NETGEAR®

ReadyRECOVER Software

User Manual

July 2014
202-11429-02

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

After installing your device, locate the serial number on the label of your product and use it to register your product at *https://my.netgear.com*. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website. For product updates and web support, visit *http://support.netgear.com*.

Phone (US & Canada only): 1-888-NETGEAR.

Phone (Other Countries): Check the list of phone numbers at *http://support.netgear.com/general/contact/default.aspx*.

Compliance

For regulatory compliance information, visit *http://www.netgear.com/about/regulatory*.

See the regulatory compliance document before connecting the power supply.

Trademarks

Contents

ReadyRECOVER Solution Overview

1

ReadyRECOVER is a complete backup and recovery appliance designed for small and medium-sized businesses. Next-generation file system technology guarantees data integrity, efficient use of storage capacity, and minimal impact to computing resources. With ReadyRECOVER, full backups are instantly created every 15 minutes and can be used independently to quickly and reliably restore files, folders, or systems to any platform, physical or virtual.

Traditional backup solutions create incremental image chains and require regular resource-draining, full backup jobs to maintain data integrity and timely restore points. With ReadyRECOVER, each snapshot is a space-efficient recovery point that never requires image chain management or consolidation. In addition, each snapshot captures the entire target system, the Windows operating system, all services, all applications, all settings, and all data for fast full-system recovery.

ReadyRECOVER is a seamless integration of the ReadyDATA unified storage platform from NETGEAR® and ShadowProtect backup and recovery software from StorageCraft.

The solution has storage-efficient data-protection capabilities that deliver the following benefits:

- **Protection of physical and virtual servers**. These servers include the following:
  - Windows physical servers
  - VMware, Hyper-V, and Xen servers (Windows guest operating systems)
- **Synthetic full backups**. Every backup is represented as a full image (`.vhdx`) and provides quick single-file restoration and hardware-independent full restoration of server operating systems and their applications to any supported platform (physical servers, virtualization platforms).
- **Fifteen-minute recovery points**. Backups can be set to 15-minute intervals, regardless of the total capacity of the server (64 TB maximum per logical drive).
- **Storage efficiency**. The storage consumption of this solution is highly efficient because all data is compressed when it is written and only unique blocks of ongoing backups must be stored on disk. The more backups that are stored, the larger the savings become.
- **WAN efficiency**. For customers replicating backup sets offsite, only incremental block changes are replicated with ReadyDATA replicate.

For more information about the topics covered in this manual, visit the support website at *http://support.netgear.com.*

Install and Configure ReadyDATA

2

If you have not done so already, install and configure the ReadyDATA unified storage platform. This chapter covers the following topics:

- *ReadyDATA Hardware Installation*
- *Determine the IP Address of Your ReadyDATA*
- *Change the Administrator Password*

ReadyDATA Hardware Installation

Information about installing the ReadyDATA 5200 and 516 is found in the following resources:

- *ReadyDATA Hardware Manual* and *ReadyDATA OS Software Manual*.

  These documents are available on the resource CD that came with your product. You can also obtain these manuals by clicking the **?** icon in the ReadyDATA dashboard.

- The support website at *http://support.netgear.com.*

Determine the IP Address of Your ReadyDATA

If you have not discovered your ReadyDATA, connect the unit to your network and make sure that a DHCP server can reach the ReadyDATA. By default, the ReadyDATA is configured to receive an IPv4 IP address from a DHCP server.

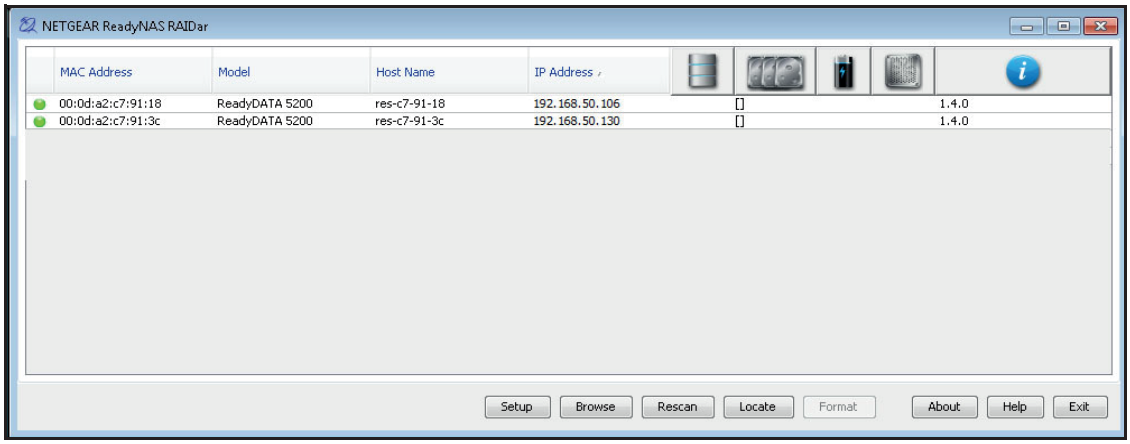
If the ReadyDATA cannot locate a DHCP server, the unit is assigned an IP address through Automatic Private IP Addressing (APIPA). For more information, see “Automatic Private IP Addressing Without a DHCP Server” in the *ReadyDATA OS Software Manual*.

RAIDar is a software application that you use to discover ReadyDATA systems on the network. RAIDar is included on the resource CD that came with your system, which includes versions for Windows, Mac, and Linux operating systems. RAIDar is also available at *www.netgear.com/readydata*.

➢ **To discover the ReadyDATA system and launch the dashboard:**

1. Install the appropriate version of RAIDar on a computer that is connected to the same LAN as the ReadyDATA.
2. Launch the RAIDar utility.

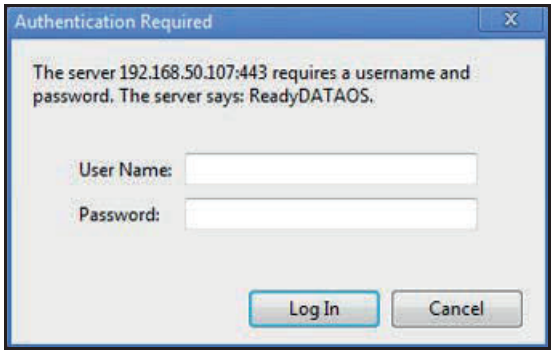
   RAIDar displays a screen that lists the systems on the network and provides details about the status of each system that it discovers.



3. Highlight the ReadyDATA and click the **Setup** button.

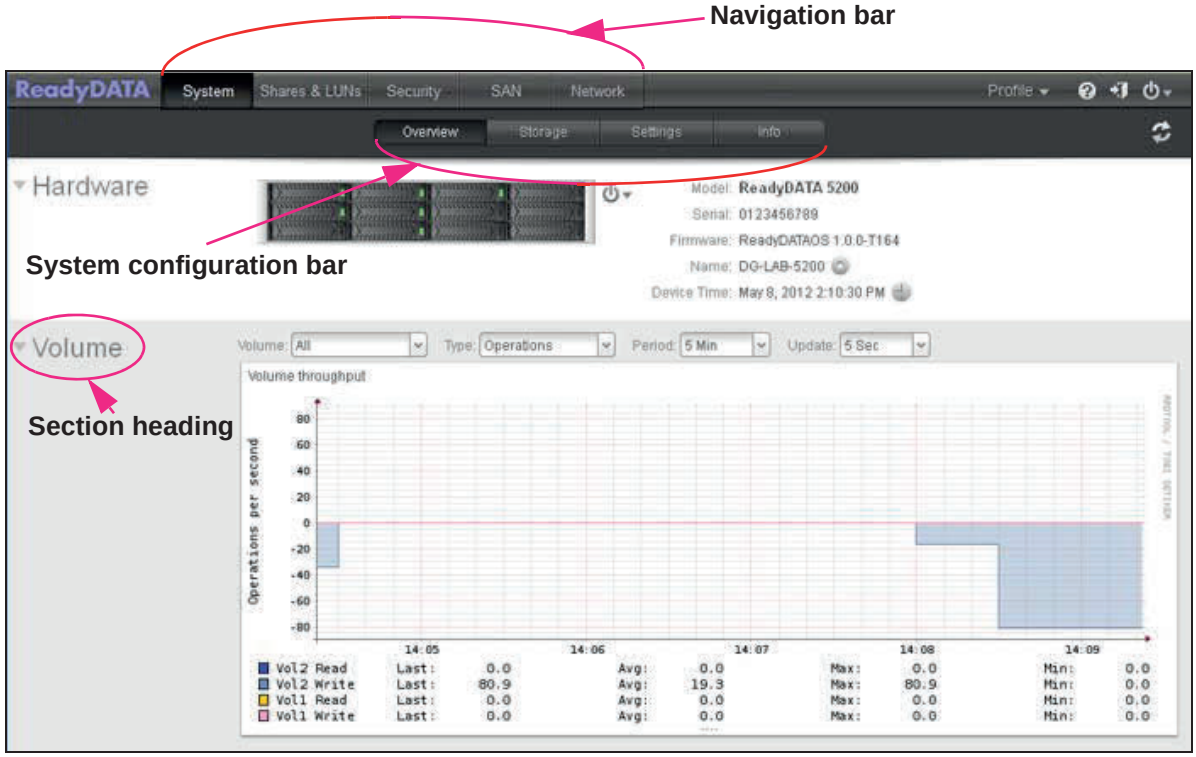
RAIDar opens your default browser and prompts you to log in to the ReadyDATA.

If you are unable to discover your ReadyDATA, see the *ReadyDATA OS Software Manual* for troubleshooting steps.



4. Log in to the ReadyDATA using the default login credentials:
   a. As the default user name, enter **admin** (case-sensitive).
   b. As the default password, enter **password** (case-sensitive).

   The dashboard screen displays.



Change the Administrator Password

Choose an administrator password that is different from the default password and keep it in a safe place. Anyone who obtains this password can change settings or erase data that is stored on the ReadyDATA.

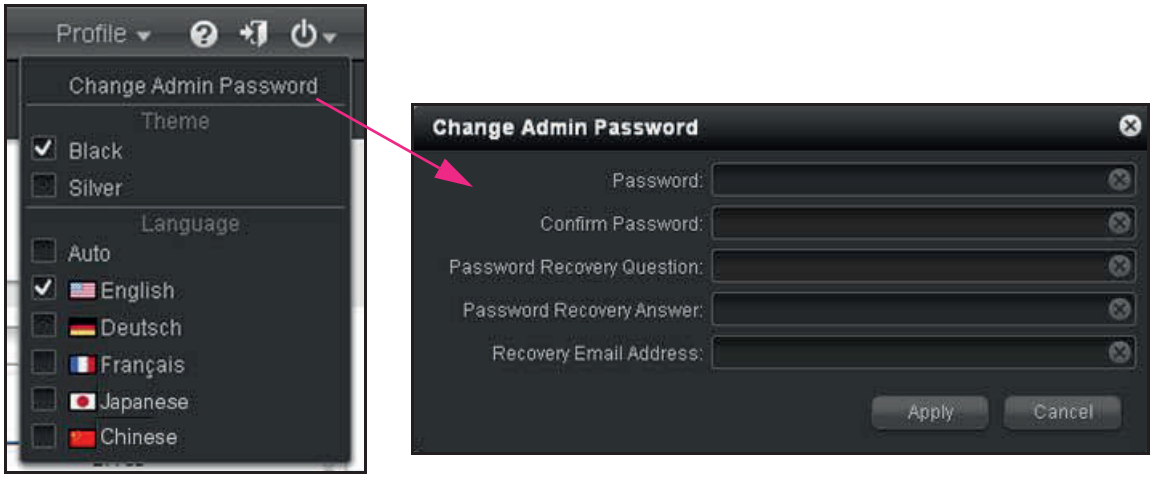
➢ **To change the administrator password:**

1. On the navigation bar at the right, select **Profile**.

   The Profile menu displays (see the following figure).

2. Select **Change Admin Password**.

   The Change Admin Password pop-up screen displays:



3. Click the **Apply** button.

Supported Disks and Initial Startup

The ReadyDATA 5200 supports up to 12 disks. With optional expansion disk arrays that can contain either 12 or 24 disks each, you can increase the total number of supported disks to 60. The following figure shows a ReadyDATA 5200 with an optional expansion disk array that supports 24 disks and another array that supports 12 disks.

The ReadyDATA 516 supports up to 6 disks and does not support expansion disk arrays.

For information about additional information about supported disk types, see the ReadyDATA OS Software Manual for your system.

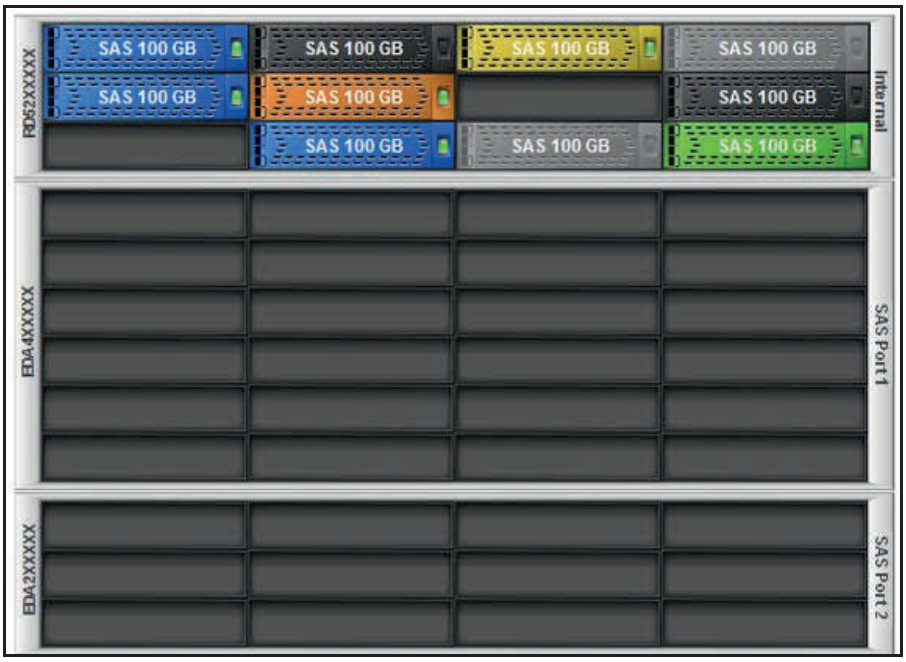


Figure 1. ReadyDATA 5200 with optional disk expansion arrays as displayed on Dashboard

Create a Volume and Select the RAID Level

Note: ReadyRECOVER requires a dedicated volume. Other workloads, such as LUNs for virtualization or file server, must be serviced by separate volumes.

