

WASABI SYSTEMS INC.

Using Wasabi Storage Builder[®] with Symantec[®] Backup Exec[™]



Version 2.0
September 2006

How to Contact Wasabi

Wasabi Systems Inc.
500 E. Main Street, Suite 1520
Norfolk, VA 23510 USA

EMAIL: info@wasabisystems.com
PHONE: +1 (757) 248-9601
FAX: +1 (757) 299-8075
URL: <http://www.wasabisystems.com/>

Font Conventions

This manual uses the following highlighting conventions:

- **Boldface** indicates graphical user interface (GUI) controls such as the names of menus and fields, the text found within the fields, or drop box entries and selections. It is also used to highlight terms in the glossary.
- **Bold Helvetica** indicates buttons.
- *Italics* indicates book titles and emphasized words.
- Courier font indicates code samples:
`syslog`
- Blue Courier font indicates complete Internet addresses (URLs):
<http://www.wasabisystems.com/>

Copyright© 2006, 2007 Wasabi Systems Inc., 500 East Main Street, Suite 1520, Norfolk, VA, 23510. All rights reserved. This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Wasabi Systems Inc. and its licensors, if any. Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California; full license and copyright information is available at: <http://www.netbsd.org/Goals/redistribution.html>. Wasabi®, the Wasabi logo, Flashware®, and Storage Builder® are registered trademarks of Wasabi Systems Inc. All other brand and product names are trademarks of their respective owners. WSBBackup_20060918

Contents

Configuration Instructions	1
Prerequisites	6
Develop a Backup Strategy	6
Install and Configure Windows 2003.....	6
Install and Configure the Storage Builder iSCSI Target.....	7
Install the Microsoft iSCSI Initiator v2.0	8
Using Symantec Backup Exec.....	10
Configuring the iSCSI Node for Storing Data.....	10
Backing Up to an iSCSI Node.....	12
Conclusion	24
Definitions	25
References.....	27



Configuration Instructions

Wasabi Storage Builder® for IP-SAN is a fast, powerful, and cost-effective IP-based storage area network (IP-SAN) solution. Built on Wasabi's industry-proven storage systems and software technologies, Storage Builder for IP-SAN delivers top-notch features and performance at a price that's hard to beat.

This document provides a technical overview of how to use Wasabi Storage Builder for IP-SAN (Storage Builder) as a disk-based backup solution created over IP with Symantec Backup Exec™ version 10d (Backup Exec) on Microsoft Windows® 2003 Advanced Server (Windows 2003). We recommend using this application note in combination with a comprehensive backup plan to create a reliable backup strategy for your organization.

Backing up data is one of the most important activities for any organization. The loss of data to any organization can greatly impact the productivity and, more importantly, the financial stability of an organization. In combination with an effective backup plan, disk-based backup over IP is a valuable tool to quickly and efficiently protect an organization's data.

First, we will provide some background on traditional disk-based backup. Disk-based backup refers to the process of creating a backup of current data on one or more hard disks. This allows for much faster data access compared to creating backups only on tape. This data can then be later archived on tape for long term storage. Disk-based backup provides a number of cost benefits when used by itself or in combination with tape. Table 1 highlights many of these benefits.

<i>Benefit</i>	<i>Description</i>
Backup Consolidation	Rather than using a large number of tapes, all backups can be consolidated onto a single machine. Hard drives are less likely to be misplaced than tape and take up far less space than keeping an expanding collection of tapes.
High Performance	Data backup and restore operations can be achieved much faster with disk than with tape. This becomes increasingly important as the volume of data continues to rise, but the backup windows remain the same or even decrease. Disk-based backup also allows you to restore single files without having to index through the entire tape, resulting in a much faster restore time.
High Reliability	In combination with hardware or software RAID, loss of a drive doesn't invalidate the backup sequence. Some experts estimate that 25% to 50% of tape backups do not restore 100% of the data that was backed up to tape due to corrupted data.
Durable Medium	Hard drives last longer, data can be rewritten more often and the media is isolated from environmental conditions such as dust.
No Multiplexing of Tapes	Manually swapping out tapes can be time consuming.

Table 1: Benefits of Disk-based Backup

Storage Builder leverages all the benefits of traditional disk-based backup as well as providing many additional advantages. It relies on a protocol, iSCSI, which allows the transfer of data over an IP network. This makes possible the creation of low-cost IP-SANs using an existing intranet, rather than having to use expensive Fibre Channel connections. In combination with an iSCSI initiator, disk-based backup creates a versatile storage platform that is accessible from any IP-SAN. Disk-based backup via IP-SAN requires both an iSCSI target such as Storage Builder and an iSCSI initiator. An iSCSI initiator could be compared to a traditional hard drive controller (SCSI), while an iSCSI target could be considered the enclosure for the hard drives and the iSCSI nodes are the hard drives. Basically, an iSCSI initiator uses the iSCSI protocol to communicate with an iSCSI target just as a traditional hard drive controller uses SCSI to communicate with SCSI drives. Figure 1 shows the comparison between traditional disk-based backups and disk-based backups over IP.

