target virtual machine using standard networking processes, such as a Windows share.

For additional details on recovery options for VMware and Hyper-V environments, or for step-by-step instructions for performing a recover, please consult the Administrator's Guide.

Physical server recovery options

The Backup Exec 3600 Appliance supports a full range of data and application recovery capabilities for physical servers. This includes:

- Application recovery
- Granular application recovery
- File and folder recovery
- Redirected recovery

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

For additional details on recovery options for physical server environments, or for step-by-step instructions for performing a recover, please consult the Administrator's Guide.

For a complete list of supported platforms and applications, please consult the Software Compatibility List available here.

Example appliance scenarios

Single site

A common scenario for the Backup Exec 3600 Appliance is the single site scenario where the appliance replaces the traditional media server constructed of hardware and software components from different vendors manually combined to form a backup server.

In this scenario, the appliance is deployed into the single site environment and configured with remote Backup Exec agents deployed to physical and virtual server resources that will be protected. Backup jobs are constructed and assigned to the protected server resources, and backup data sets are copied, as per the job schedule, to the disk storage system of the appliance.

From there, backup data is copied off-site. This is accomplished either by copying backup sets to removable USB media (RDX), or by copying backup sets to a remote resource, such as a network B2D folder or a Nirvanix cloud storage account.

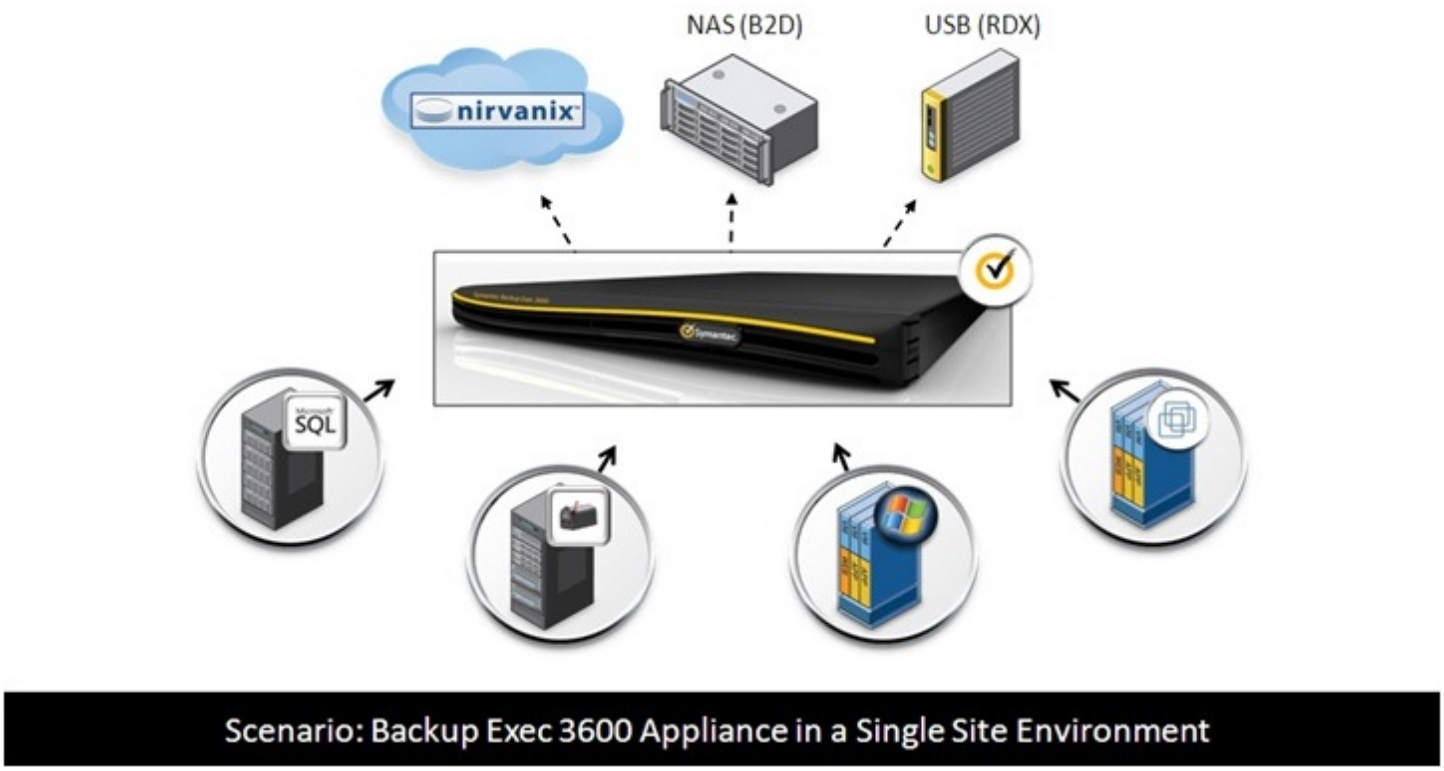

Figure 8: Example Backup Exec 3600 Appliance configuration from a single site.

Virtual server backup

Another important scenario for the Backup Exec 3600 Appliance is virtual environments. With built-in support for VMware and Hyper-V protection, as well as 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 solution for both partially and fully virtualized environments.