For small ReadyRECOVER volumes with six disks or less, RAID 5 or RAID 6 can be used. Larger ReadyRECOVER volumes with more than six disks should use RAID 50 or RAID 60.

Table 1. RAID level and required number of disks

RAID Level	Number of Required Disks	Redundancy
RAID 0	1 or more	None
RAID 1	2 only (more disks are not supported in RAID 1)	Supported
RAID 5	3 or more	Supported for one disk
RAID 6	4 or more	Supported for two disks
RAID 10	4 or more, but an even number	Supported for all disks

Table 1. RAID level and required number of disks (continued)

RAID Level	Number of Required Disks	Redundancy
RAID 50	6 or more, but an even number	Supported for one disk per RAID 5 set
RAID 60	8 or more, but an even number	Supported for two disks per RAID 6 set

To create a volume and select the RAID level:

1. On the ReadyDATA screen, select **System > Storage**.

   The Storage screen displays.

   The following figure shows one optional expansion disk array and one volume. A new system does not have any volumes.

2. In the enclosure, click the disks that you want to select as members of the volume.

   You can select disks with a black color coding only. If you have an expansion disk array, you can select disks from both the ReadyRECOVER Software and the expansion disk array.

   The selected disks are highlighted and all volume buttons become available, including the **New Volume button** under the enclosure:

3. Below the enclosure, click **New Volume** button.

   The New Volume pop-up screen displays:

   The RAID levels that are displayed depend on the number of disks that you selected.

   Note: For ReadyRECOVER, RAID 50 or RAID 60 should be used with disk groups that are no larger than nine disks.

4. Configure the following settings:
   - **Name**. Enter a name for the volume. The volume name must begin with a letter, and can contain only alphanumeric characters, underscores (_), hyphens (-), periods (.), and colons (:). The volume names *mirror*, *logs*, and *spare* are reserved and cannot be used, as are all names that begin with the *c[0–9]* pattern. However, you can use names that begin with the *C[a–z0–9]* or *c[a–z]* pattern.
   - **RAID**. From the drop-down list, select the RAID level. The RAID level that you can select depends on the number of disks that you selected in *Step 2*. For more information, see *Table 1* on page 9.

If you select RAID 5 and six or more disks (or RAID 6 and eight or more disks), a screen opens letting you select RAID 5+0 instead of RAID 5 (or RAID 6+0 instead of RAID 6).

5. Click the **Create** button.

   The volume is created.

Install and Configure ShadowProtect Agents

3

To use ReadyRECOVER with your NETGEAR ReadyDATA unified storage platform, install and configure the ShadowProtect backup and recovery software from StorageCraft. This chapter covers the following topics:

Supported Platforms

ShadowProtect for ReadyRECOVERY runs on the following operation systems:

- Desktop and mobile
  - Windows XP
  - Windows Vista
  - Windows 7
  - Windows 8.x
- Server
  - Windows Server 2003
  - Windows Server 2008 & 2008 R2
  - Windows Server 2012 & 2012 R2

Note: ReFS is not supported at this time.

Install ShadowProtect

To install ShadowProtect, you need the following:

- ShadowProtect install file (*www.storagecraft.com/downloads/software-updates*)
- ShadowProtect license key (obtained through your sales representative, NETGEAR, or StorageCraft)

Note: If you are using this product under an MSP model, obtain your key through your MSP portal login.

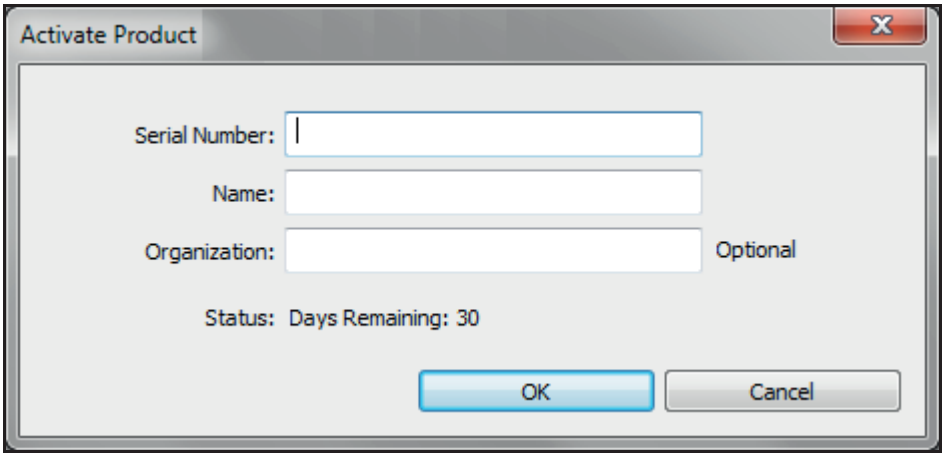
➢ **To install ShadowProtect:**

1. Place ShadowProtect software on the Windows server or client that you want to back up.
2. Run the installer and follow the wizard.
3. Accept the default settings.
4. When the installer finishes, reboot the server or client.

➢ **To activate ShadowProtect:**

1. Obtain a ShadowProtect license key.
2. Open the ShadowProtect Console.

3. Select **Help > Product Activation** from the menu.
4. Complete the Activation screen.



5. Click the **Activate** button.

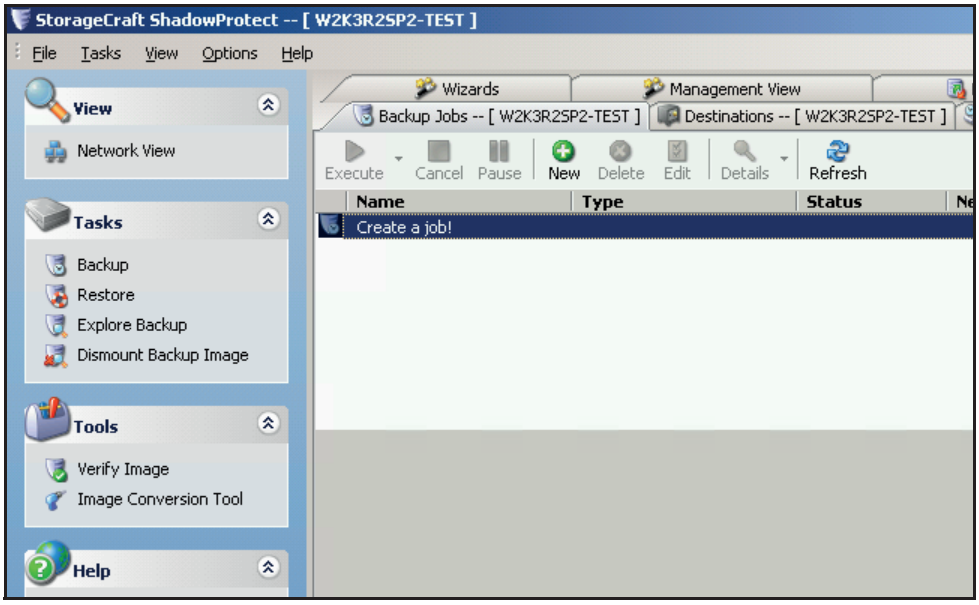
Configure Your First Backup Job

After a reboot, ShadowProtect drivers are engaged and ready to start protecting your data. You need the following information to set up successful backups:

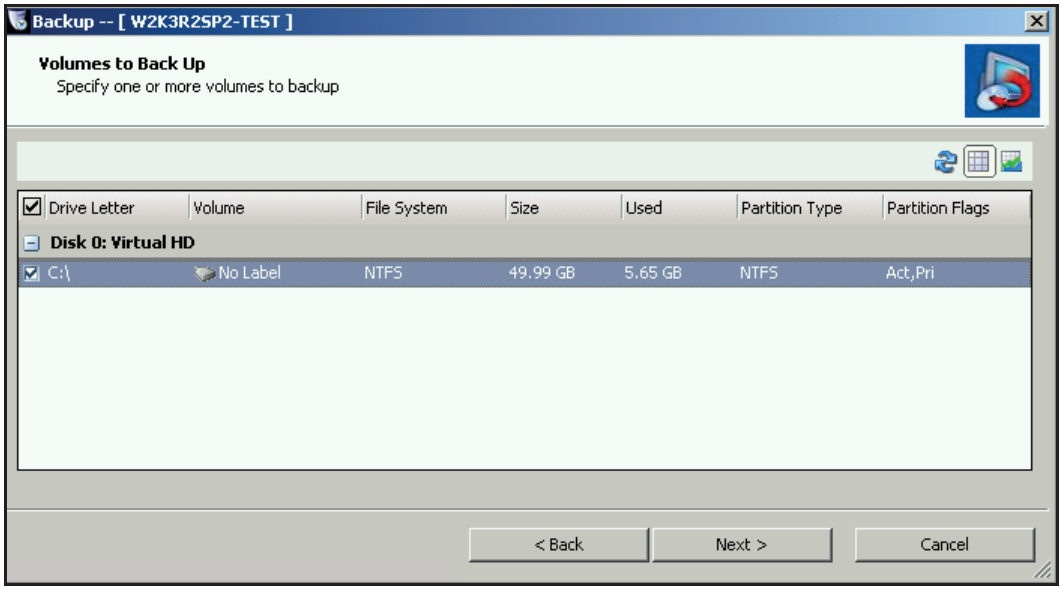
- IP address of the ReadyDATA appliance
- Administrative credentials of the ReadyDATA appliance

➢ **To set up your backup job:**

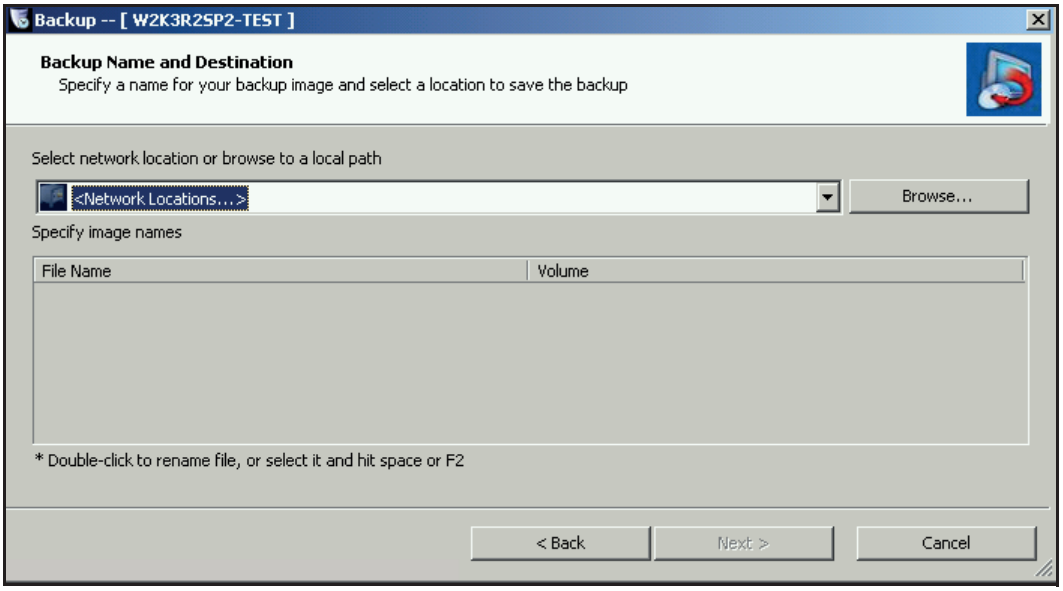
1. Launch the backup wizard.
2. From within ShadowProtect interface, select **Backup** from the tasks on the left-hand menu.



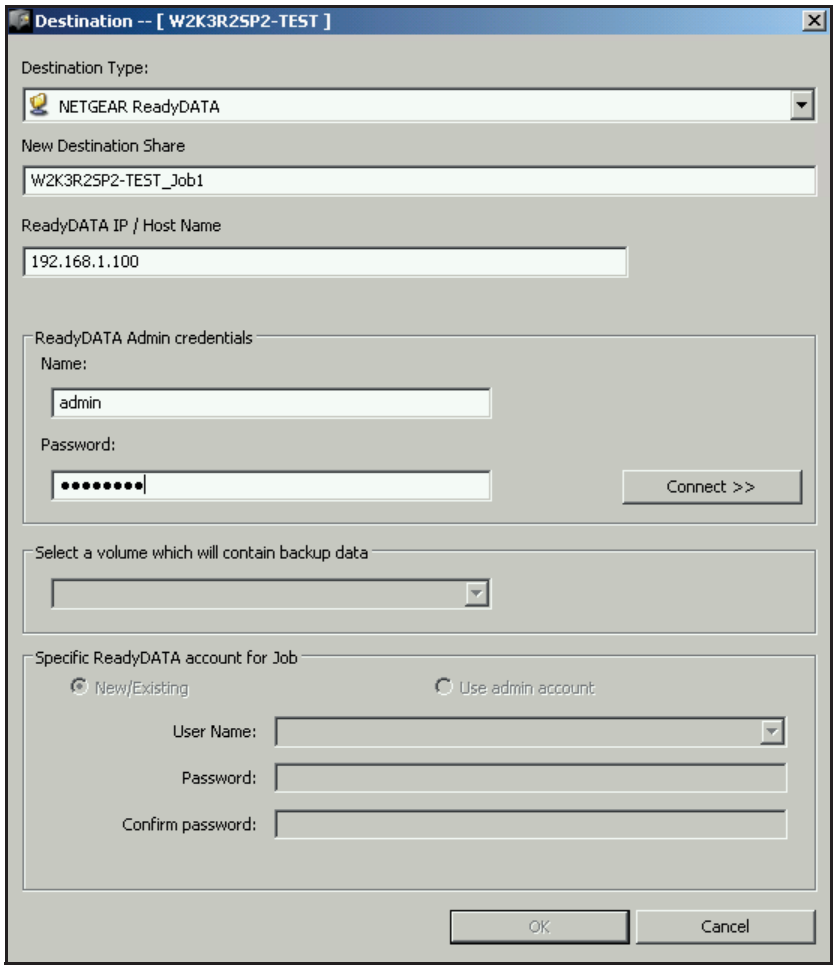
3. Step through the wizard.