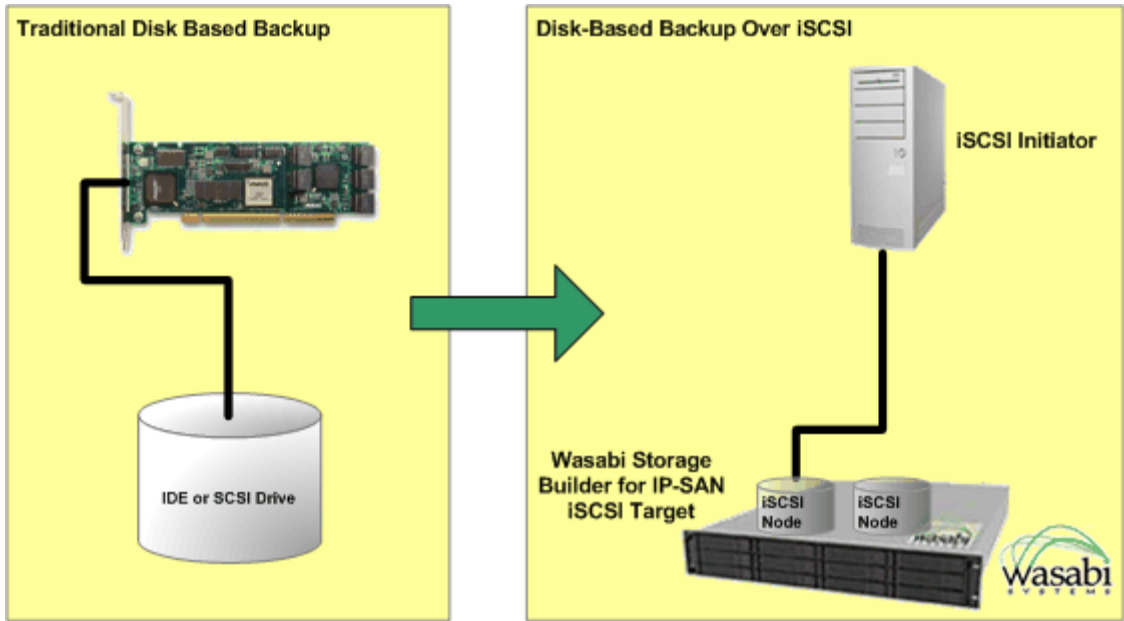


Figure 1: Comparison of Disk-Based Backup to Disk-Based Backup over IP

Even though disk-based backups over IP involve the same fundamental process as traditional disk-based backups, disk-based backups over iSCSI have many additional benefits. Some benefits of using Storage Builder with Symantec’s Backup Exec include:

Exceptional Scalability

Additional Storage Builder iSCSI targets can be added to the network at anytime without having to reboot a network or server.

Centralized Management

From beginning to end, a Storage Builder iSCSI target can be managed through a single web browser.

Centralized Storage

A Storage Builder iSCSI target provides centralized and off-site storage over traditional IP networks.

Storage Builder provides exceptional scalability for multiple operating systems over traditional Gigabit Ethernet. When additional storage is required that exceeds the physical limitations of an existing iSCSI target, additional iSCSI targets can be quickly added to the network. Once the additional iSCSI targets are brought online, the iSCSI initiators can be configured to use the additional iSCSI disk-based storage without having to take the initiators offline for upgrades. Scalability is vital to any business-critical environment and is a key feature of the Storage Builder solution.

A Storage Builder iSCSI target can be completely managed from a single web browser. From creation of the RAID array to provisioning of an iSCSI node for use with an initiator, everything can be managed from a central location. With Storage Builder, a two Terabyte (2048 Gigabytes) iSCSI node can be provisioned and available for use in less than 10 minutes. This includes the time to boot the iSCSI target, provision the RAID array, create access credentials, initialize nodes and connect the initiator into the target.

With Storage Builder, a two Terabyte iSCSI node can be provisioned and available for use in less than 10 minutes.

Data can be backed up from Solaris, BSD, Linux, Macintosh, and Windows based systems to a single Storage Builder iSCSI target. Any storage server that has an iSCSI initiator installed can connect into the iSCSI target over traditional Gigabit Ethernet. Storage Builder supports creating multiple iSCSI nodes with different file systems so that data from machines running different operating systems can be backed up to the same iSCSI target. This results in fewer dedicated back up machines and therefore lower acquisition and maintenance costs.

In addition, Storage Builder allows simultaneous read and write access from multiple machines so that all backups can be done within the same time frame. Once a node is provisioned on the iSCSI target, the storage server can connect into the iSCSI nodes and create a file system for the native operating system. In combination with a disaster recovery plan, a Storage Builder iSCSI target can be placed within any IP-based network. For instance, one iSCSI target could be within the same building, while another iSCSI target is stored at a remote facility for disaster recovery. Both of the iSCSI targets would be visible to the iSCSI initiators as hard drives. Having remotely accessible storage can provide additional time savings by automating off-site backups without the need to transport tapes. With traditional disk-based backups, this is not an option. Figure 2 demonstrates the flexibility of using multiple operating systems on a LAN and multiple iSCSI targets within a SAN in order to provide storage for multiple storage server platforms.

