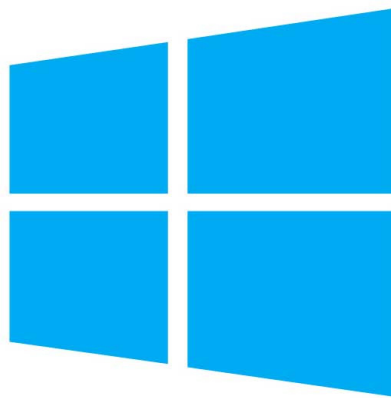




Windows Backup Utility

Used with RDX QuikStor® USB Removable Storage Systems



Windows

©2020 Overland-Tandberg. All rights reserved.

Overland®, Overland Storage®, DynamicRAID®, NEO®, NEO Series®, PowerLoader®, RAINcloud®, RapidRebuild®, REO 4000®, REO Series®, VR2®, and XchangeNOW® are registered trademarks of Overland Storage, Inc.

Tandberg®, Tandberg Data®, AccuGuard®, AccuVault®, BizNAS®, QuadPak®, QuikStation®, QuikStor®, RDX®, RDXPRESS®, RDXPRO®, StorageLoader®, SupportSuite®, Tandberg SecureService®, and Tandberg StorageLibrary® are registered trademarks of Tandberg Data Holdings S.A.R.L.

Overland-Tandberg™ is a trademark of Overland Storage, Inc.

All other brand names or trademarks are the property of their respective owners.

The names of companies and individuals used in examples are fictitious and intended to illustrate the use of the software. Any resemblance to actual companies or individuals, whether past or present, is coincidental.

PROPRIETARY NOTICE

The information contained in this document is subject to change without notice.

All information contained in or disclosed by this document is considered proprietary by Overland-Tandberg. By accepting this material the recipient agrees that this material and the information contained therein are held in confidence and in trust and will not be used, reproduced in whole or in part, nor its contents revealed to others, except to meet the purpose for which it was delivered. It is understood that no right is conveyed to reproduce or have reproduced any item herein disclosed without express permission from Overland-Tandberg.

Overland-Tandberg provides this manual as is, without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Overland-Tandberg may make improvements or changes in the product(s) or programs described in this manual at any time. These changes will be incorporated in new editions of this publication.

Overland-Tandberg assumes no responsibility for the accuracy, completeness, sufficiency, or usefulness of this manual, nor for any problem that might arise from the use of the information in this manual.

Overland-Tandberg
4542 Ruffner Street, Suite 250
San Diego, CA 92111 USA

TEL 1.800.729.8725 (toll free)
1.858.571.5555
FAX 1.858.571.3664

Tandberg Data
Feldstraße 81
44141 Dortmund, Germany

TEL +49 231 5436 0
FAX +49 231 5436 111



www.overlandtandberg.com



Preface

Audience and Purpose

This guide describes how to install and operate an RDX QuikStor in Fixed-Disk mode to provide a removable media option for Windows Backup that is not otherwise available.

This eBook covers both RDX QuikStor and RDX QuikStation products. It discusses One Button Disaster Recovery (OBDR) and Ransomware security options.

Organization

The following chapters are included in this guide:

Overview

- [Chapter 1, “Overview,”](#) provides an overview of the benefits and features of using RDX QuikStor with Windows Backup.

Installation and Setup

- [Chapter 2, “Configure Fixed-Disk Mode,”](#) describes information on how to initially configure the RDX QuikStor in Fixed-Disk mode for use with Windows Backup.
- [Chapter 3, “Bootable Recovery Cartridge,”](#) describes how to create a bootable recovery cartridge in case of a system failure.
- [Chapter 4, “Set up Windows Backup,”](#) provides the steps necessary to configure and schedule Windows Backup to work with RDX QuikStor.
- [Chapter 5, “Bare Metal Recovery of a Server,”](#) covers the critical process of recovering your system in the event of a system failure.

Supplemental Information

- [Appendix A, “BitLocker Encryption,”](#) describes Windows BitLocker software and its usage to encrypt a Windows System Image Backup.

Product Documentation & Software Updates

Product documentation and additional information are available online at our Knowledge Base website:

<https://www.overlandtandberg.com/knowledgebase/>

At the Overland-Tandberg Knowledge Base, select:

- **Product Type = RDX Solutions**

- **Product Family** = **All** or a product name
- **Model** = **All** or a product name

Use **Document Type** to select the document for which you are specifically looking.