4. Select the volumes that you want to protect.
5. Click the **Next** button.



6. From the list, select **Network Locations**.
7. Click the **Next** button.



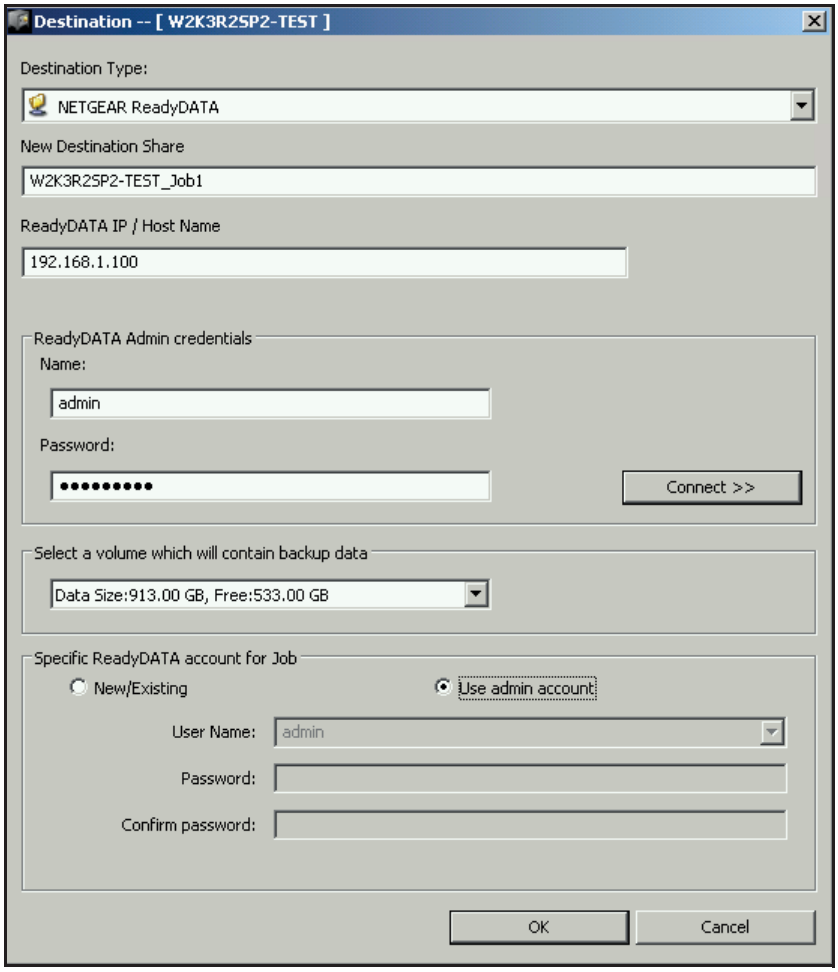
8. From the **Destination Type** list, select **NETGEAR ReadyDATA**.
9. Complete the fields in the top half of the screen.

Note: The admin password on ReadyDATA must not be the default password (which is password).

---

10. Click the **Connect >>** button.

    When ShadowProtect connects to the destination, the ShadowProtect Agent lists the available ReadyDATA volumes.



11. Select a volume from your ReadyDATA.

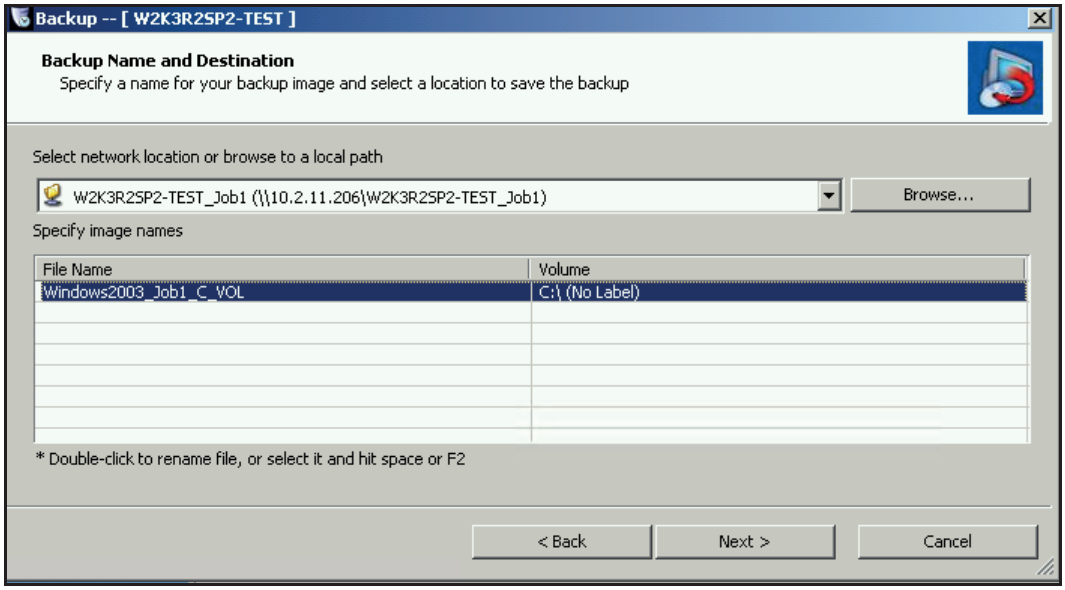
> **Note:** If ReadyDATA does not have a volume created already (the factory default), this setup procedure creates a volume for you with the default settings.

12. Select a ReadyDATA user account as the backup owner.

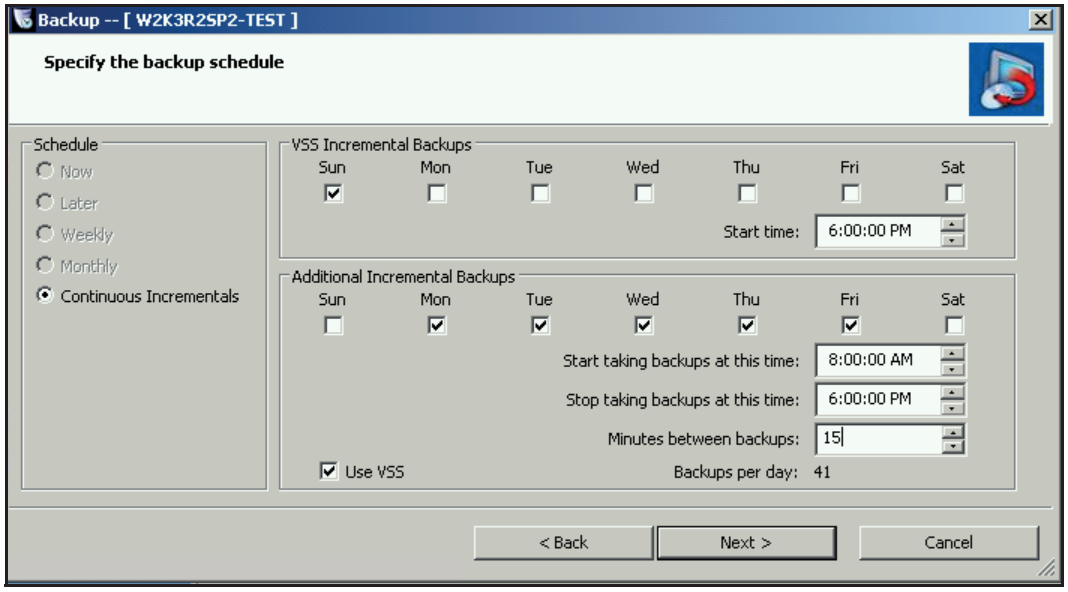
    A new backup user on the ReadyDATA is created.

13. Click the **OK** button.

    A NETGEAR ReadyDATA destination object is created.



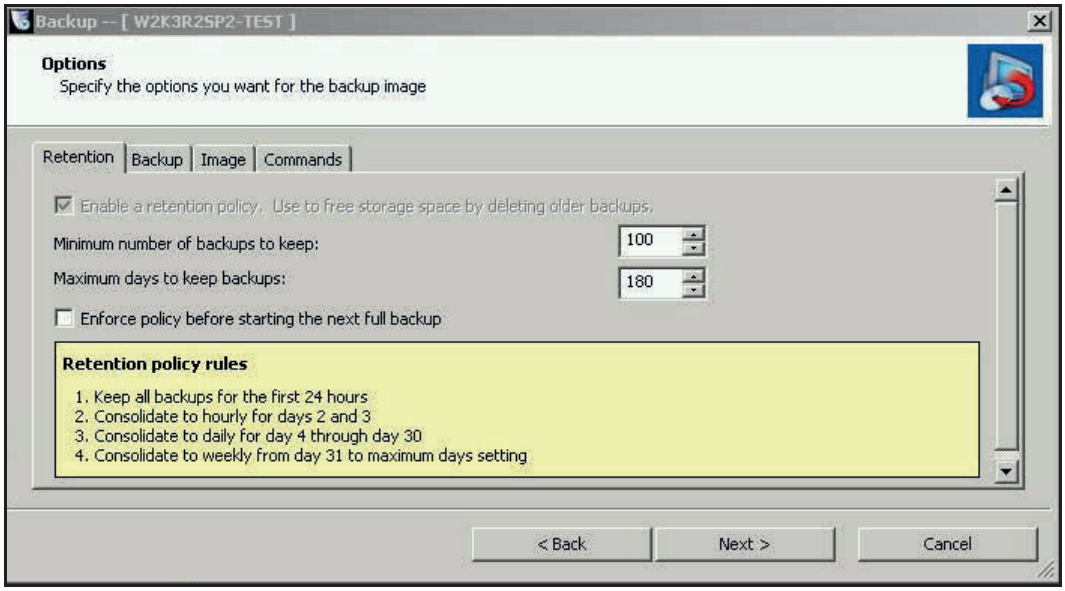
14. Click the **Next** button.



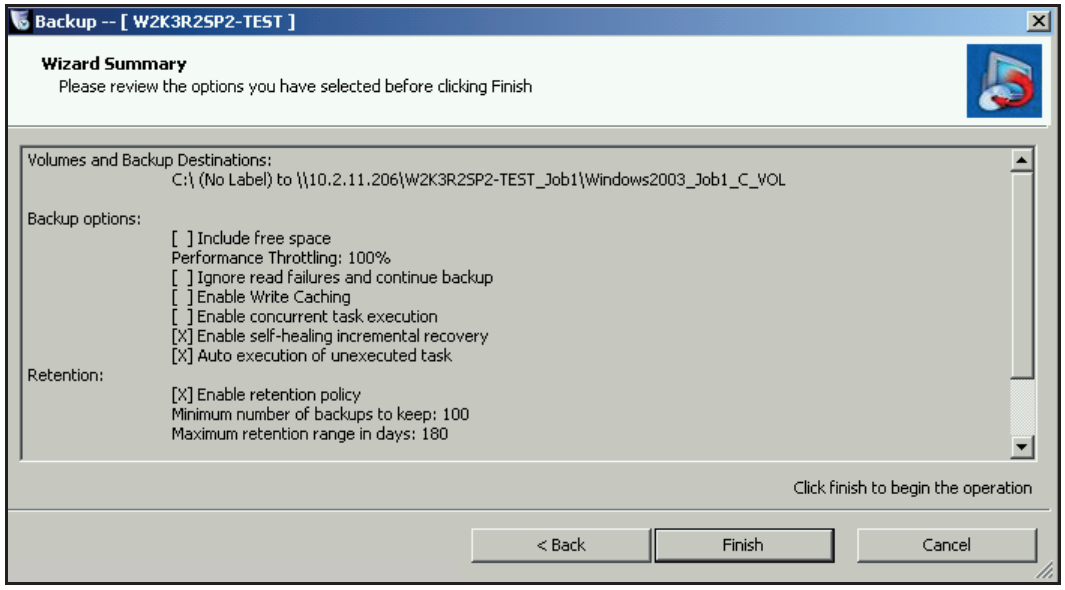
Note: The only option that is available is **Continuous Incrementals**. This solution never requires a full backup process after the first backup. For that reason, the other options are always be grayed out.

15. Adjust backup schedule as desired.

16. Click the **Next** button.



17. Change the retention parameters.
18. lick the **Next** button.



19. Select the **Finish** button.

    The backup job is saved and appears in the ShadowProtect interface.

Browse Recovery Points

On the ReadyDATA appliance, for each ShadowProtect backup, a share is created. On the appliance, a share is represented with the following icon:

Figure 2. Share icon

After backups have been running for a while, under the share created, a folder called Completed_Backups is created.

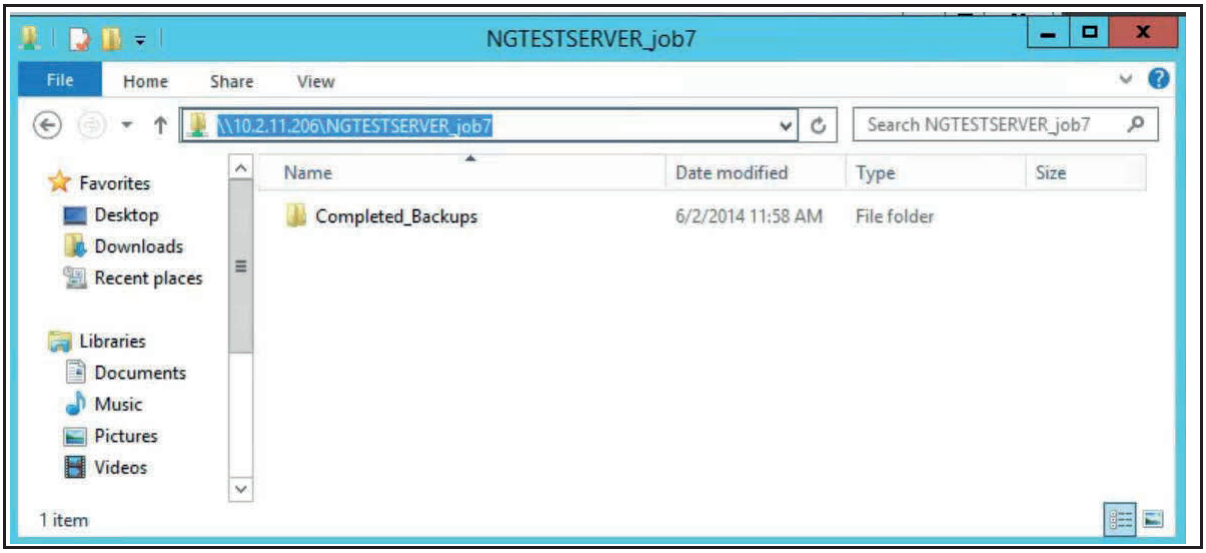


Figure 3. Completed_Backups folder

Within the completed backup folder, each point in time is represented with a folder for the date and time that the backup was created.