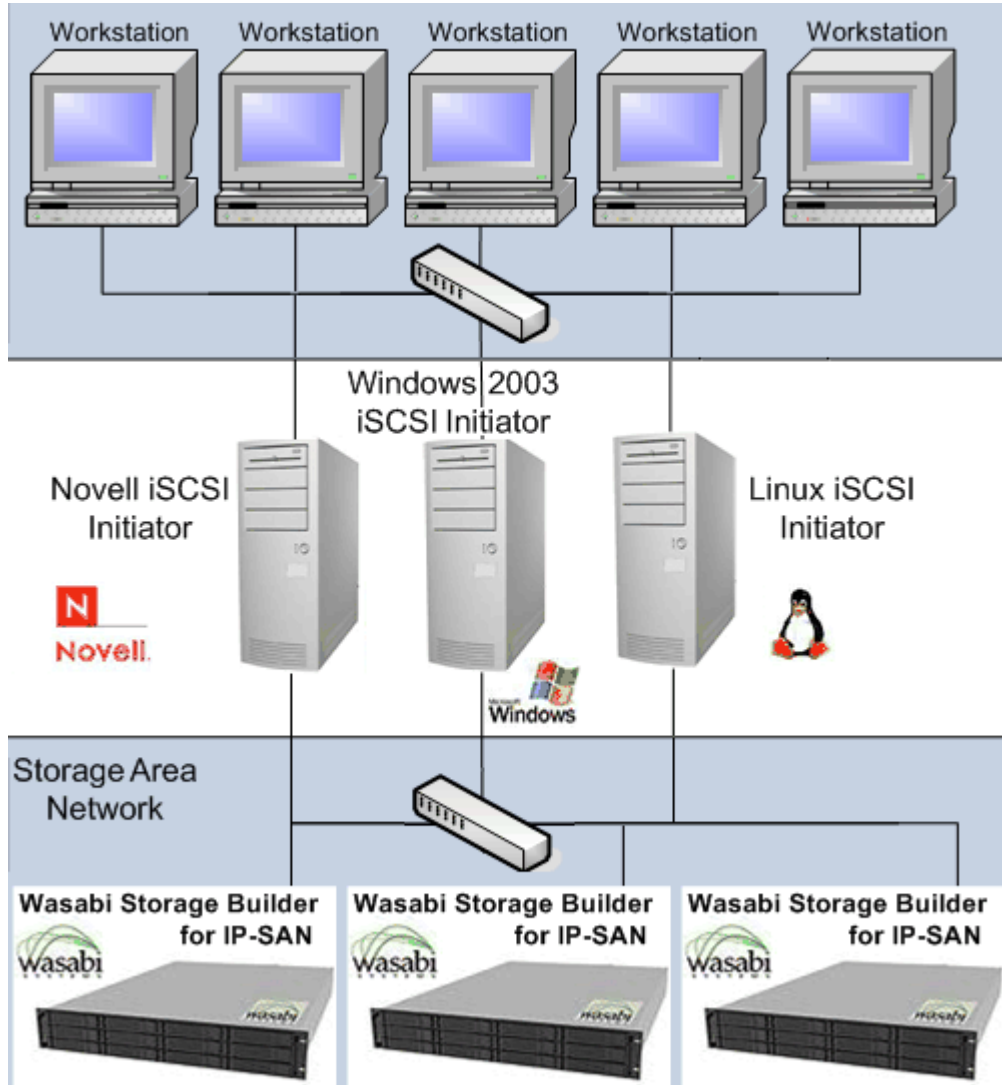


Figure 2: Conceptual LAN and SAN Usage Model over Gigabit Ethernet

Wasabi Storage Builder for IP-SAN provides the ideal solution for any iSCSI disk-based backup solution for small-to-medium businesses (SMBs). Next, we will review the prerequisites to implementing Storage Builder and Backup Exec in a typical SMB environment.

Prerequisites

Before configuring Backup Exec to work with Storage Builder, complete the following four steps:

- Develop a comprehensive backup strategy that meets your specific requirements,
- Install and configure Windows 2003 server,
- Install and configure Storage Builder iSCSI Target, and finally,
- Install the Microsoft iSCSI Initiator v2.0 on the Windows 2003 server.

This document focuses on configuring Backup Exec to work with Storage Builder as an iSCSI disk-based backup solution. Further information on Storage Builder for IP-SAN can be found in the Storage Builder for IP-SAN User's Manual and Storage Builder for IP-SAN Quick Start Guide, available in the Downloads section at:

<http://support.wasabisystems.com>

Develop a Backup Strategy

Great care should be taken to implement a backup strategy that meets your organization's needs. There are many things to consider including backup frequency, size, and types. There are many books and online references to assist with creating an effective backup strategy.

Install and Configure Windows 2003

Next, Microsoft Windows 2003 must be installed on a compatible platform. Be sure to also install Service Pack 1 (SP1). We are using the latest service pack as of February 1, 2006, as available from the Microsoft Windows Update service. The details of our example configuration are shown in Table 2.

<i>Detail</i>	<i>Description</i>
Operating System	Windows 2003 Advanced Server
Processor	Single 2.4 Ghz Xeon
Hard Drive	Western Digital 80 GB IDE Drive
IP Address	192.168.7.12

Table 2: Windows 2003 Server Configuration

Install and Configure the Storage Builder iSCSI Target

After installing Windows 2003 Server, we will setup and configure the Storage Builder iSCSI target. Installation and configuration details for Storage Builder are included in the *Wasabi Storage Builder for IP-SAN User's Manual* and the *Wasabi Storage Builder for IP-SAN Quick Start Guide*. For this application note, the configuration of the Storage Builder iSCSI target is shown in Table 3.

Setting	Value
Number of Hard Drives	4
Size of the Hard Drives	250 GB
Total Raw Storage	Approximately 720 GB
RAID Controller	3ware 9500-4
RAID Configuration	RAID 5
Volume Unit Size	Approximately 720 GB
Volume Group Size	Approximately 720 GB
Node Size	Approximately 720 GB
iSCSI Credentials	CHAP
Portal	1 Portal on Ethernet Port 0
IP Address of Ethernet Port 0	192.168.7.23

Table 3: Sample Storage Builder iSCSI Target Configuration

Install the Microsoft iSCSI Initiator v2.0

Finally, we download and install the Microsoft iSCSI Initiator v2.0 (or current version) onto the server. The latest Microsoft iSCSI Initiator can be downloaded from Microsoft at:

<http://www.microsoft.com/downloads/>

After installing the iSCSI Initiator, we connect the Windows 2003 Initiator to the Storage Builder iSCSI node. Figure 3 shows a simple network diagram of the Storage Builder iSCSI target and Windows 2003 Server.