To download drivers and software updates, see the [Drivers and Downloads](#) page.

Technical Support




For help configuring and using your RDX QuikStor system, email our technical support staff using the Online Support email addresses for your region.

- [Support - Americas](#)
- [Support - Asia Pacific and Middle East](#)
- [Support - Europe and Africa](#)

For additional assistance, search the Support section at <https://www.tandbergdata.com>.

Conventions

This document exercises several alerts and typographical conventions.

Convention	Description & Usage
 WARNING	A <i>Warning</i> contains information concerning personal safety. Failure to follow directions in the Warning could result in bodily harm or death.
WARNUNG	Eine <i>Warnung</i> enthält Informationen zur persönlichen Sicherheit. Das Nichtbeachten der Anweisungen in der Warnung kann zu Verletzungen oder zum Tod führen.
AVERTISSEMENT	Un <i>avertissement</i> contient des informations relatives à la sécurité personnelle. Ignorer les instructions dans l'avertissement peut entraîner des lésions corporelles ou la mort.
 CAUTION	A <i>Caution</i> contains information that the user needs to know to avoid damaging or permanently deleting data or causing physical damage to the hardware or system.
 IMPORTANT	An <i>Important</i> note is a type of note that provides information essential to the completion of a task or that can impact the product and its function.
Item_name	Words in this special boldface font indicate the names of buttons or pages found in the Web Management Interface.
Ctrl-Alt-r	This type of format details the keys you press simultaneously. In this example, hold down the Ctrl and Alt keys and press the R key.
NOTE	A <i>Note</i> indicates neutral or positive information that emphasizes or supplements important points of the main text. A note supplies information that may apply only in special cases, for example, memory limitations or details that apply to specific program versions.
Menu Flow Indicator (>)	Words with a greater than sign between them indicate the flow of actions to accomplish a task. For example, Setup > User > Password indicates that you should click the Setup tab, then the User secondary tab, and finally the Password button to accomplish a task.
<i>Courier Italic</i>	A variable (for example, " n ") for which you must substitute a value.

Convention	Description & Usage
Courier Bold	Commands you enter in a command-line interface (CLI) or a file name.

Information contained in this guide has been reviewed for accuracy, but not for product warranty because of the various environments, operating systems, or settings involved. Information and specifications may change without notice.



Contents

Preface

Organization	3
Overview	3
Installation and Setup	3
Supplemental Information	3
Conventions	4

Chapter 1: Overview

What This eBook Covers	7
Advantages of RDX QuikStor	7
Why Media Rotation Matters	8
The Whole Solution	8
RDX QuikStor vs. Backup to External USB Disks	8
RDX QuikStor vs. Backup to Cloud	8
RDX QuikStor vs. Backup to NAS	9
RDX QuikStor vs. Backup to Tape	9

Chapter 2: Configure Fixed-Disk Mode

Configure Fixed-Disk using RDX Manager	10
Directly Configure Fixed-Disk Mode	12

Chapter 3: Bootable Recovery Cartridge

Create a Bootable Recovery Cartridge	13
Verify the RDX Media	17

Chapter 4: Set up Windows Backup

Server OS Backup Configuration	20
Using Media Rotation	25
Running a Backup Outside the Schedule	27
Use BitLocker to Encrypt Your RDX QuikStor	27

Chapter 5: Bare Metal Recovery of a Server

Server Restoration	28
--------------------------	----

Appendix A: BitLocker Encryption

System Requirements	32
Using BitLocker to Encrypt Volumes	33
Encrypting Volumes using the BitLocker Control Panel	33
Data Volume Encryption	33

Index

1

Overview

The built-in Windows Backup Utility utility included with current Windows operating systems does not support removable media. That means, to back up your system or user data with removable storage products and Windows Backup Utility, you must backup to a fixed local disk or incorporate third-party backup software that recognizes the removable storage device.

RDX QuikStor has solved this problem by providing a mode that emulates a fixed disk which allows removable RDX media to be used with the Windows Backup Utility.