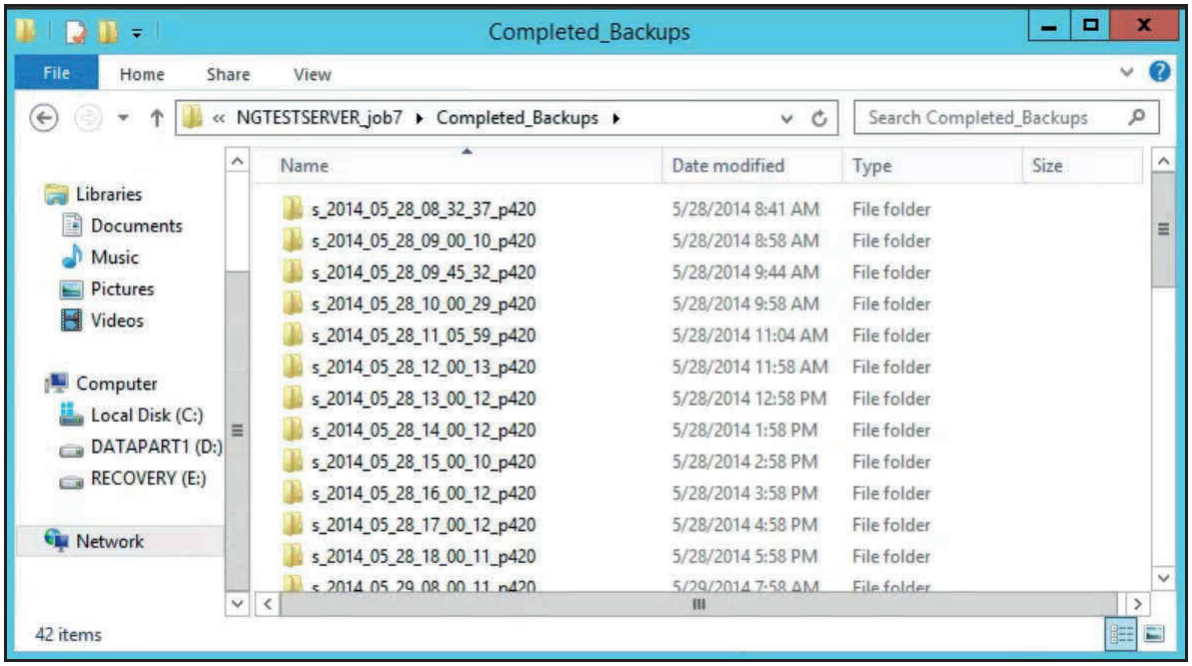


Figure 4. Backup folder contents

Within each folder recovery point, a set of .VHDX files represent the data points for that given point of time. These .VHDX files are used for file folder recovery through mounting or full volume restore.

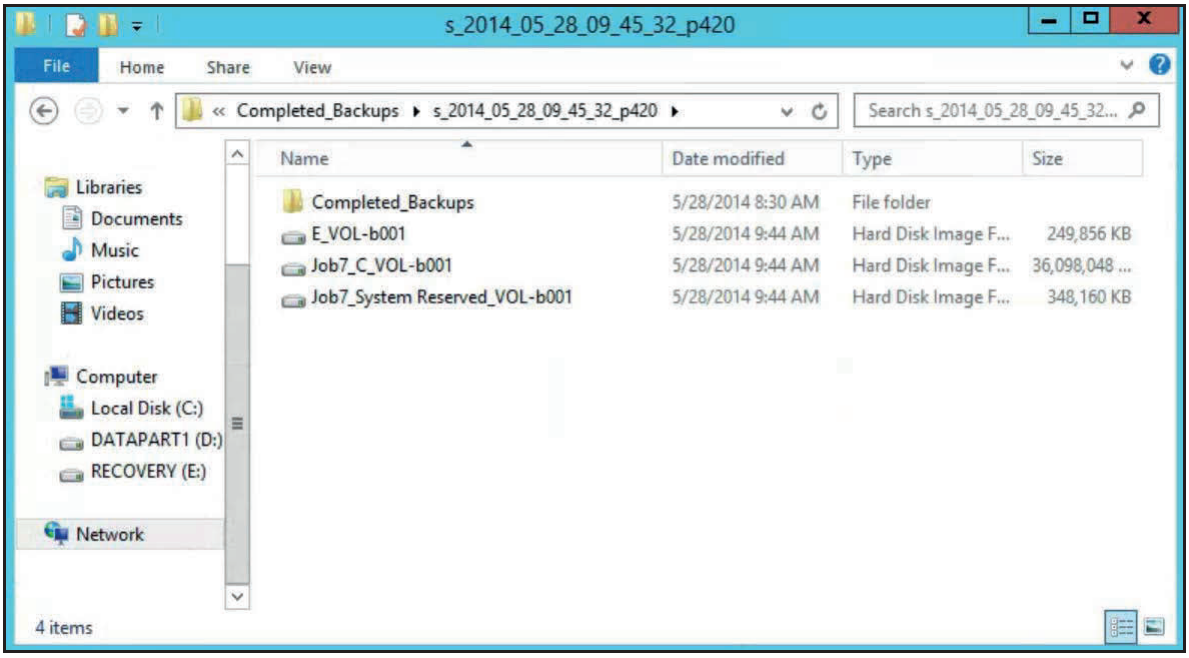


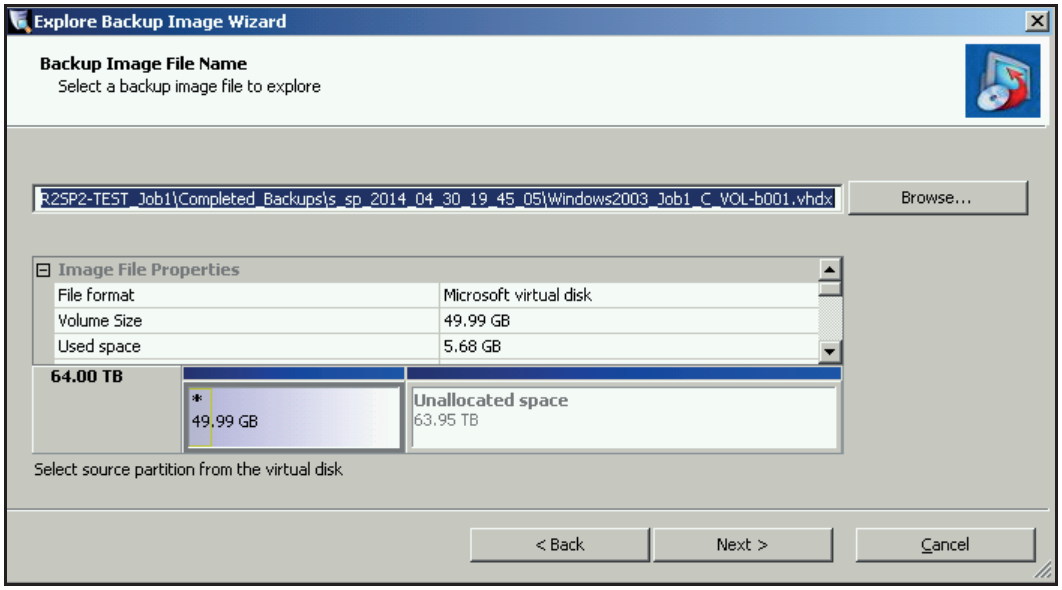
Figure 5. Folder recovery point files

Mount Recovery Points for File Recovery

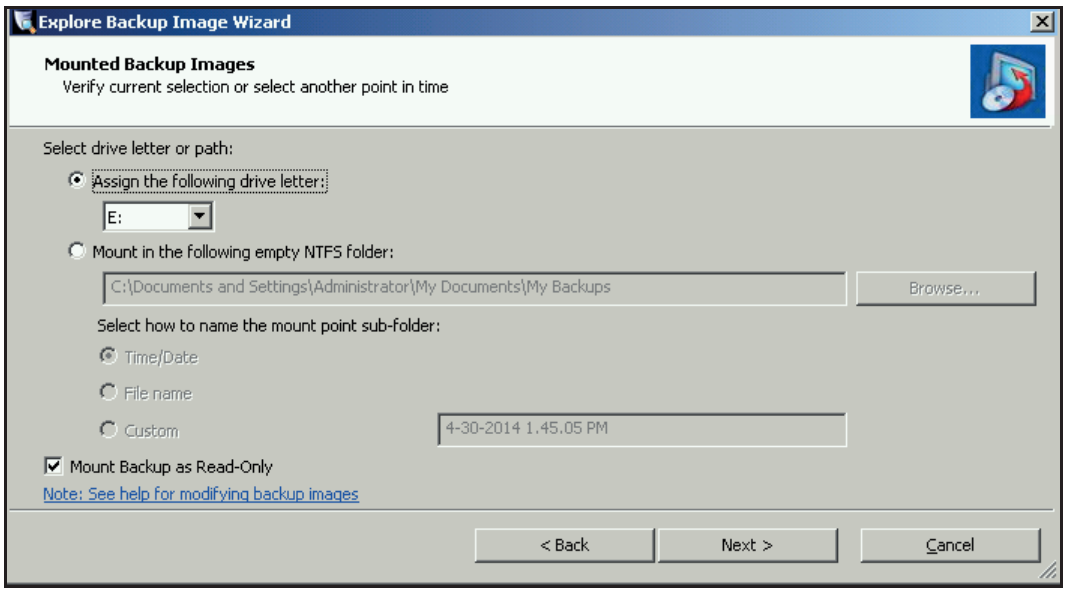
Mounting takes the `.vhdx` (point and time) file and presents it as a disk for browsing. This method is preferred for individual file folder recovery. Once a file is mounted, copy and paste it from the mounted drive to its intended destination.

➢ **To mount and recover files:**

1. From a UNC path to the data share, select the latest `.vhdx` file where you have written the data.
2. Right-click the `.vhdx` and select **StorageCraft Mount**.
3. Follow the wizard.
4. Select the mount parameters.



5. Click the **Next** button.



6. Browse to the drive letter that is selected in the mount wizard and look for the data you backed up earlier.
7. Save that data back to the desktop or other location.
8. Click the **Next** button.
9. In Windows Explorer, right-click the mounted drive and select **Quick Dismount**.

   The drive is removed.

Note: In a non-Windows domain security model, the administrator might need to take ownership of the files before browsing them.

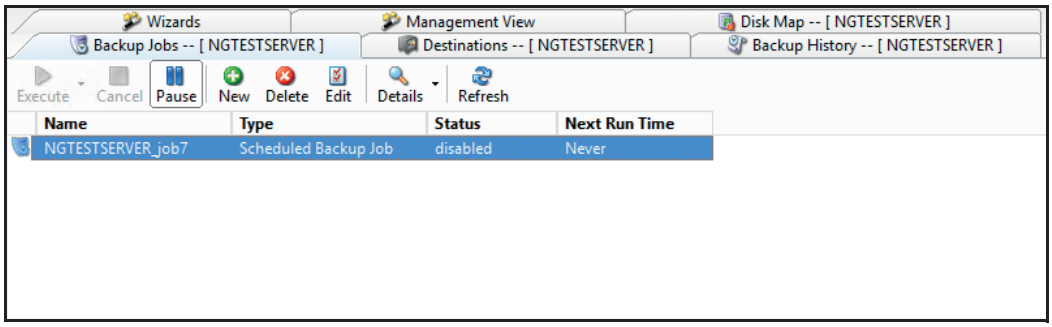
Full Volume Restore for Data Volumes

If the OS is intact, but the full data volume needs restoration, you can take the recovery point (.VHDX) and restore the full volume.

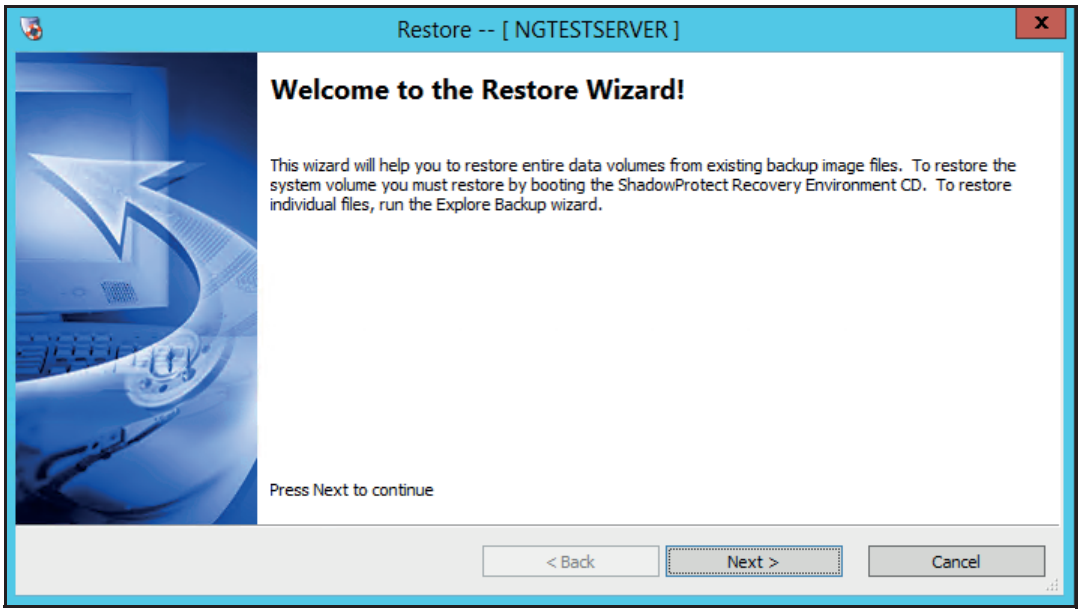
This option replaces all data on the target partition. Use this option only when you intend to replace the data.