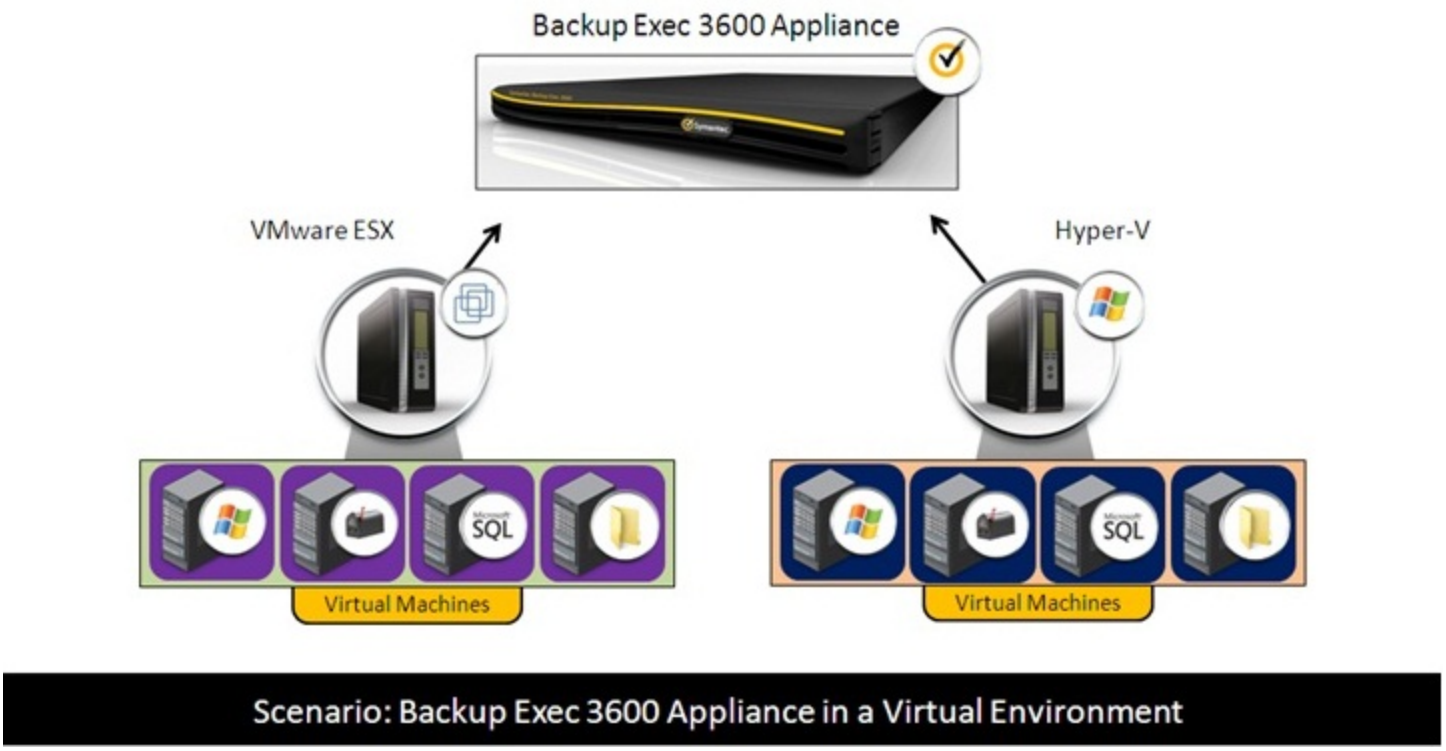

Figure 9: Example Backup Exec 3600 Appliance configuration in a virtual environment.

Sister site or disaster recovery (DR) site scenario

Another scenario for the Backup Exec 3600 Appliance is the sister site or DR site scenario where a Backup Exec 3600 Appliance is configured at each site, with remote agents deployed to protected physical and virtual server resources. Backup data sets are captured at each site from protected 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 taken from both sites.

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 are managed properly. Another advantage of a CAS is that the operations of both appliances can be controlled and operated from the single CAS console.

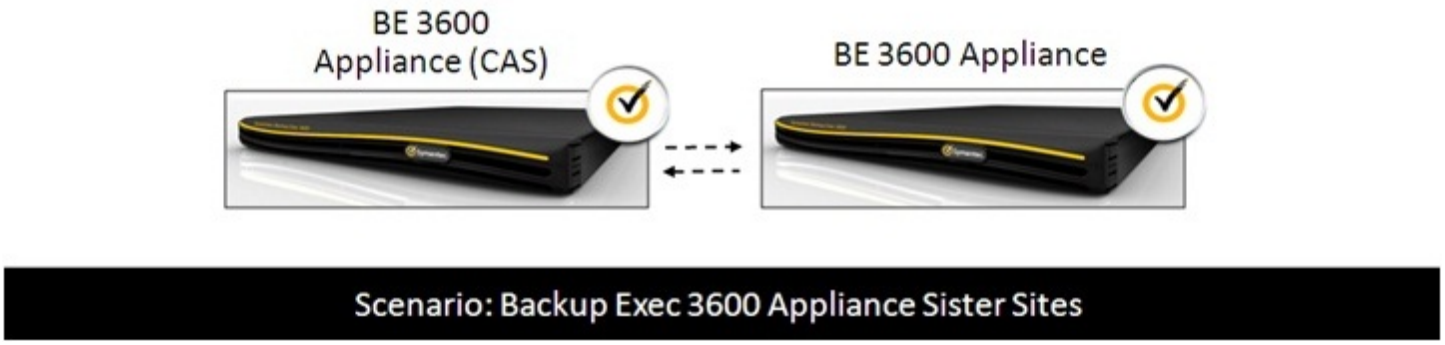

Figure 10: Example Backup Exec 3600 Appliance configuration for a sister site evironment.

Remote office scenario

Another key scenario supported by the Backup Exec 3600 Appliance is the remote office scenario.

Distributed organizations with server infrastructure at remote sites struggle to properly protect and back up servers at remote sites, 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, server backup data is stored to the Backup Exec 3600 Appliance. From there, backup sets can be copied 'up stream' to a centralized Backup Exec media server, which allows for DR protection of the remote sites without having to manage tape media at the remote sites.

In this scenario, a central administration server must be present, and most cases, the Backup Exec media server at the central data center would play this role.

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.