What This eBook Covers

This eBook provides:

- Information on the features and benefits of using RDX QuikStor Fixed-Disk mode with Windows Backup.
- Step-by-step instructions for a Windows Server environment on how to:
 - Create a bootable RDX media including a system recovery image.
 - Set up a backup job including media rotation for full disaster protection.
 - Recover from a system crash using RDX QuikStor recovery media.
- Additional information regarding the powerful Ransomware security software.
- Setting up deduplication on server volumes to save disk and backup media space.

Advantages of RDX QuikStor

RDX QuikStor removable disk systems fill an important gap and provide the missing Windows Backup functionality that enables you to use removable RDX media for your day-to-day backup operations. This means no extra backup software is required thus reducing operational costs.

The RDX QuikStor is simple to administer and gives you the flexibility of using removable media to create offsite copies to provide media rotation and offsite vaulting to meet compliance requirements.

With bootable RDX media and system image backup, full One Button Disaster Recovery (OBDR) is possible.

You can protect your data against cyber-attacks with the RansomBlock feature of **rdxLOCK** software and WORM media.

Why Media Rotation Matters

The removability of the RDX media allows implementing data protection best practices by rotating cartridges to provide multiple layers of protection using the Air Gap security concept. One media would reside in the drive ready for the backup, one media is located offsite at an external location, and the third one is on its way either to or from the office. A media rotation scheme with at least three media cartridges allows you to meet most disaster protection and compliance requirements.

The Whole Solution

When compared with other possible backup solutions, it is easy to see the superiority of the RDX QuikStor solution.

RDX QuikStor vs. Backup to External USB Disks

The RDX QuikStor system includes significant removable cartridge features and value benefits that are lacking in basic external USB disk subsystems. While external USB disks seem to do the job of RDX QuikStor at a lower price, those USB disks are not built for professional environments. The RDX QuikStor and RDX media are business grade and provide a higher level of reliability and durability. This results in a much longer lifetime and the media ventilation (airflow) ensures cool operation and best write and read performance whenever you need it.

Other key differences include:

- **Drop Resistant** – RDX media is incredibly rugged and shock resistant to accommodate accidental falls from the rack or desk. This also means it can be transported offsite without concerns regarding the protection of your business data!
- **Static Protection** – The special design of RDX QuikStor eliminates server failures due to statically charged peripherals.
- **Stable Drive Letter** – Because the RDX QuikStor stays connected, when an RDX media is either inserted or removed, the RDX QuikStor drive letter remains the same.
- **Server Chassis Integration** – An RDX QuikStor can be connected to the USB port as an external drive or as an internal drive directly in a server chassis eliminating the need to unplug components after each backup. This constant connection simplifies backup automation and eliminates user-induced problems.

RDX QuikStor vs. Backup to Cloud

Backup to Cloud (Backup as a Service, or BaaS) is becoming more popular, but there are still concerns about security, bandwidth, and cost. Users question if their data is safe against spying or manipulation.

Other concerns:

- **Network Dependency** – Recovery from the Cloud might be too slow due to weak network bandwidth or might even be impossible due to total IT breakdown and loss of a network connection. Because RDX QuikStor systems are directly connected to the computer system, a backup is fast and done locally, not over the network/Internet. Restores can be performed easily even if the system needs to be rebuilt from scratch.

- **Cost of Ownership** – Many Cloud providers attract with low entry level fees, but if data is growing, the price increases rapidly. Accessing data usually has high fees charged by most cloud providers, so this will increase recovery cost dramatically. RDX QuikStor is an affordable alternative as user cost is manageable and predictable.
- **Data Security** – Many companies are afraid of sending their business critical and sensitive data into the Cloud. With RDX QuikStor, data is kept locally or at a secure offsite location that is easily accessed. That means backup data is secure as it resides in a known and protected environment.

RDX QuikStor vs. Backup to NAS

Using NAS systems as the only backup repository is very common. But, as NAS systems can be threatened by virus and ransomware attacks, backups are not secure. There must be a secondary backup implemented to removable media. Also, NAS systems are complex in deployment and usage. RDX QuikStor provides flexible, economical, and easy to use backup storage.

Some advantages over NAS:

- **Virus/Malware Protection** – As a removable disk system, RDX QuikStor provides virus and ransomware protection with offsite storage capabilities. With features like WORM, RansomBlock ransomware protection, or PowerEncrypt FIPS 140-2 validated hardware encryption, RDX QuikStor provides powerful and business-grade backup storage.
- **Disaster Recovery** – In case of a local disaster, backups on NAS systems would also be lost. By implementing media rotation with RDX QuikStor, at least one copy of backup data is still available.
- **Media Spanning** – Numerous backup softwares are able to span backups across multiple media in case the media is full or backup sets exceed the capacity of one media. With RDX QuikStor, media spanning is fully supported.