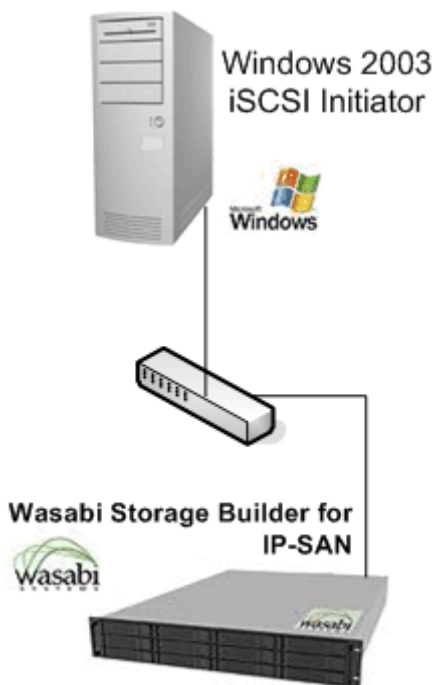


Figure 3: SAN Disk-Based iSCSI Backup with Symantec Backup Exec

Figure 4 shows the configuration screen of the Windows node on the Wasabi Storage Builder iSCSI target. Note that the iSCSI credentials were set to CHAP in this configuration. We highly recommend implementing CHAP authentication for optimal data security. This feature is turned on in our example configuration. Additional information about CHAP authentication can be referenced in the *Wasabi Storage Builder for IP-SAN User's Manual*.

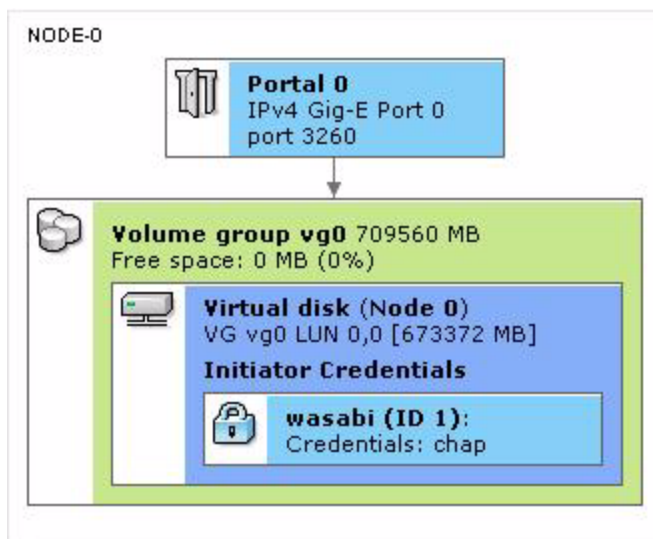


Figure 4: iSCSI Node Configuration

Using Symantec Backup Exec

This section describes the configuration, backup, and restore processes required when using disk-based backup with Wasabi Storage Builder iSCSI Node and Backup Exec on the Windows 2003 Initiator. All prerequisites must be completed before continuing.

Configuring the iSCSI Node for Storing Data

First, format the iSCSI node to allow Windows 2003 Server to create a file system on the Wasabi Storage Builder iSCSI target. Before proceeding, make sure that the Windows 2003 Server is connected into the target with the Microsoft iSCSI version 2.0 Initiator.

Next, run Computer Management:

Start→Control Panel→Administrative Tools→Computer Management

in order to format the iSCSI node. Within Computer Management, we click on the plus sign next to Storage and select **Disk Management** as shown in Figure 5.



Figure 5: Disk Management

If this is the first time the drive has been initialized, after clicking Dick Management, an initialization wizard will appear. We will navigate through each of the options while leaving the default settings. After clicking the **Finish** button the hard drive will be initialized. The iSCSI node settings should look similar to the image shown in Figure 6.



Figure 6: Basic Initialized Disk

In this example, we use the entire 657.58GB iSCSI node for our backup. The size of the iSCSI node will vary based on the size of the node allocated on to the iSCSI node.

Next, format the iSCSI node in order to store our backups to disk. To format the newly initialized disk, right click on the newly initialized disk and select **New Partition...** shown circled in red in Figure 7.



Figure 7: Creating a New Partition

The **New Partition Wizard** will appear. Step through the wizard and create a Primary 657.58GB NTFS Drive E partition, and label the partition “iSCSI Backup.” The drive letter of the partition and the disk label chosen for the partition can vary based on the Windows 2003 system configuration. We opt not to do a Quick Format by leaving that option unchecked. When the wizard completes, the iSCSI node will be fully formatted. A full format is important to verifying the integrity of our iSCSI node as a new NTFS disk.

After clicking **Finish** on the **New Partition Wizard**, the disk begins to format. The time it takes to format the iSCSI partition depends on a number of factors including network speed between the Windows 2003 Server and the Initiator and the size of the iSCSI node. Figure 8 shows an example screenshot of an iSCSI node being formatted.

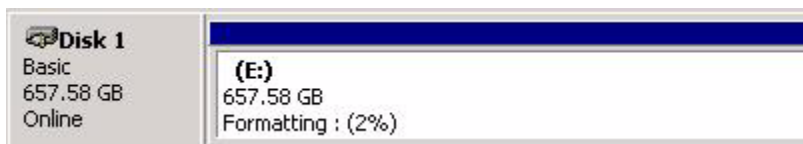


Figure 8: Formatting the Initialized iSCSI Node

You must wait for the iSCSI node to finish formatting before the node can be used for backups. After formatting the iSCSI node, configure Backup Exec to use the newly formatted iSCSI node to store your backups.