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

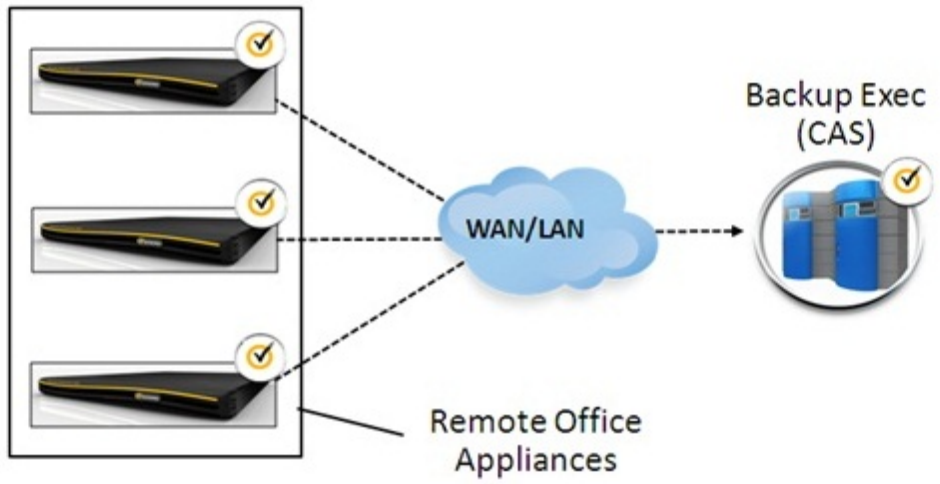

Figure 11: Example Backup Exec 3600 Appliance configuration for a remote office environment.

Symantec NetBackup PureDisk™ Appliances

It is also possible to use one or more Backup Exec 3600 Appliances along with a Symantec NetBackup™ Deduplication Appliance, such as the NetBackup 5000 and 5020 Appliances.

The configuration is similar to that of the remote office scenario, except that one of the Backup Exec 3600 Appliances will have to be promoted to the role of central administration server, with the NetBackup Appliance being configured as a target for backup data duplication.

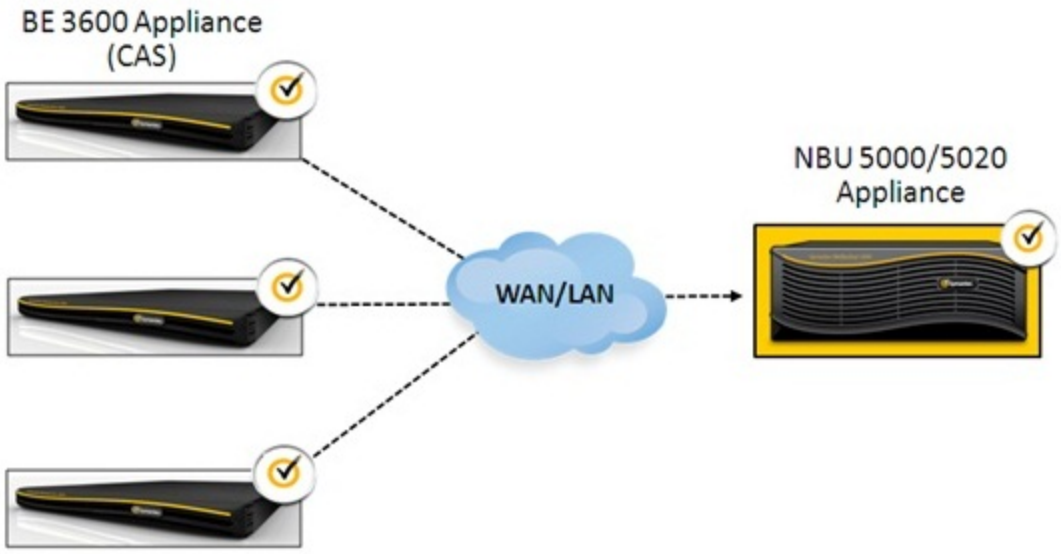

Figure 12: Example Backup Exec 3600 Appliance configuration with a NetBackup PureDisk Appliance.