➢ **To recover a data volume:**

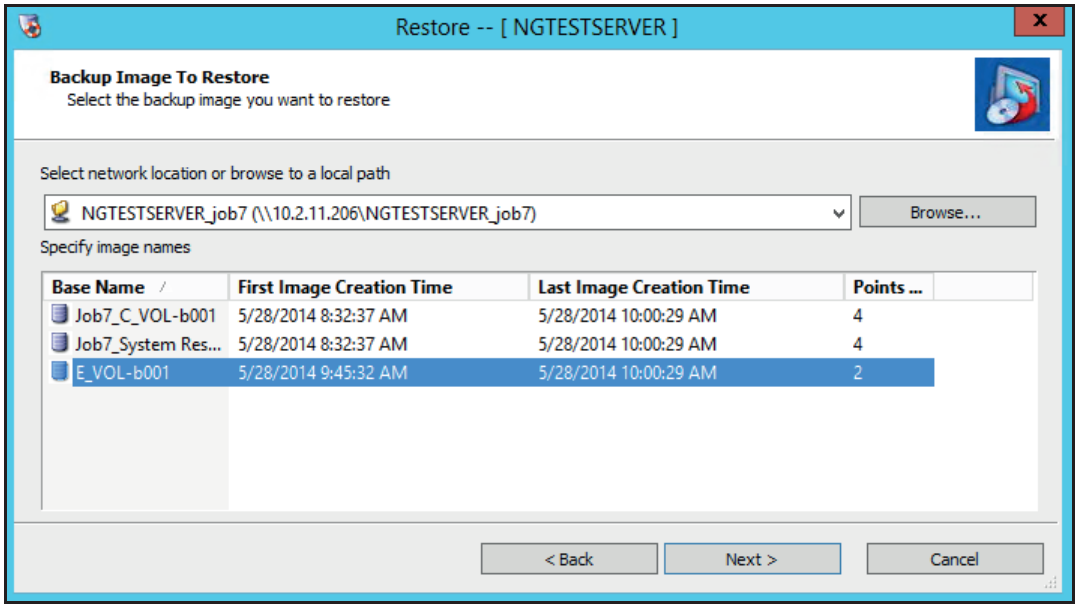
1. If you have a running backup job on the server for the given volume, pause the backup process.



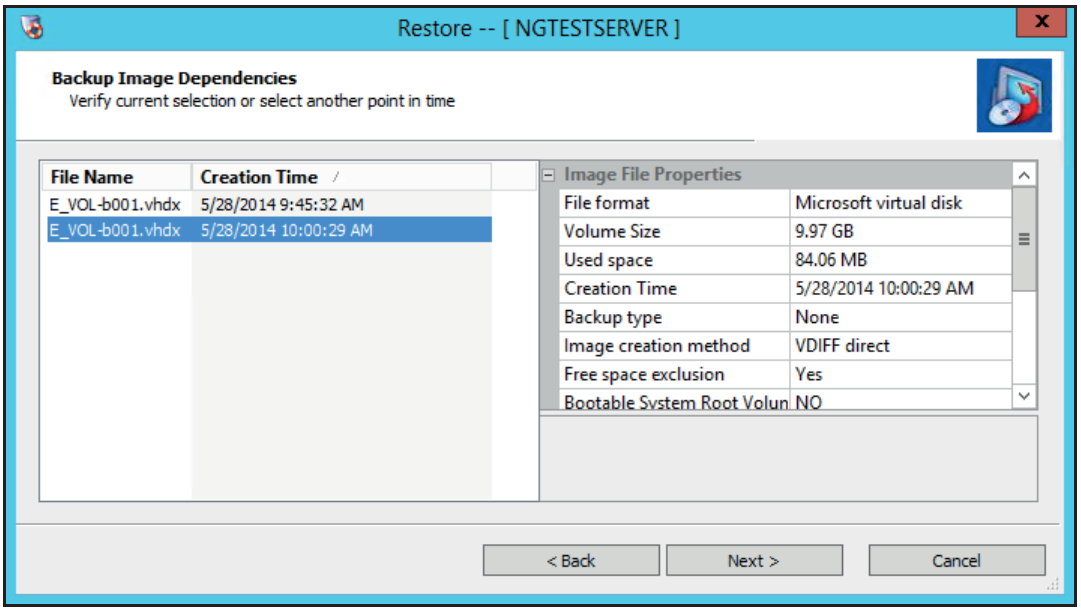
2. In ShadowProtect, launch the volume Restore Wizard.



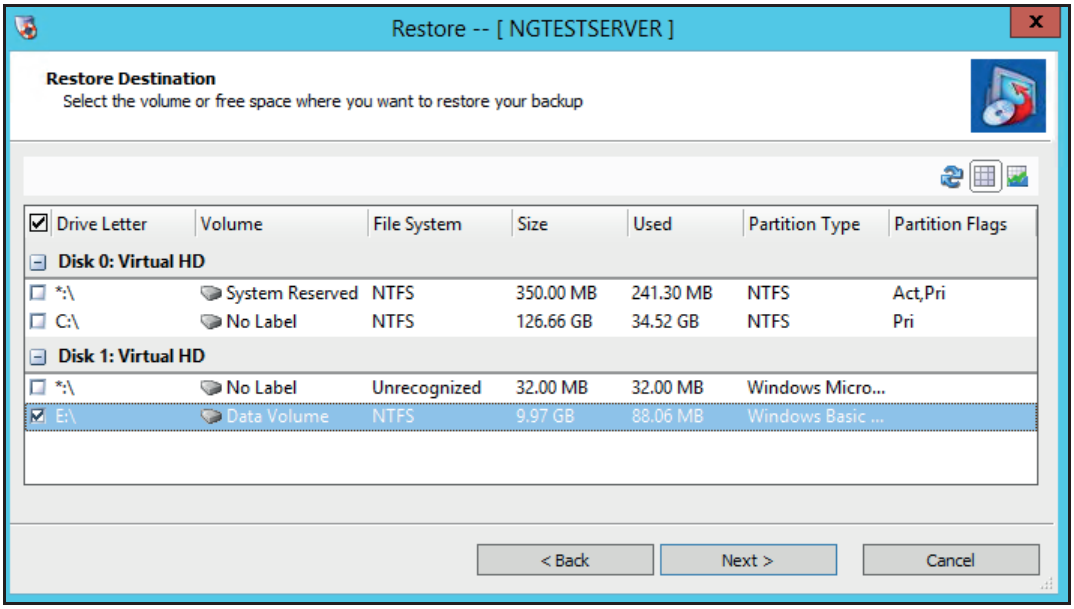
3. Click the **Next** button.



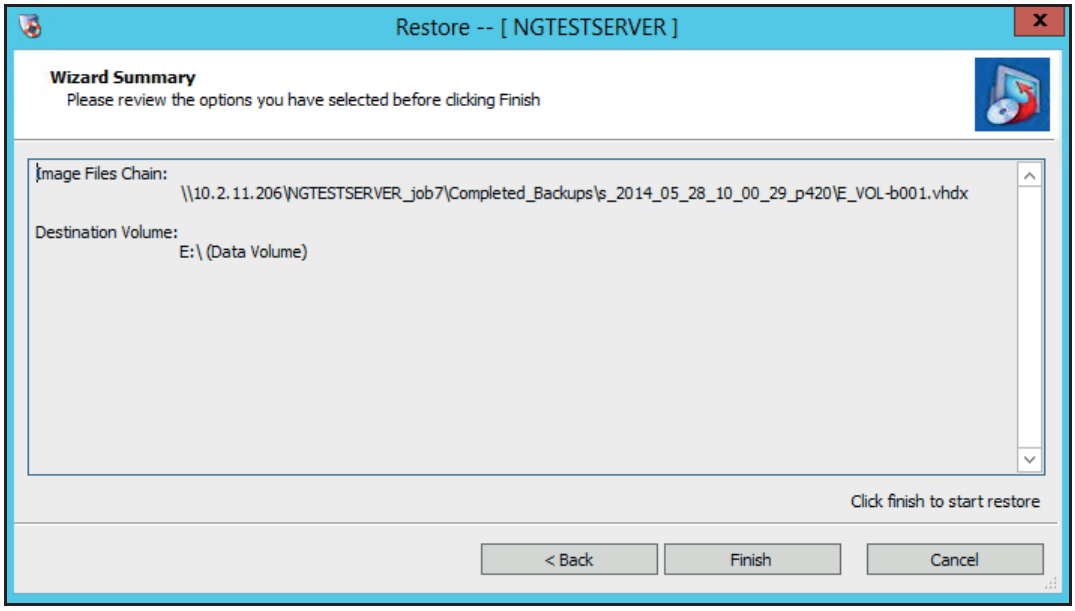
4. Select the data volume to be restored.
5. Click the **Next** button.



6. Select the point in time to be restored.
7. Click the **Next** button.



8. Select the restore destination volume.



9. Click the **Finish** button.

   The restore process starts.

Full System Restore or Bare Metal Recovery

A full system recovery is also known as a bare metal recovery.

A secondary boot environment provides a temporary operating system on the recovery server to allow for OS replacement.

The target servers can be physical or virtual.

When you are restoring data to hardware that is different from the source hardware, the hardware independent restore (HIR) process inserts the proper drivers from the Windows catalog of drivers contained within the recovery environment (RE). If the driver is not present, you can add your own driver to the HIR process.

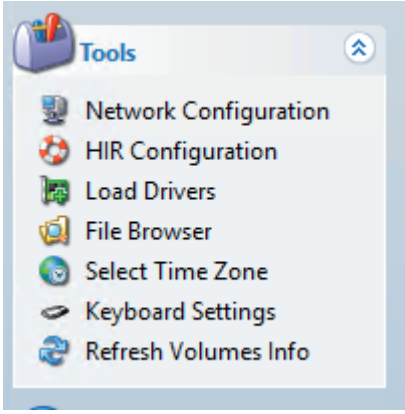
Boot the Recovery Environment and Map to the VHDX Stores

➤ **To boot the recovery environment and map to the VHDX stores:**

1. Place the recovery environment CD or `.iso` file into a target server and turn on to boot.

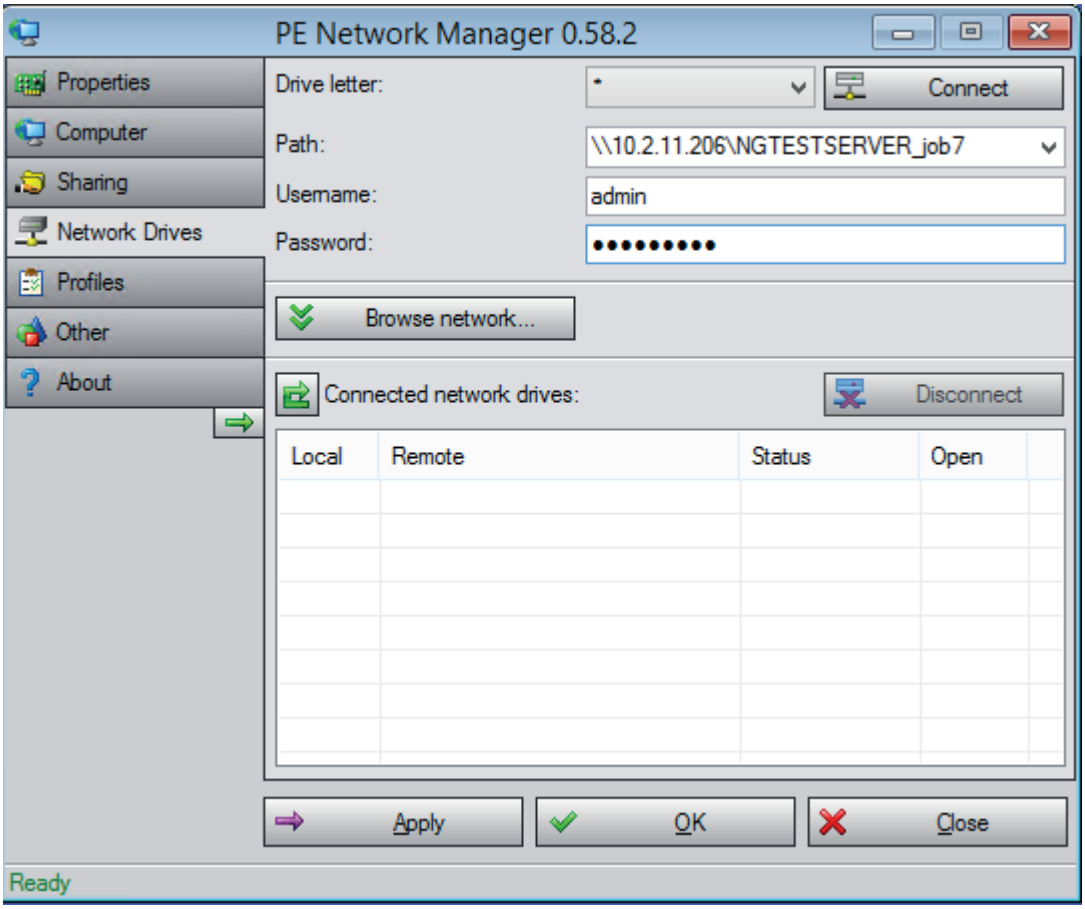
2. When prompted, click the **Yes** button to start network support.
3. When prompted, select the proper time zone.

   The PE environment is configured by default for DHCP. If you see an IP address in the information section on the left-hand panel, you have a properly running network interface.
4. To map a network drive, from the left-hand Tools panel, select **Network Configuration**.



5. From the left-hand menu, select **Network Drives**.
6. Complete the information for the share and the credentials to connect.

   The share name is the name that you created in the backup job process.
7. Click the **Connect** button.