Backing Up to an iSCSI Node

Before continuing, make sure that the iSCSI node has finished formatting. Figure 9 shows an example iSCSI node that has finished being formatted and is ready for disk-based backup using TBU.



Figure 9: Formatted iSCSI Node

Note that in Figure 9 the Basic disk is **Online**, **Healthy**, and the drive letter E has been assigned to the iSCSI node.

Step 1: Configuring Backup Exec for the First Time

Launch Backup Exec by selecting:

Start→**All Programs**→**Symantec Backup Exec 10d for Windows Servers**.

Click **Next** to start the wizard. If this is your first time running Backup Exec on this system, a **First Time Startup Wizard** will appear as shown in Figure 10. Symantec requires configuring Backup Exec through this wizard before using Backup Exec for the first time. If you have already executed the First Time Startup Wizard, each of these wizards can be executed manually under the Symantec Backup Exec main menu under **Tools**→**Wizards**.



Figure 10: Backup Exec Wizard

Follow these steps, starting in the **First Time Startup Wizard** window, shown in Figure 10.

1. Click **Next** to continue.
The **Media Management with Media Sets** window appears
2. Click **Next** to continue.
The **Default Media Set Properties** window appears, as shown in Figure 11.
3. Select the radio button for **Yes, I want to edit this set or create new media sets that will allow Backup Exec to automatically recycle some media for my backups**, and click **Next** to continue.

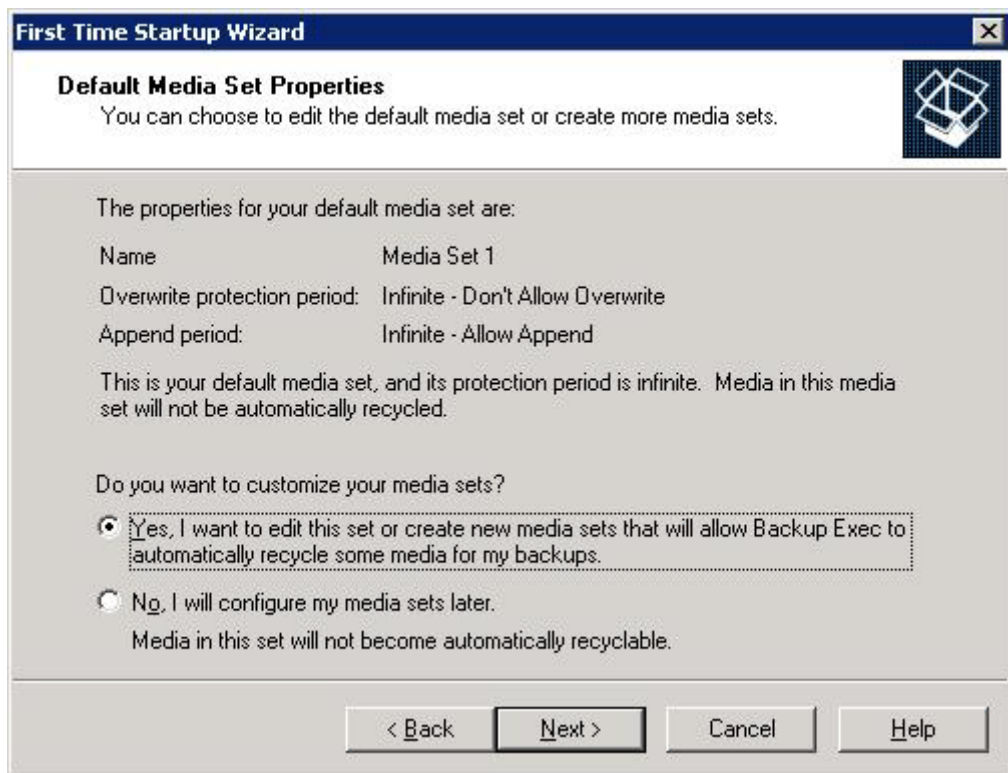


Figure 11: Default Media Set Properties

After following the steps above, the **First Time Startup Wizard** will close and the **Media Set Wizard** will automatically launch as shown in Figure 12.



Figure 12: Media Set Wizard

1. Click **Next** to continue.
The **Create or Edit a Media Set** dialog box appears.
2. Accept the default setting, **Create a new media set**, and click **Next** to continue.
The **Name the Media Set** dialog appears.
3. Enter a name for this new media set. For this example, we recommend “iSCSI Backup1.” Click **Next** to continue.
The **Set the Overwrite Protection Period** dialog box appears.
4. Accept the default setting, **Infinite - Don’t Allow Overwrite**, and click **Next** to continue.
The **Set the Append Period** dialog appears.
5. Accept the default setting, **Infinite – Allow Append**, and click **Next** to continue.
The **Media Set Summary** window appears.
6. Review the settings, and click **Next** to continue.
The final dialog box appears.

7. You have successfully completed the Media Set Wizard. Leave the checkbox for **Add or edit another media set after click Finish** unchecked and click **Finish**.

Next, the **First Time Startup Wizard** will reappear as shown in Figure 13.