RDX QuikStor vs. Backup to Tape


Tape provides advantages like removability and high data-transfer rates. In addition, the tape write format prevents infection by virus and ransomware attacks. However, in comparison to RDX media, tape needs special care in handling and use limiting its effectiveness.

RDX QuikStor system advantages:

- **Environmental Flexibility** – Harsh environments with dust and dirt can destroy the tape surface and with this, the data. Read/write heads require cleaning on a regular basis due to tape debris. RDX media is impervious to damage in such conditions.
- **Drop Resistant** – Tape cartridges do not withstand drops or shocks. The RDX media is incredibly rugged and shock resistant to accommodate accidental falls from the rack or desk.
- **Durability** – Tape insert/eject cycles are limited to 350, where RDX media offers 5000 cycles.
- **Temperature Range** – The archive temperature of a tape cartridge is between 16° C and 32° C (60° F and 90° F). The archive temperature of an RDX QuikStor is between -40° C and 65° C (-40° F and 194° F).
- **Compatibility** – With tape, compatibility issues exist when switching to a new generation of tape. LTO drives are only able to read one or two prior media generations requiring drives needing to be renewed and existing data being migrated to the new media. In comparison, an RDX QuikStor system is fully backward and forward compatible. requiring no data migration when more capacity is needed.

2

Configure Fixed-Disk Mode

 **IMPORTANT:** The RDX QuikStor must be in Fixed-Disk mode to use Windows Desktop OS System Image Backup.

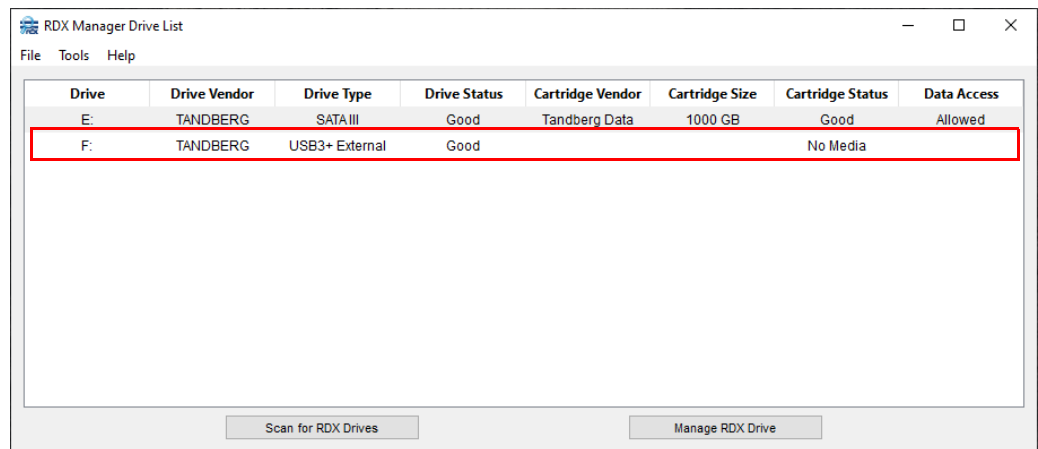
Use the RDX Manager software (version 1.0.1.20 or later) to configure your RDX QuikStor to a Fixed-Disk mode. The latest software is available on the RDX QuikStor download section of the Tandberg Data website ([Products > Software > RDX Manager](#)). RDX SATA III drives cannot be used with Windows Backup at this time as they do not have a Fixed-Disk mode.