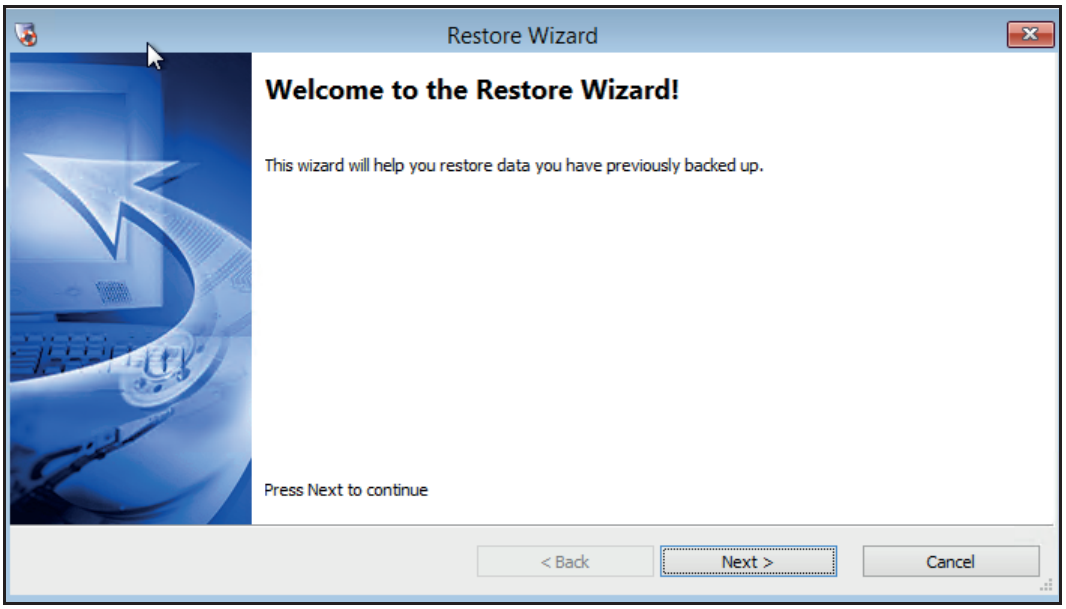
8. Click the **OK** button.
9. On the Network Configuration screen, click the **Close** button.

Restore Volumes

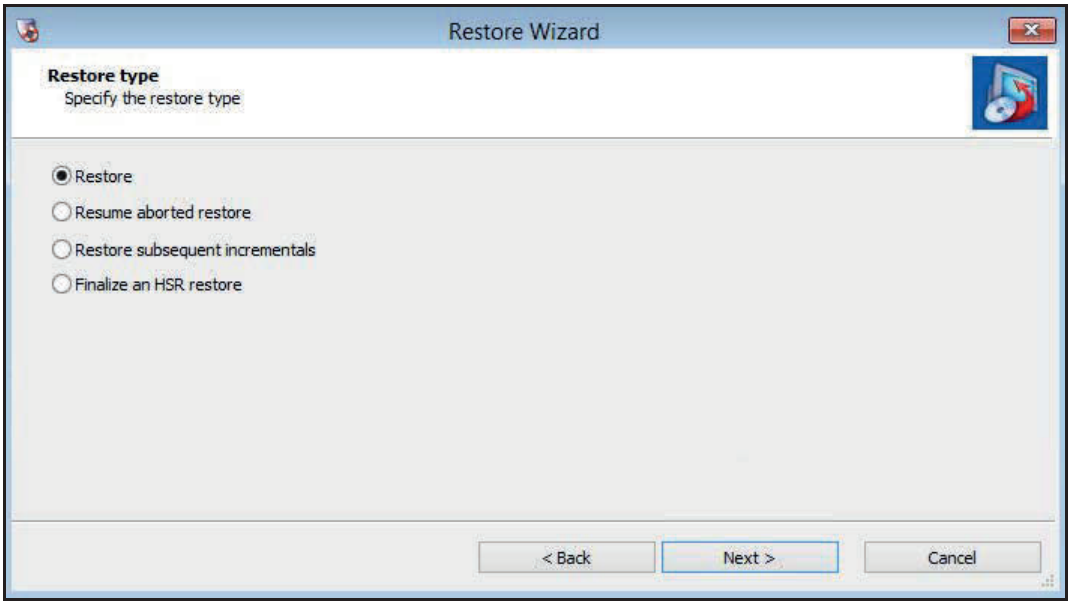
The restore volumes process is similar to data volume restore process.

➢ **To restore the volumes:**

1. From the main ShadowProtect menu, select **Restore Wizard**.



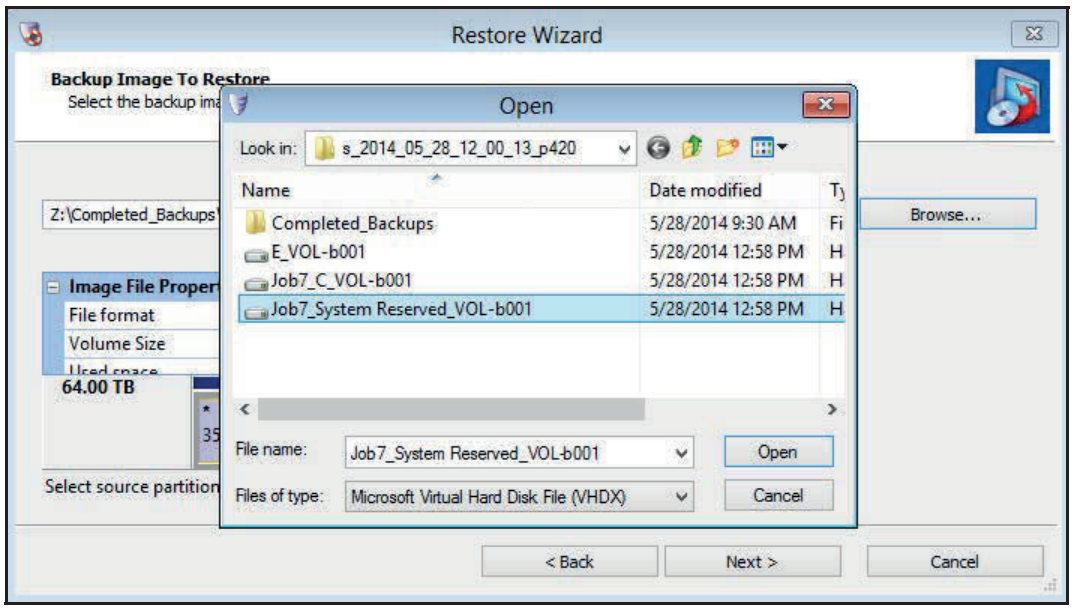
2. Click the **Next** button.



3. Select the **Restore** radio button.
4. Click the **Next** button.

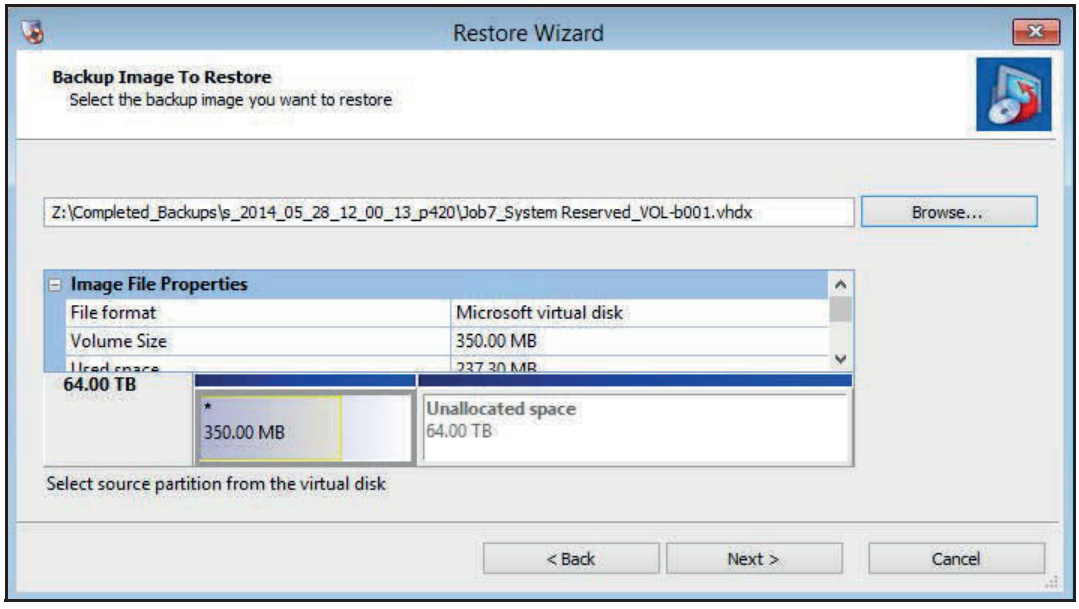
5. Browse to the image sets on the mapped drive and look for the proper point in the completed backups folder.

Note: The default file type is the ShadowProtect `.SPF` and `.SPI`. Change the file type to `.VHDX` to see virtual hard drives.



The screen changes and is populated with information about the original volume.

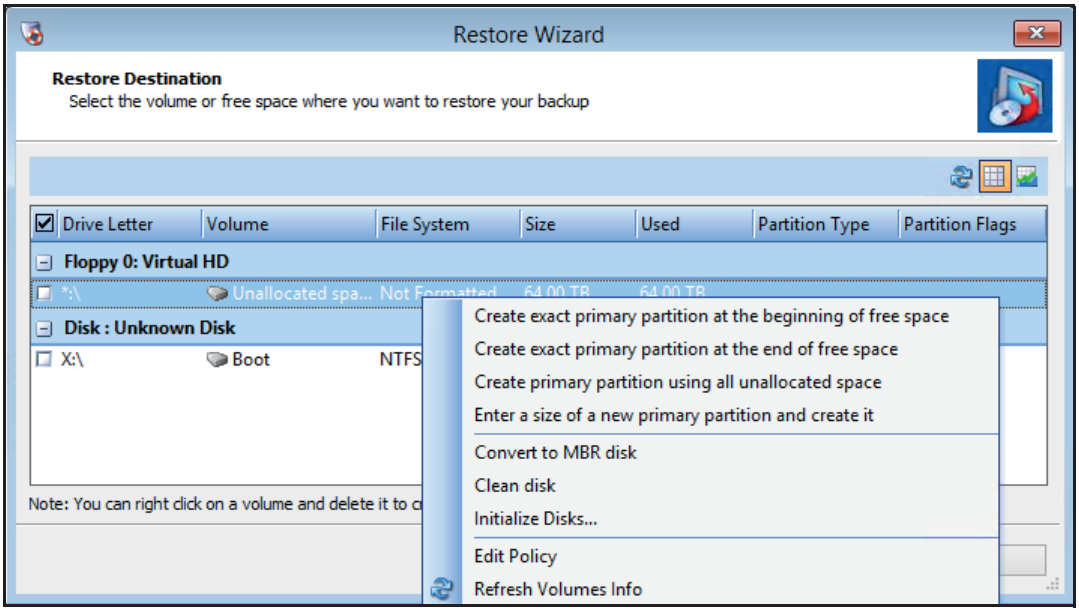
6. Click the **Next** button.



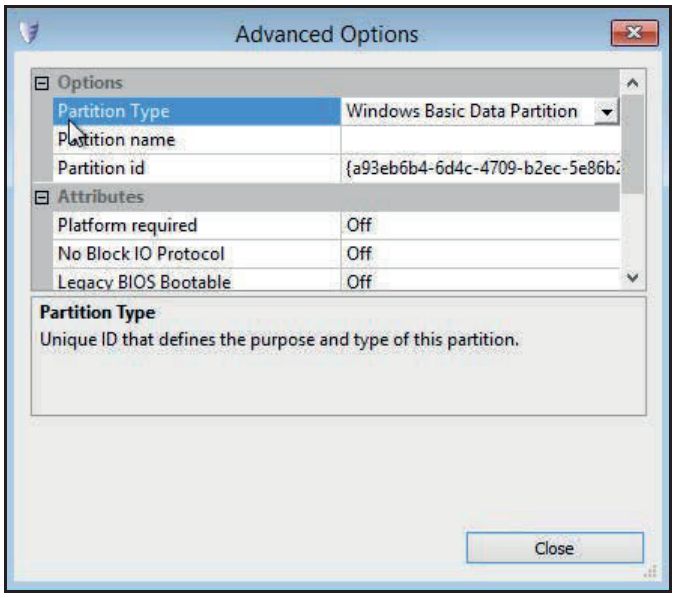
A partition must be created on the target disk to receive the data.

7. Click the **Next** button.
8. To create a volume, right-click and select your option.

   Most users select **Create exact primary partition at the beginning of free space**.



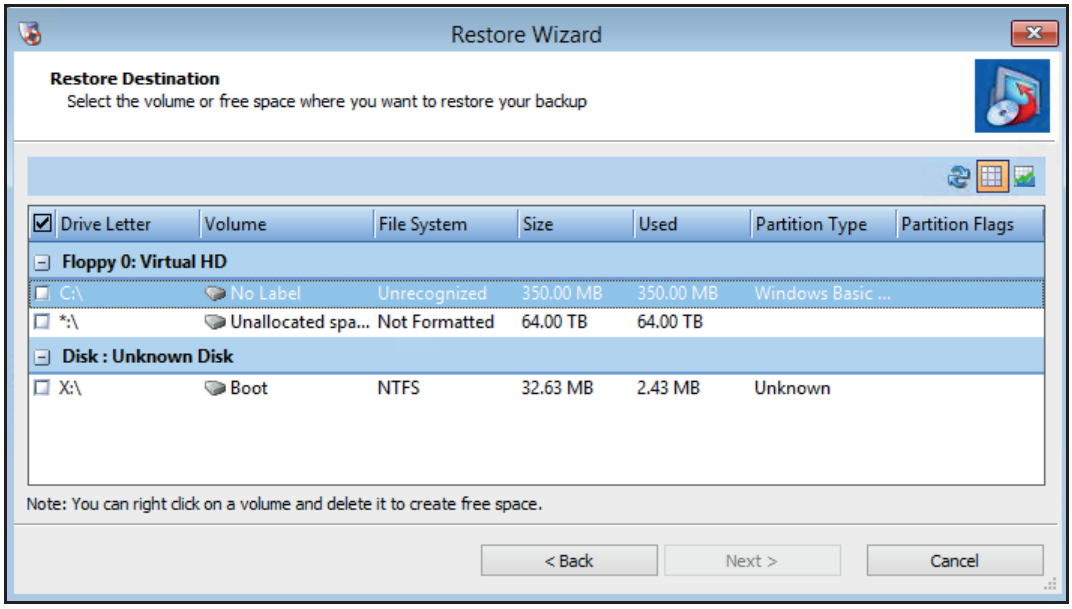
9. To complete the task, click the **Close** button.