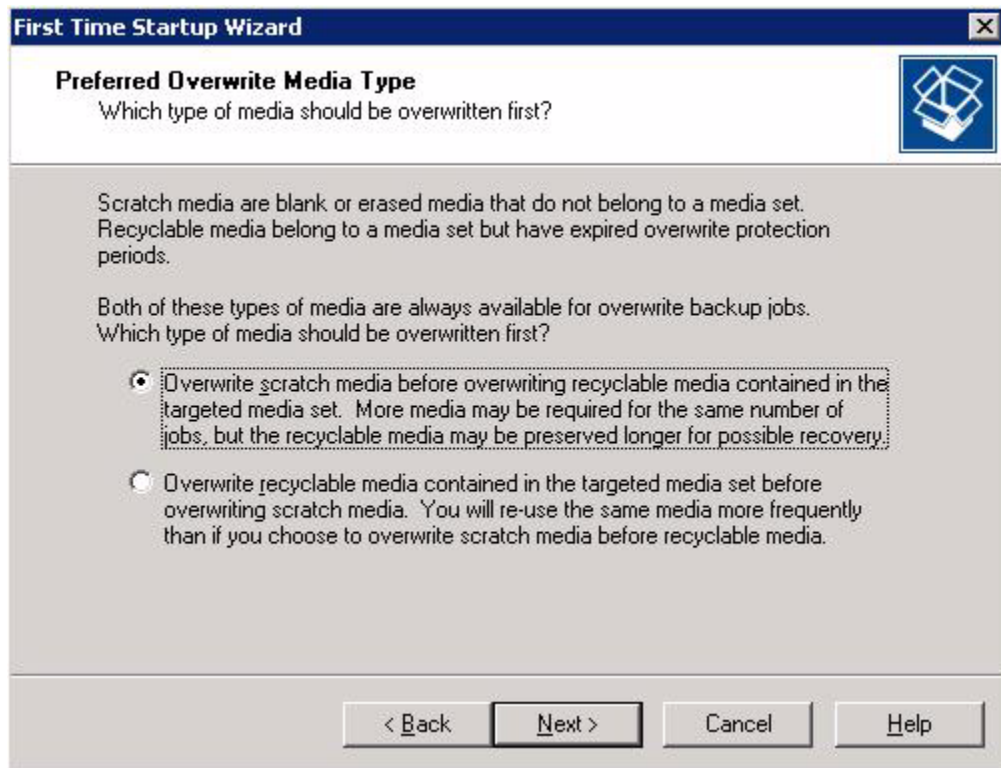


Figure 13: First Time Startup Wizard Options

The **First Time Startup Wizard** displays the Preferred Overwrite Media Type.

1. Accept the default radio button setting, as shown in Figure 13, and click **Next**. The **Overwrite Protection Level** dialog box appears.
2. Accept the default radio button setting: **Partial – Prevents allocated media from being overwritten. Imported media can be overwritten.**
3. Leave the checkbox checked for **Prompt before overwriting imported media**.
4. Click **Finish**.

Next, the **Device Configuration Wizard** will reappear as shown in Figure 14.



Figure 14: Device Configuration Wizard

1. To begin, click **Next**.
The **Detected Hardware** dialog box appears.
2. Leave the **Backup devices** field blank and click **Next**.
The **Detected Backup-to-Disk Folders** screen appears.
3. The screen displays any Back-to-Disk Folders that were found.
 - a. Click **Add Backup-to-Disk Folder**.
The **New Backup-to-Disk Folder** screen appears.
 - b. Enter a name for the new folder. For example, “Backup-to-Disk Folder 1.”
 - c. Enter a path name. For example, E:\
 - d. Click **OK**.
The **Detected Backup-to-Disk Folders** screen reappears.
 - e. Click **Next**. The **Drive Configuration** window appears.
4. In the **Drive Configuration** window, verify that your drive configuration is correct and click **Next**.
5. Device configuration is complete. Click **Finish** to close this wizard.

Last, the **Logon Account Wizard** will reappear as shown in Figure 15.



Figure 15: Logon Account Wizard

1. You can click **Next** to continue or **Cancel** to exit the wizard. Click **Next**. The **Setup Up your Default Logon Account** screen appears.
2. Click on **Select an existing logon account**.
3. Select the logon account from the list displayed. In this example, we will choose the **System Logon Account (Administrator)**. Click **Next**.
4. Leave unchecked **Add or edit another logon account after clicking Finish**. Your changes will be applied after you click **Finish**.

Backup Exec is now configured to use the Storage Builder iSCSI target. For more information on configuring Backup Exec, please reference to the *Symantec Backup Exec Continuous Protection Server™ 10d Administrator's Guide* available from:

<http://support.veritas.com>

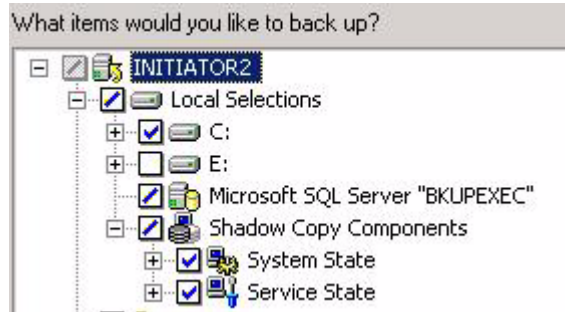
Step 2: Configuring NT Backup for Backup

Now that the Storage Builder iSCSI target and Back Exec are configured, the following section describes how to manually execute a backup for the first time. To start the Backup Exec Backup Wizard, click **Tools→Wizards→Backup Wizard...** from the Symantec Backup Exec main menu. Figure 16 shows the first window of the Backup Wizard. The options you choose for the Backup Wizard should match that of your backup strategy. In this example, we will run a backup that simulates a full backup of the entire Windows 2003 server.



Figure 16: Backup Wizard

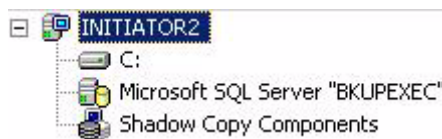
1. To begin creating a backup job, click **Next**.
2. Which files and directories do you want to backup? Selecting the options shown below and click **Next**.