In this scenario, backup data is transferred to the NetBackup Appliance in deduplicated or compressed form, reducing bandwidth requirements and speeding up the data movement process.

Hardware configuration

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

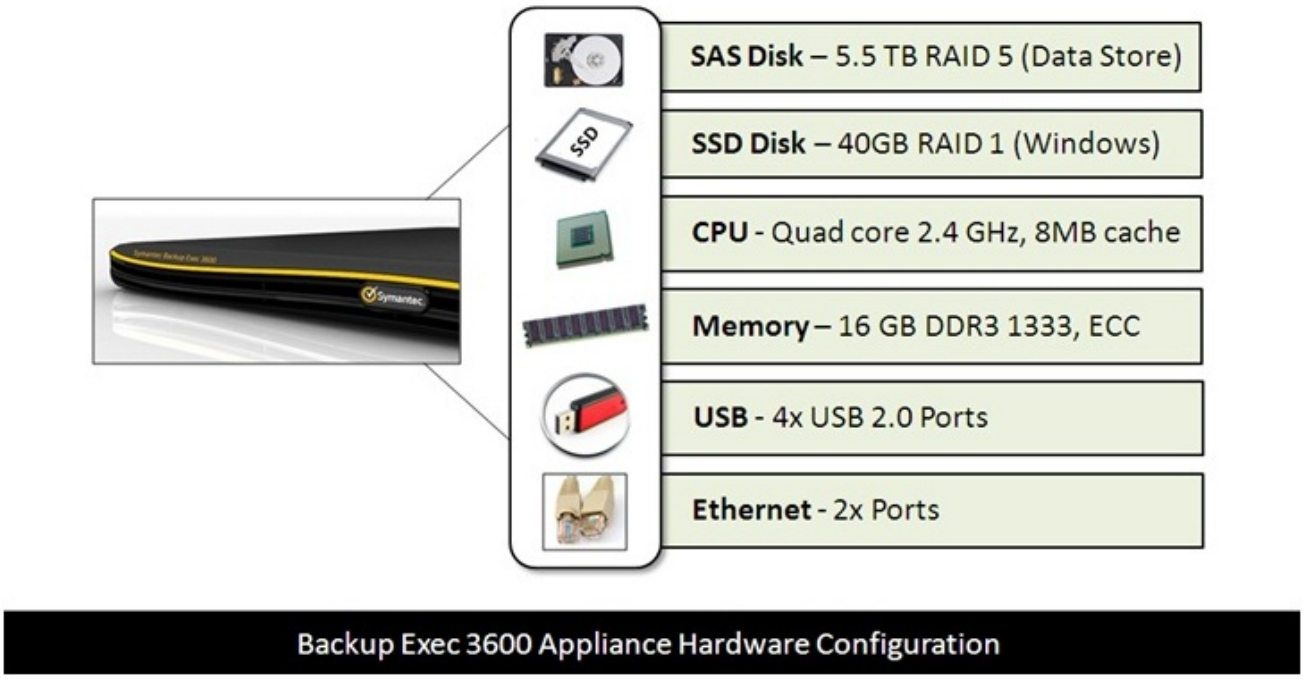

Figure 13: Backup Exec 3600 Appliance hardware configuration.

The disk configuration of the Backup Exec 3600 Appliance includes a set of solid state (SSD) disks on which the operating system, Windows Storage Server 2008 R2, is housed. The 5.5 TB array of SAS disks is used for housing backup data captured in the environment.

It's important to note that although the diagram above lists two Ethernet ports on the appliance, and only one Ethernet port is available for data transport. The other Ethernet port is used by the administrator to connect to the appliance for setup and management purposes, and cannot be used for transport of backup data.

The Backup Exec 3600 Appliance includes dual power supplies.

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.