Note: If the original source disk was of the type MBR, the destination disk needs to be of the same type. If the original source was GPT, the destination disk needs to be GPT. Conversion of the disk is displayed within the disk map tab on the main screen.

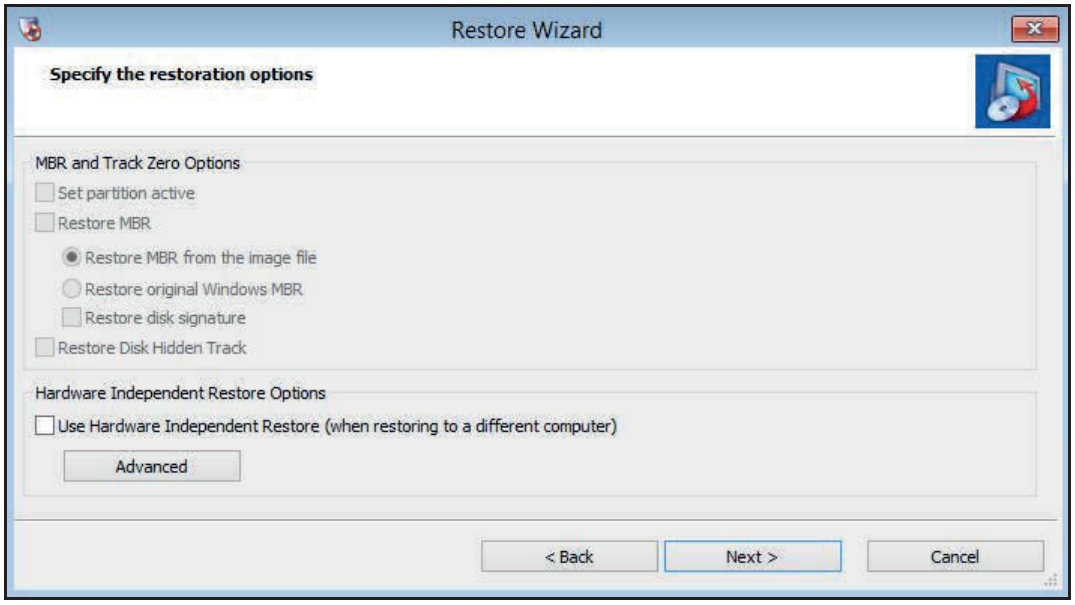
A target partition is created.

10. Select the target partition.
11. Click the **Next** button.

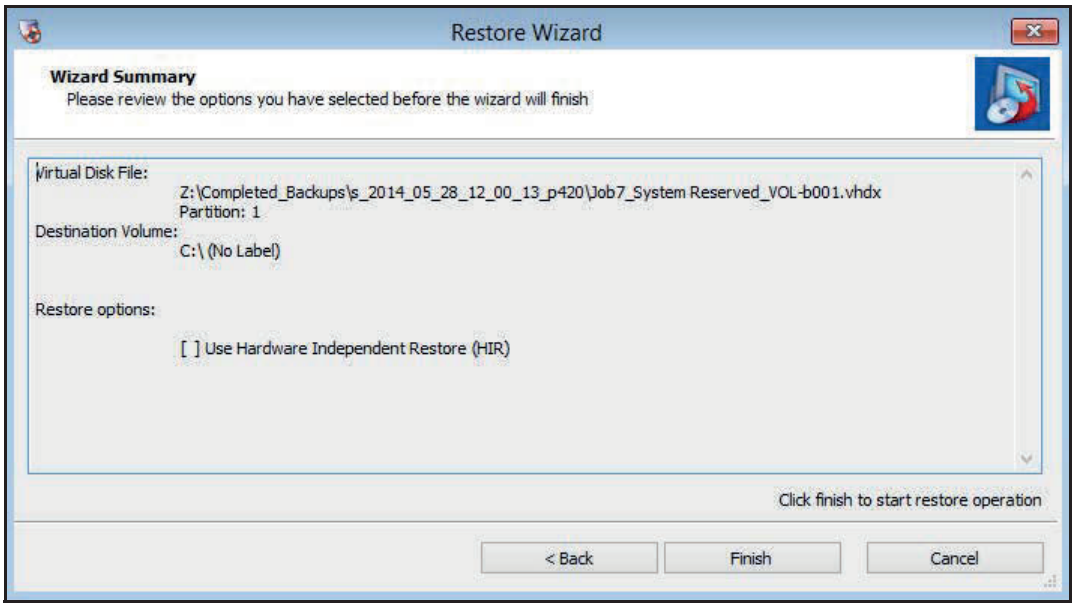


This screen displays and applies only to system volumes.

12. Click the **Next** button.

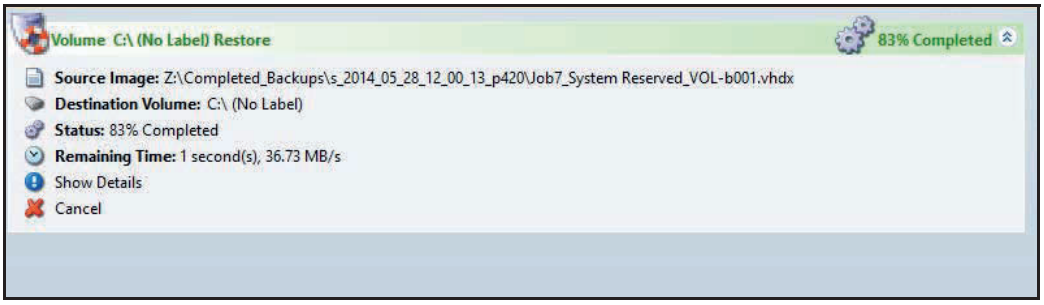


13. Click the **Next** button.



14. To start the restore process, click the **Finish** button.

    A new tab labeled Tasks displays in the ShadowProtect interface and shows the progress of the volume restore.

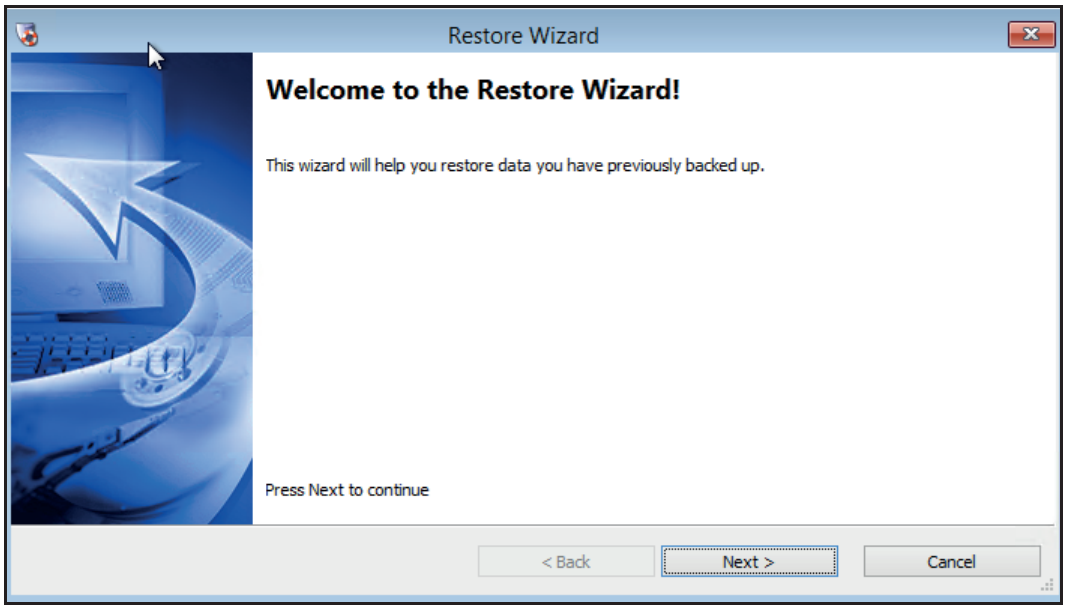


Hardware Independent Restore

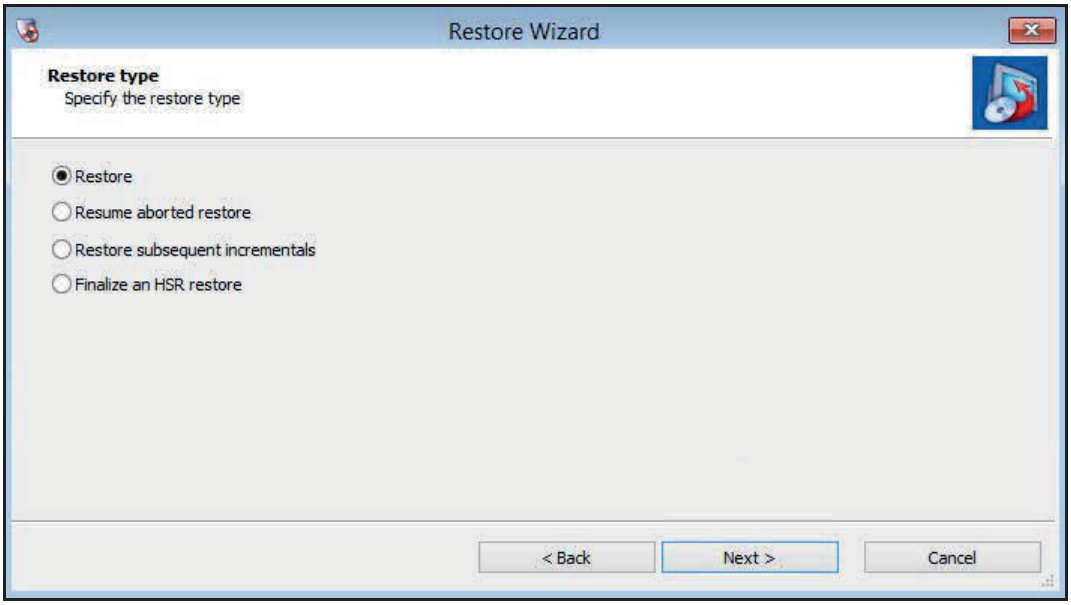
For any system volume that contains an OS on which you are restoring data to a device with a different hardware configuration, you must run the hardware independent restore (HIR) process against the restored volume.

➢ **To restore the hardware:**

1. From the main ShadowProtect menu, select **Restore Wizard**.

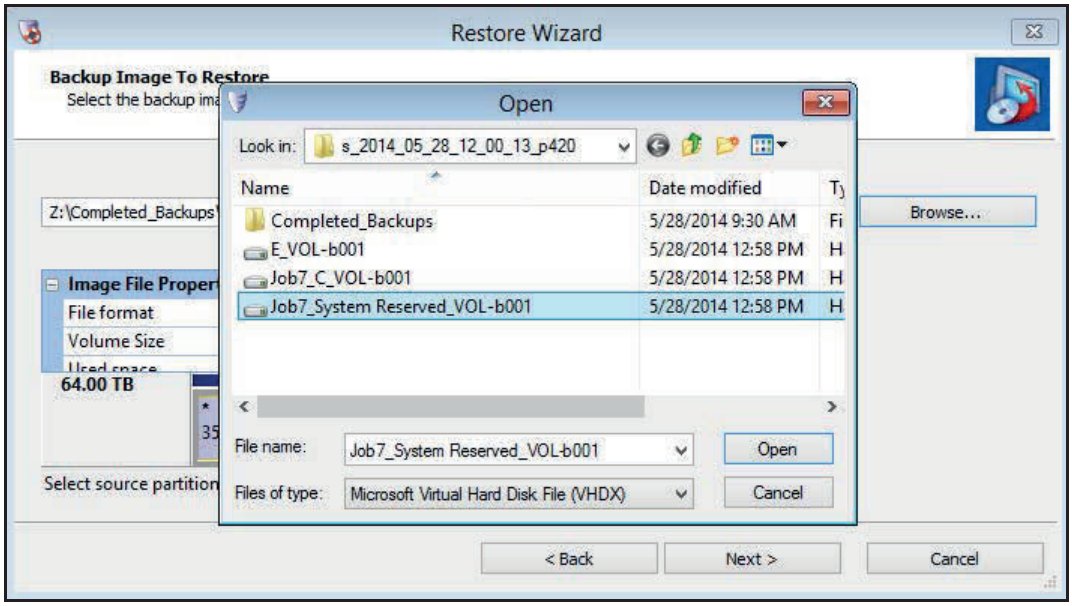


2. Click the **Next** button.



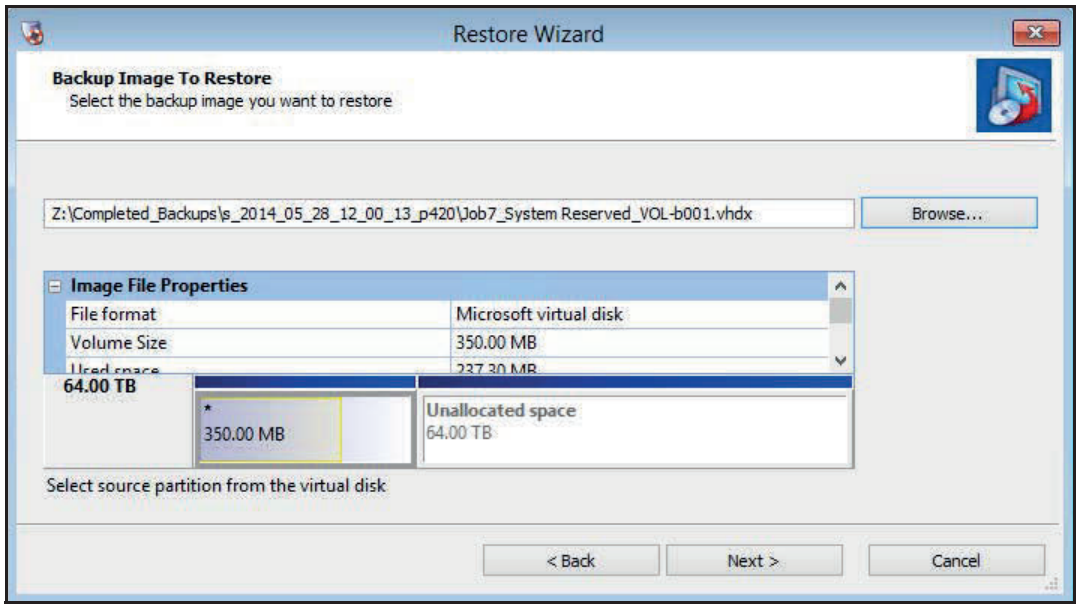
3. Select the **Restore** radio button.
4. Click the **Next** button.
5. Browse to the image sets on the mapped drive and look for the proper point in the completed backups folder.