3. Select Volume Credentials. For each resource, select an appropriate logon account to use for this backup. Select the Resource and click the **Test** button to the right. If successful, each resource will look as shown in the figure below. Click **Next**.

Resource	Logon Account	Test Results
INITIATOR2	System Logon Acco...	Successful
C:		Successful
Microsoft ...		Successful
Shadow C...		Successful

4. Select Volume Order. You can determine the order that the volume will be backed up. Accept the default settings shown below and click **Next**.



5. Select a backup name. What would you like to call this backup job? The default is "Backup 0000xx," where 0000xx is a sequential number. Accept the default or enter a different name. Click **Next**.
6. Select backup device and media.
 - a. Which device would you like to use to back up your data?. The default is "All Devices."
 - b. Select the media set you want to use to back up your data. The default is "Media Set 1." Click **Next**.

7. Select a backup overwrite method.
 - a. When this backup job begins would you like Backup Exec to append to media or overwrite available media? The default is “Append to media, overwrite if no appendable media is available.”
 - b. If overwriting media, what name would you like to give to the media? The default is “Leave this as the default value or provide some other description to identify this media.” Click **Next**.
8. Select backup options.
 - a. Which backup method would you like to use to back up files? The default is “Full – Back Up Files – Reset Archive Bit.”
 - b. Would you like to verify that the selected files were backed up successfully after the backup job has completed? The default is “Yes, verify after backup.” Click **Next**.
9. Select SQL options.
 - a. Which backup method would you like to use to back up SQL databases?. The default is “Full – Back up entire database or filegroup.”
 - b. Do a consistency check before backup? The default is “None.”
 - c. Do a consistency check after backup? The default is “None.”After making your selections, click **Next**.
10. To complete the Backup Wizard, select a time to run the backup. The default is “Yes, run the job now.” Click **Finish**.

After finishing the steps above, a window similar to the one shown in Figure 17 will appear.



Figure 17: Job Submitted Notification

Click **OK** and the back up will start. To monitor the backup process, click the **Job Monitor** tab at the top. Once the backup job is completed, the **Job Monitor** window will look similar to the one shown in Figure 18.

Current Jobs - 0 Items					
State	Job Name	Device Name	Job Type	Job Status	Pri
None					


Job History - 1 Item				
Job Name	Device Name	Job Type	Job Status	Percent ...
 Backup 00002	Backup-to-Disk Folder 1	Backup	Successful	100%

Figure 18: Job Monitor: First Completed Backup

This concludes the overview of backing up to an iSCSI target using Symantec Backup Exec. For more information on configuring Backup Exec, please reference to the *Symantec Backup Exec Continuous Protection Server™ 10d Administrator's Guide* available from:

<http://support.veritas.com>

The next step with conducting a backup routine is to restore backed up data from the Storage Builder iSCSI target.

Step #3: Restoring Data

Before being able to restore data from the Storage Builder iSCSI target, the following prerequisites must be met:

- The iSCSI initiator is connected into the target and the status is OK.
- A Backup Exec backup has been successfully completed to an iSCSI node on the Storage Builder iSCSI target as outlined within Section 4.2.2.

Assuming the prerequisites are met, the following section outlines the process for restoring data from a Storage Builder iSCSI target. To start the Restore Wizard, click **Tools→Wizards→Restore Wizard...** from the Symantec Backup Exec main menu.

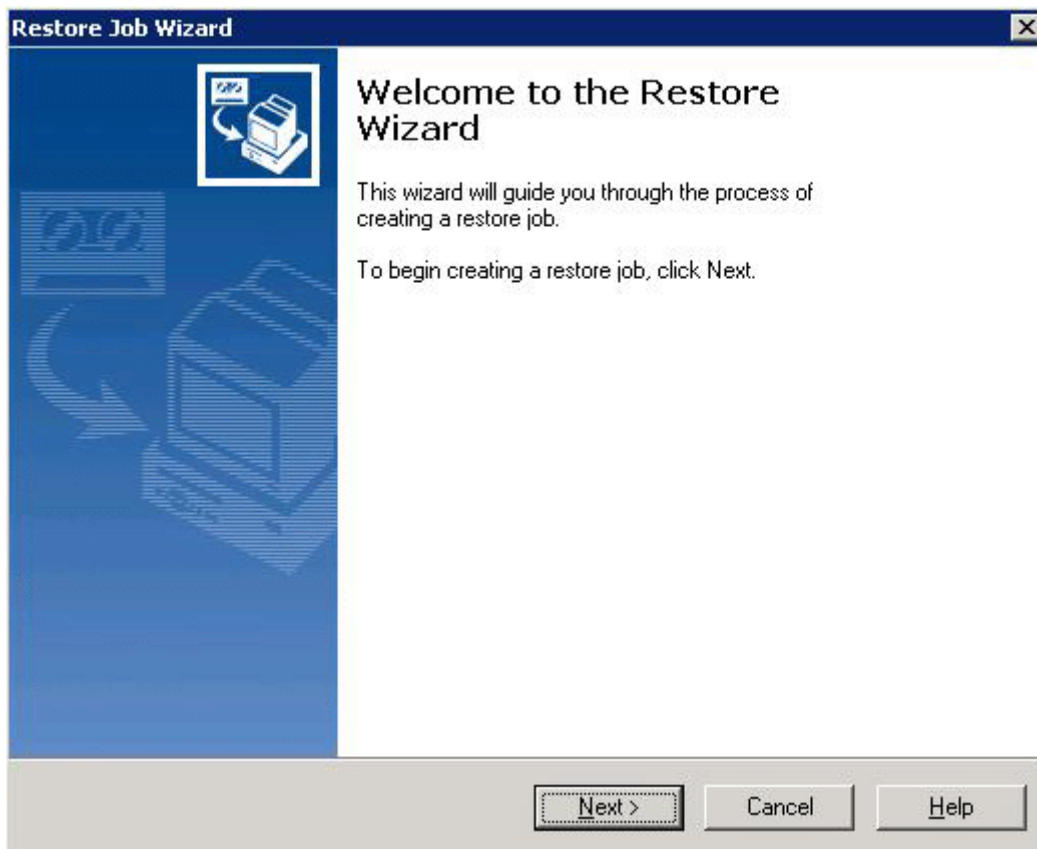


Figure 19: Restore Wizard

1. To begin creating a restore job, click **Next**.
2. Select the files and folders you wish to restore. In this example, we choose the **Intel** folder from the most recent backup as shown below.