Configure Fixed-Disk using RDX Manager

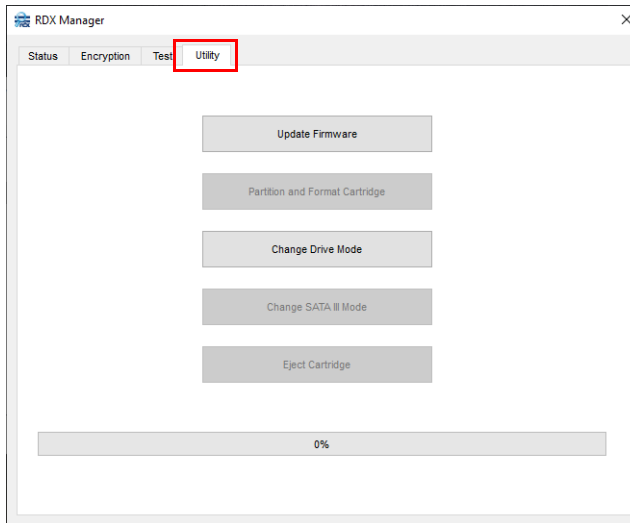
NOTE: If there is RDX media in the drive, eject it.

After installing the RDX Manager software, configure it in Fixed-Disk mode:

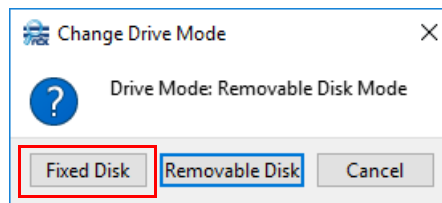
1. Start **RDX Manager**.
2. From the RDX Manager Drive List, select (click) the **drive** with which you will be working to open the Management Pop-up Window.



- 3. Select the **Utility** tab.

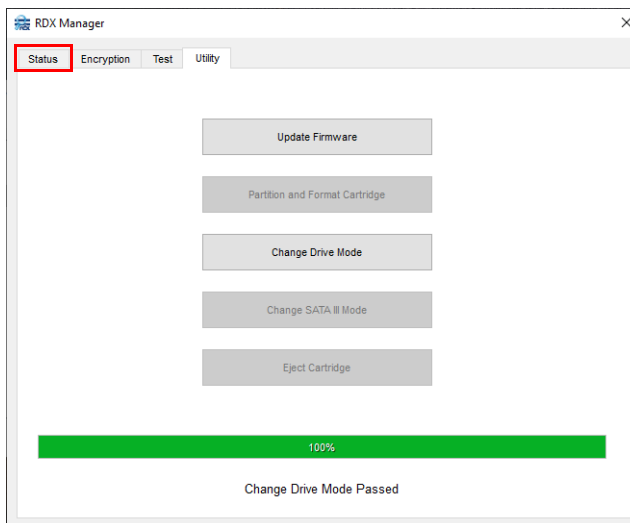


- 4. Click **Change Device Mode**.
If media is in the drive, you are directed to eject it.
- 5. Click **Fixed Disk**.

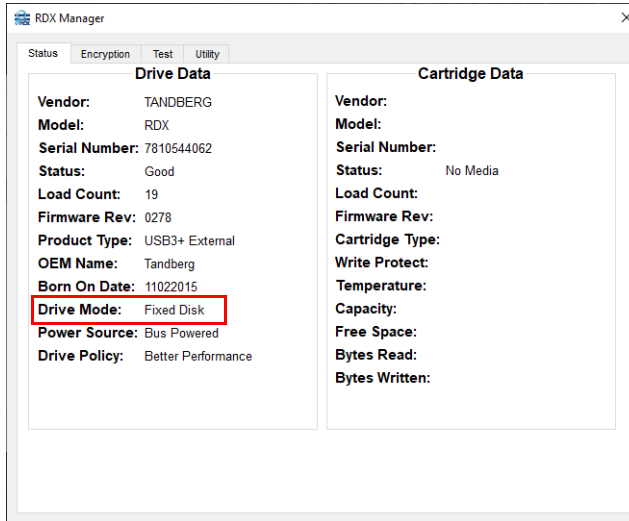


The drive automatically changes modes and updates.

- 6. When the 100% green bar is shown, click the **Status** tab.



- 7. Confirm the **Drive Mode** shows **Fixed Disk**.



8. Close the Management Pop-up Window.

Directly Configure Fixed-Disk Mode

You can change the mode directly at the RDX QuikStor by following these steps:

1. Verify there is **no media** in the drive.
If media exists, eject it.
2. Press and hold the **eject button** for five seconds.
The LED on the button flashes alternatively yellow and green.
3. Press the **eject button once** to set the drive into the Fixed-Disk mode
The LED will now flash continuously yellow–green–green.
4. Press the **eject button twice** quickly to confirm the change.