Note: The default file type is the ShadowProtect `.SPF` and `.SPI`. Change the file type to `.VHDX` to see virtual hard drives.



The screen changes and is populated with information about the original volume.

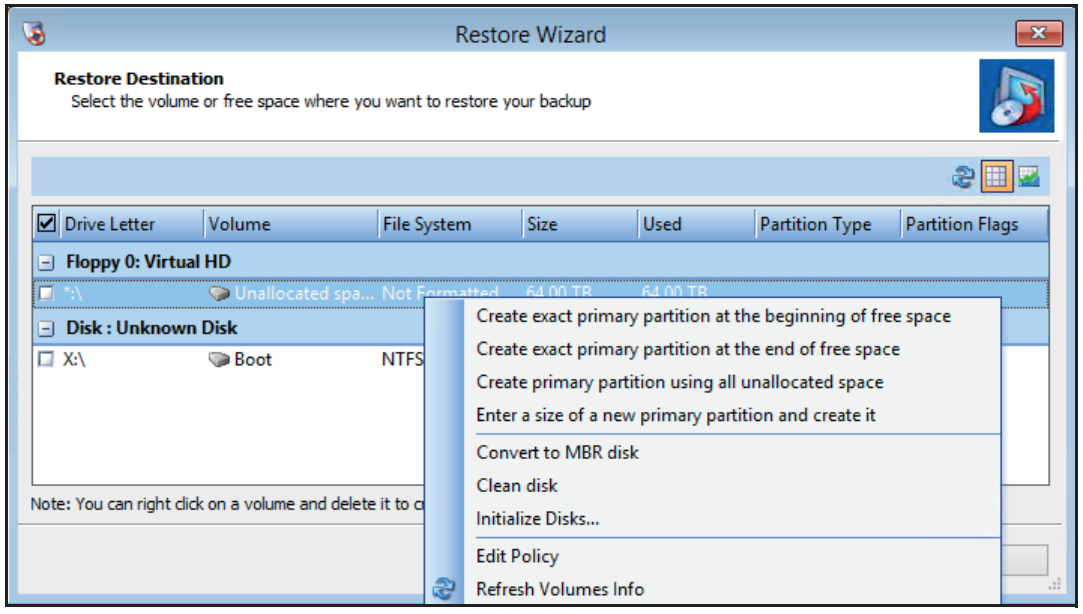
6. Click the **Next** button.



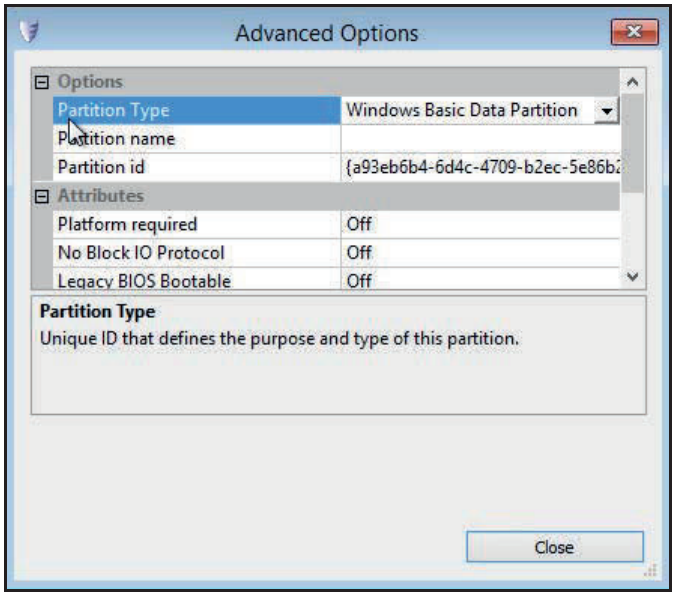
A partition must be created on the target disk to receive the data.

7. Click the **Next** button.
8. To create a volume, right-click and select your option.

   Most users select **Create exact primary partition at the beginning of free space**.



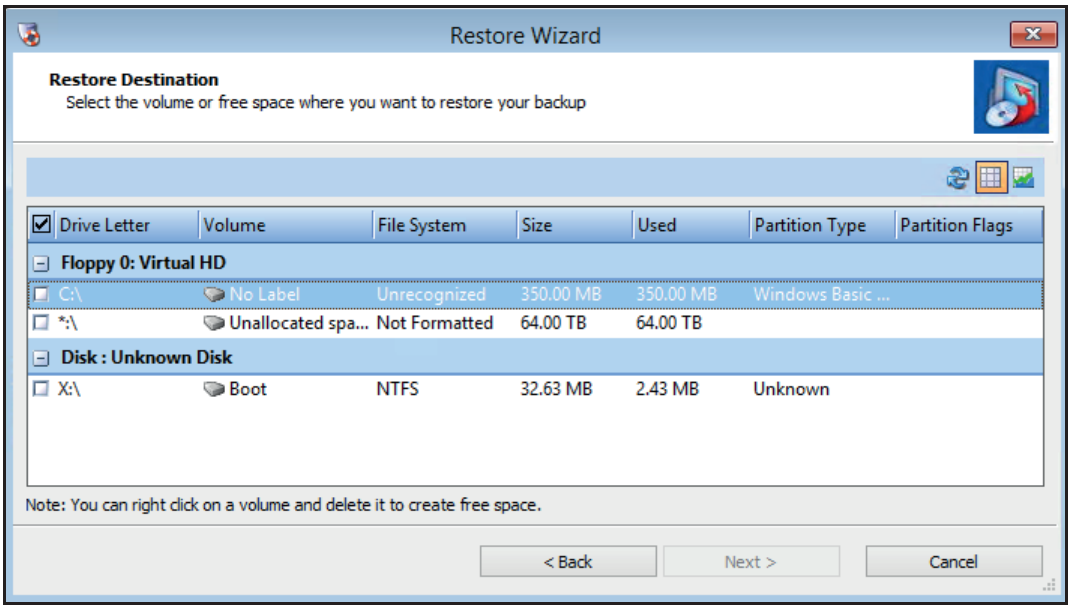
9. To complete the task, click the **Close** button.



Note: If the original source disk was of the type MBR, the destination disk needs to be of the same type. If the original source was GPT, the destination disk needs to be GPT. Conversion of the disk is displayed within the disk map tab on the main screen.

A target partition is created.

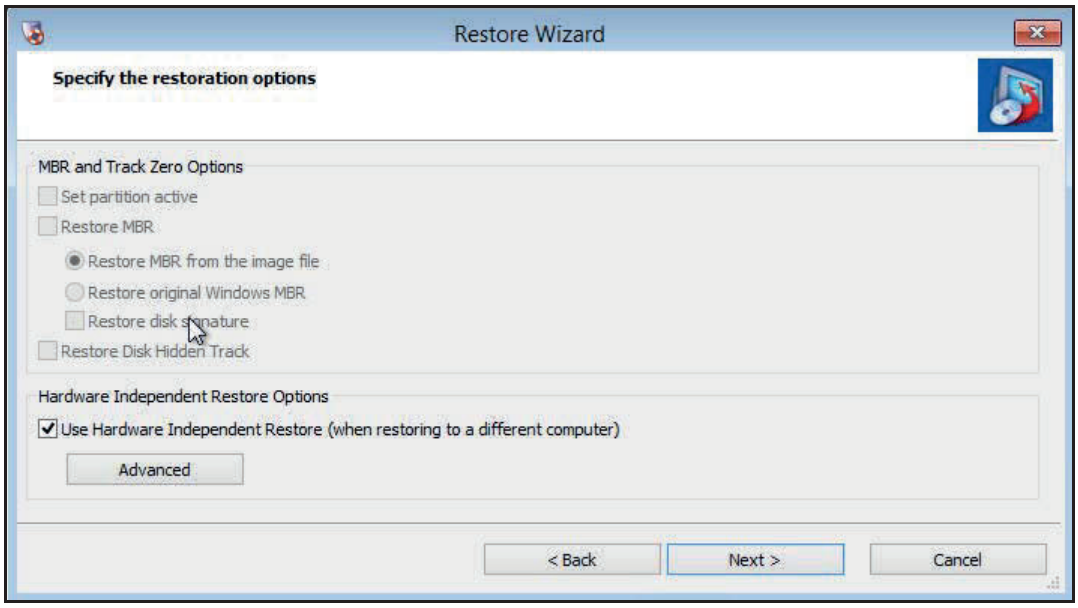
10. Select the target partition.
11. Click the **Next** button.



This screen displays and applies only to system volumes.

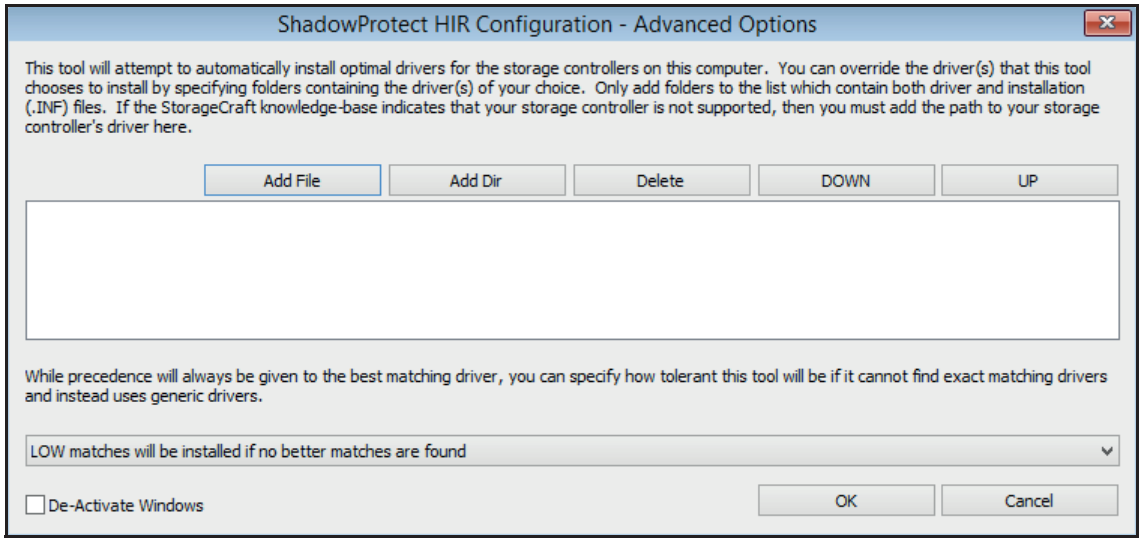
12. Click the **Next** button.

    The Specify restoration options screen displays.



13. To force the HIR process after a restore, select the **Use Hardware Independent Restore (when restoring to a different computer)** check box.
14. If you anticipate that a specific driver is needed (such as the RAID controller driver), click the **advanced** button.
15. Click one of the following buttons:
    - The **Add File** button to add a specific individual driver.
    - The **Add Dir button** to point a directory that contains drivers and their INF files.

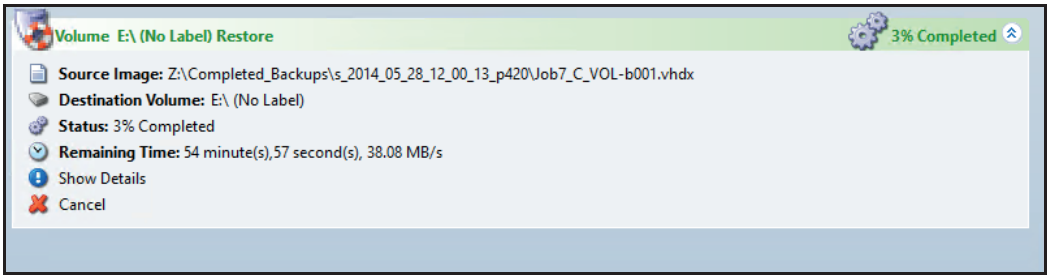
Note: This choice is not always needed. HIR attempts to use the base Windows drivers available from the driver catalog in the OS.



16. To apply the drivers, click the **OK** button.

    To close the screen, click the **Cancel** button.

17. In the Wizard, click the **Next** button.
18. To start the restore process, click the **Finish** button.
19. To see the details about the restore process in the recovery environment, from the task manager screen, click **Show Details**.



The HIR process occurs as the last task after the restore process. The following entries in the detail log show that the restore is complete.

28-May-2014 14:14:40	sptask	109	HIR Configuration Starting
28-May-2014 14:14:40	sptask	109	HIR Configuration Status:Starting HIR Configuration...
28-May-2014 14:14:42	sptask	109	HIR Configuration Status:Searching for Devices...
28-May-2014 14:14:42	sptask	109	HIR Configuration Status:Searching for Device Drivers...
28-May-2014 14:15:00	sptask	109	HIR Configuration Status:Installing Device Drivers...
28-May-2014 14:15:01	sptask	109	HIR Configuration Status:Finishing HIR Process...
28-May-2014 14:15:02	sptask	109	HIR Configuration Status:Finished
28-May-2014 14:15:02	sptask	200	HIR Configuration Completed

20. When all volumes are restored, either close the recovery environment or force a reboot to start the restored system.

Note: Occasionally, the Windows Catalog does not have the proper driver and you must locate and place the driver manually. When this happens, reboot the system to the recovery environment and select the HIR process from the left Tools panel. This component runs the process independent of the restore process.