Licensing overview

The Backup Exec 3600 Appliance includes all-you-can-eat access to most agents and options included in the Backup Exec technology suite. This includes key agents, such as the Agent for VMware and the Agent for 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 midsized customer.

Here is a list of Backup Exec technologies that are either included, available to be purchased, or not supported by the Backup Exec 3600 Appliance:

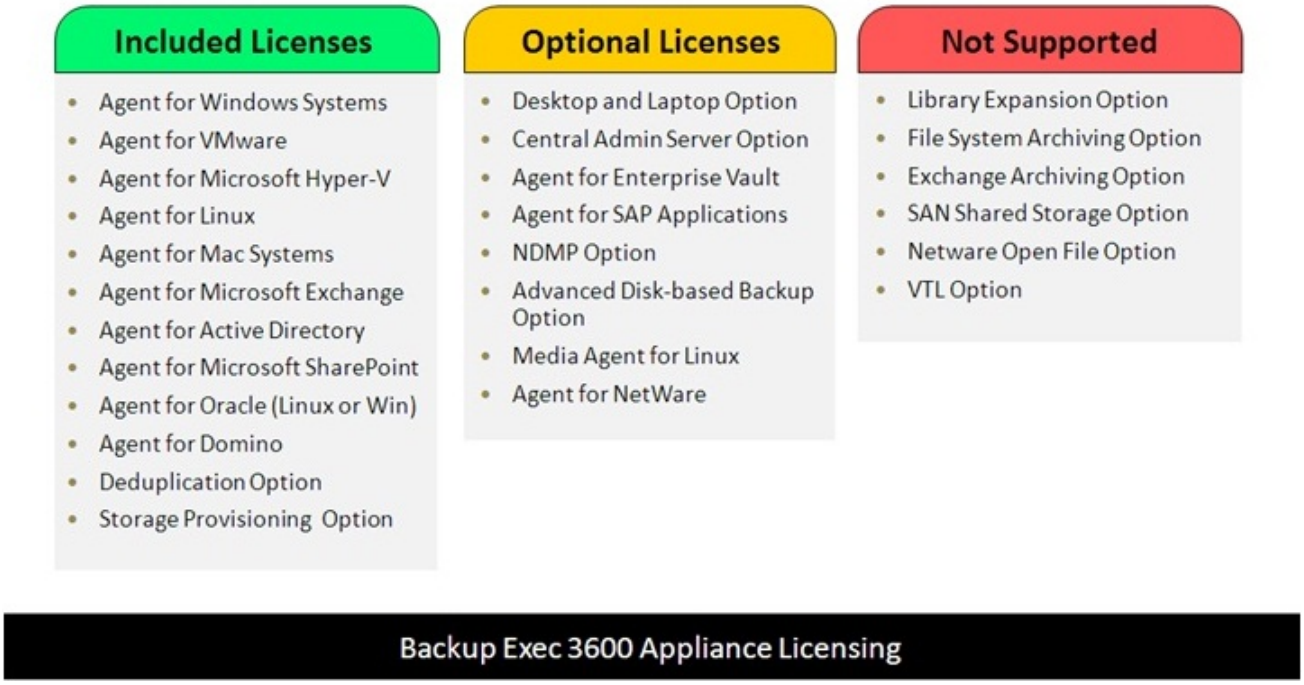

Figure 15: The Backup Exec 3600 Appliance includes a large number of a key Backup Exec Agent and Option technologies in an all-you-can-eat model.

The agents and options that are included with the Backup Exec 3600 Appliance allow for the protection of any number of physical and virtual server resources, limited only by the available 5.5 TB of deduplication-enabled storage space on the appliance.