3. Select the logon account to use for restoring data to each filesystem. Select each resource that needs to be restored and click **Test**. Then click **Next**.

4. Select a name for the restore job. The default is “Restore 000xx,” where 000xx is a sequential number. Otherwise, you can enter the name of your choice. When finished, click **Next**.
5. Select a data source. Which device or device pool would you like to restore from? The default is “All Devices.” When finished, click **Next**.
6. If a file being restored already exists on disk, select existing file options. This option depends on if you would like to restore a file that was previously deleted. For this option, we will choose to Overwrite the file on disk. Click **Next**.
7. You have completed the Restore Wizard. Do you want to run this restore job now? The default is “Yes, run the job now.” Click **Finish**.

As Figure 20 indicates, the restore job process can be tracked within the Job Monitor window just as after running a backup.



Figure 20: Restore Notice to View the Job Monitor

Once the restore job is completed, the Job Monitor window will look similar to the one shown in Figure 21.

Current Jobs - 0 Items					
State	Job Name	Device Name	Job Type	Job Status	Pr
None					

Job History - 2 Items				
Job Name	Device Name	Job Type	Job Status	Percent ...
Restore 00002	Backup-to-Disk Folder 1	Restore	Successful	100%
Backup 00002	Backup-to-Disk Folder 1	Backup	Successful	100%

Figure 21: Job Monitor After Restore

This concludes the overview for restoring data from a Storage Builder iSCSI target using Backup Exec. For more information on configuring Backup Exec, please refer to the *Symantec Backup Exec Continuous Protection Server™ 10d Administrator's Guide* available at: <http://support.veritas.com>

Conclusion

Wasabi Storage Builder for IP-SAN provides an easily configurable and reliable disk-based backup solution for nearly any environment. In combination with Symantec Backup Exec, a fast and easy to manage disk-based backup can be setup with very little effort. For more information about Wasabi Storage Builder for IP-SAN, please visit:

<http://www.wasabisystems.com>

Definitions

CHAP

Acronym for Challenge Handshake Authentication Protocol. An access control protocol used for user authentication that does not require sending a password over the network in unencrypted form.

CIFS

An Internet file system protocol based on Microsoft's Server Message Block (SMB). CIFS runs on top of TCP/IP and uses the Internet's Domain Name Service (DNS).

Initiator

Also referred to as an iSCSI Initiator.

IP

Acronym for the Internet Protocol.

iSCSI

Acronym for Internet SCSI. A transport protocol for the SCSI command protocol that uses TCP/IP.

iSCSI Credential

An authentication method and set of credentials used by an iSCSI initiator to log into an iSCSI node.

iSCSI Initiator

A SCSI initiator that implements the iSCSI transport protocol.

iSCSI Node

A target device instance that is presented by an iSCSI target to an iSCSI initiator.

iSCSI Target

A SCSI target that implements the iSCSI transport protocol.

NAS

Acronym for Network-Attached Storage. A server that is dedicated exclusively to file sharing.

NFS

Acronym for Network File System. A protocol developed by Sun Microsystems, and defined in RFC 1094, which allows a computer to access files over a network as if they were on its local disks. NFS is implemented using a connectionless protocol (UDP) in order to make it stateless.

RAID

Acronym for Redundant Array of Independent Disks. A family of methods that

employ two or more disk drives in combination for fault tolerance and performance.

RAID 1

A RAID method that uses two disk drives to store two copies of each block of data. This is the least space-efficient RAID level, but provides the best performance in the event of a disk failure. Also known as RAID 1 or mirroring. A variant of RAID level 1, known as N-way mirroring, can use more than two disk drives to store additional copies of the data.

RAID 5 – A RAID method that uses three or more disk drives and stripes data and stores redundancy (parity) information across all disks; the location of the parity blocks rotate for each stripe (row). A RAID level 5 array has the capacity of n-1 disks. In the event of a disk failure, the redundancy information for a given stripe is used to reconstruct the missing data blocks.

SCSI

Acronym for Small Computer System Interface. A standard architecture and command protocol that enables computer systems and peripherals to communicate with each other. SCSI also refers to a parallel interface standard used to connect computer systems and peripherals together.

SAN

Acronym for Storage Area Network. A high-speed network of shared storage devices. A storage device is a machine that contains storage media and whose sole purpose is the storage and retrieval of data, such as a disk array.

Target

Also referred to as an iSCSI target.

References

Symantec Backup Exec Continuous Protection Server™ 10d Administrator's Guide
(English).

<http://support.veritas.com>. 10/07/2005

Disk Based Backup: All Hype or the Best Protection for your Data?

Shinder, Debra Littlejohn. WindowsSecurity.com.

<http://www.windowsecurity.com/articles/Disk-Based-Backup.html>

The Free On-line Dictionary of Computing.

Howe, Denis. 1993-2005

<http://dictionary.reference.com/search?q=00-database-info&db=foldoc>