Limitations and considerations

General:

- **No disk expansion support**—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 hardware can be added to the environment.
- **LAN-based backups**—The Backup Exec 3600 Appliance does not include Fibre SAN or iSCSI SAN capability. Backups of SAN-connected servers will travel over the LAN transport path. Only one Ethernet port is available for backup data transport, and as such NIC teaming is currently unsupported.
- **No direct-attached tape support**—The Backup Exec 3600 Appliance does not support direct-attached tape devices. For removable storage support, a removable USB (RDX) device can be used, or the appliance can be connected to a remote Backup Exec server with access to a tape device. Backup sets can be copied to the remote Backup Exec server and stored to tape there.

VMware notes and limitations:

Virtual machines configured with Raw Device Mapping (RDM) physical compatibility mode disks

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

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

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

Virtual machines configured with GUID Partition Table (GPT) disks

The Backup Exec 3600 Appliance can be used to back up and recover virtual machines that are configured with GPT disks using image-level (vStorage) backups. This includes full, differential, and incremental backups. However, granular file/folder recovery and granular application recovery from virtual machines configured with GPT disks is not currently supported using image-based (vStorage) backups.

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

Virtual machines configured with vSphere 4.0 Fault Tolerance

The Backup Exec 3600 Appliance cannot be used to protect vSphere 4.0 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 Servers to that virtual machine and protect it as you would a standalone physical machine.

Virtual Machines Located on Network File System (NFS) Storage

Due to limitations in the VMware vStorage API, the Backup Exec 3600 Appliance, when using image-based (vStorage) backup methods, is unable to determine used vs. unused blocks of VMDK files associated with virtual machines located on NFS storage. This results in image-based (vStorage) backups of virtual machines on NFS storage captured by the Backup Exec 3600 Appliance to be full backups, including both used and unused blocks of VMDK files.

A workaround for protecting VMware virtual machines located on NFS storage with the Backup Exec 3600 Appliance is to install the Backup Exec Agent for Windows Servers to the virtual machines and protect them in the standard fashion.

Hyper-V notes and limitations

Image-based backup requirements

The Backup Exec Agent for Windows Servers 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.

No incremental/differential backup support

Incremental and differential backups are currently unsupported for image-based backups of Hyper-V virtual machines using the Backup Exec 3600 Appliance; all backups are full backups of the virtual machine and associated VHD files.

No block optimization support

Block optimization is currently unsupported image-based backups of Hyper-V virtual machines using the Backup Exec 3600 Appliance. This means that the entire VHD is protected during backups (including free space within the VHD).

Non-VSS aware platforms and applications

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

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 Backup Exec Agent for Windows Servers.
- **Physical or pass-through disks**—Virtual machines utilizing physical or pass-through disks should be protected using the standard Backup Exec Agent for Windows Servers.
- **Dynamic Disks** (http://technet.microsoft.com/en-us/library/cc757696(WS.10).aspx) —Virtual machines using Dynamic Disks can be protected. However, online backups of these virtual machines are unsupported. Granular recovery of Dynamic Disk volume backups captured through image-based backup is also unsupported. Virtual machines utilizing Dynamic Disks can be protected using the standard Backup Exec Agent for Windows Servers.
- **GPT disks**—Online backups of virtual machines using GPT disks, as well as granular recovery of virtual machines using GPT disks is unsupported. Virtual machines utilizing GPT disks should be protected using the standard Backup Exec Agent for Windows Servers.
- **FAT32 volumes**—Virtual machines using FAT32-formatted VHDs can be protected using image-based backups. However, online backups of FAT32 volumes are not supported. Other features, such as granular recovery of FAT32 volumes, are supported.

For more information on these disk configuration types, please visit: http://technet.microsoft.com/en-us/library/cc754747.aspx.

For more information

Link	Description
http://www.symantec.com/business/support/index?page=landing&key=60491	Backup Exec 3600 Appliance support landing page
www.backupexec.com	Backup Exec family landing page

Link	Description
www.symantec.com/business/products/whitepapers.jsp?pcid=pcat_business_cont&pvid=57_1	White papers, data sheets, 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

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.

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 © 2011 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
10/2011 21215015