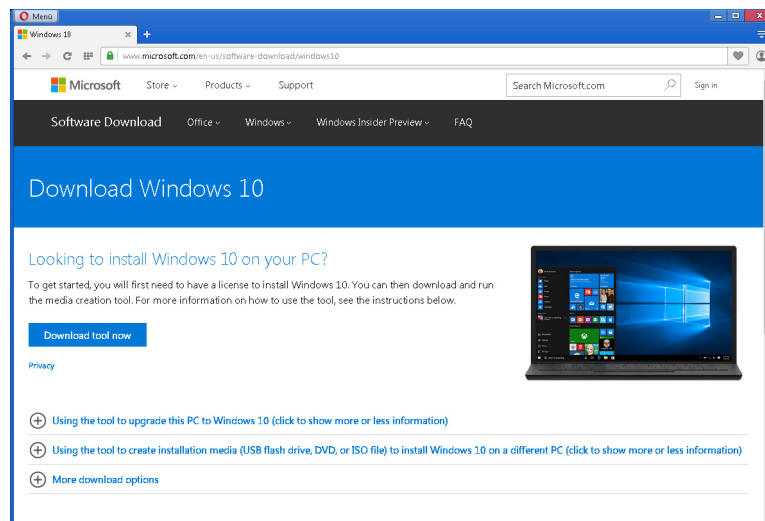
3

Bootable Recovery Cartridge

In case of a total system crash, in addition to the application and user files, the entire operating system needs to be recovered. While this could be done by inserting the Windows startup DVD, a more convenient solution is to create a RDX recovery media which includes a bootable Windows Recovery Environment and the backup files.

Create a Bootable Recovery Cartridge

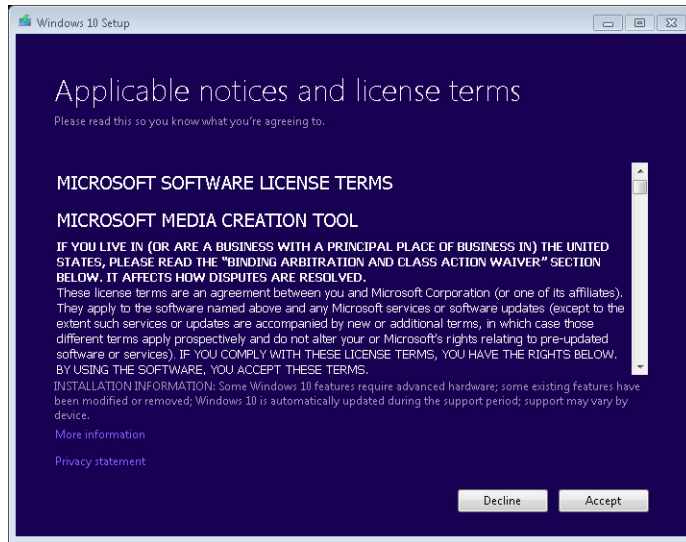
1. Download the Microsoft **Media Creation Tool**.



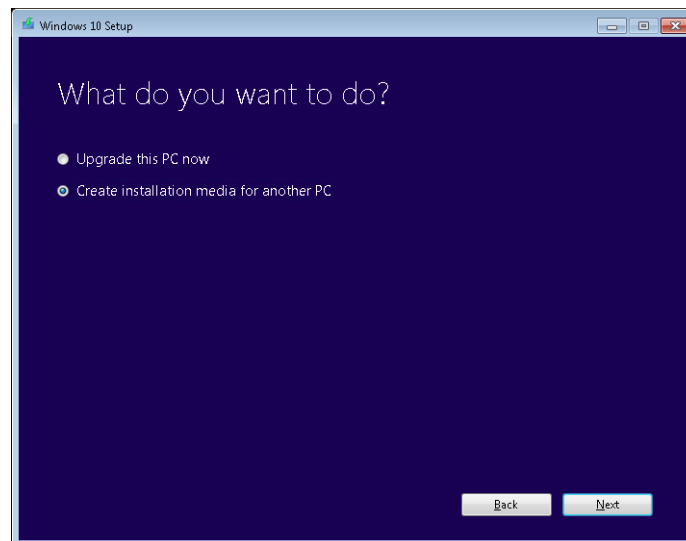
You might use this link:

<https://www.microsoft.com/en-us/software-download/windows10>

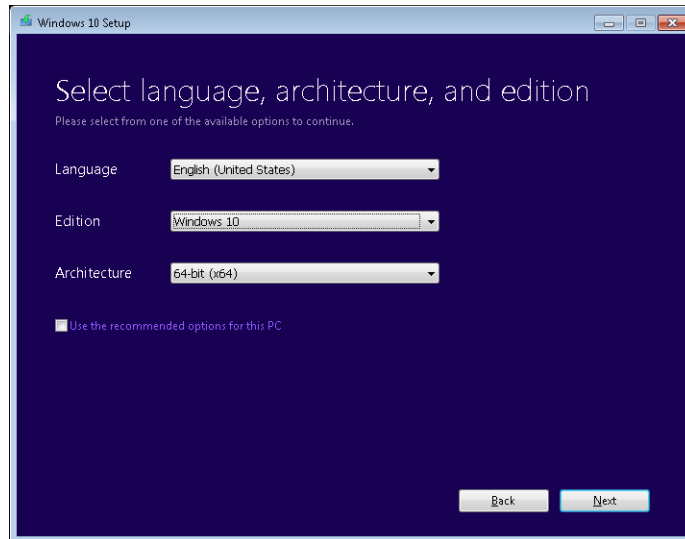
2. Start the Media Creation Tool and accept the license terms.



3. Select Create installation media for another PC and click Next.

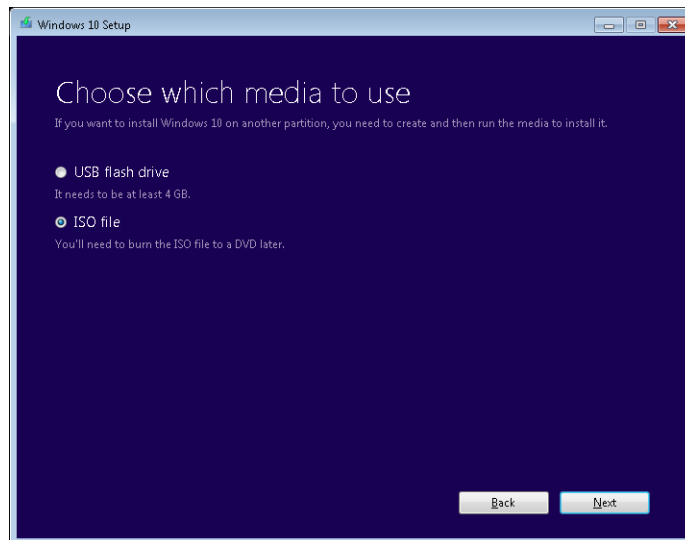


4. Select the appropriate **options** for your system and click **Next**.

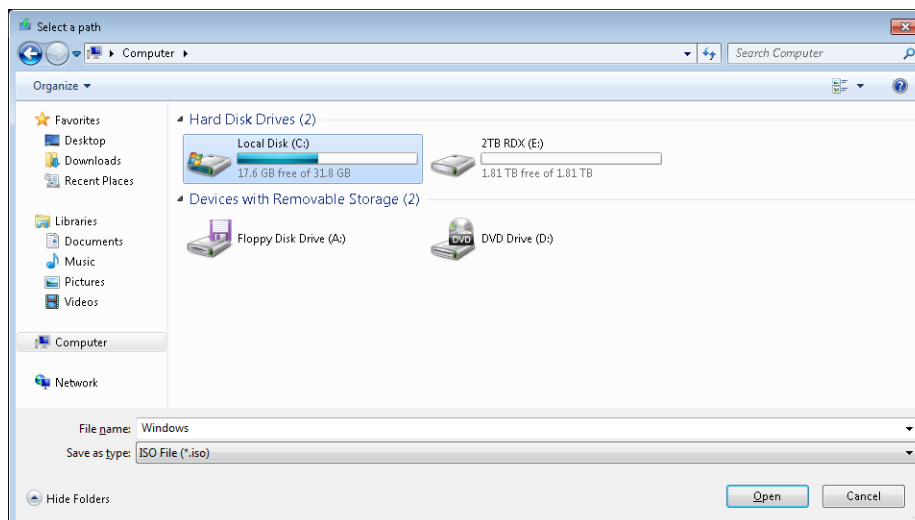


The settings shown on the screenshot might work for most systems.

5. Choose **ISO file** for the media to use and click **Next**.

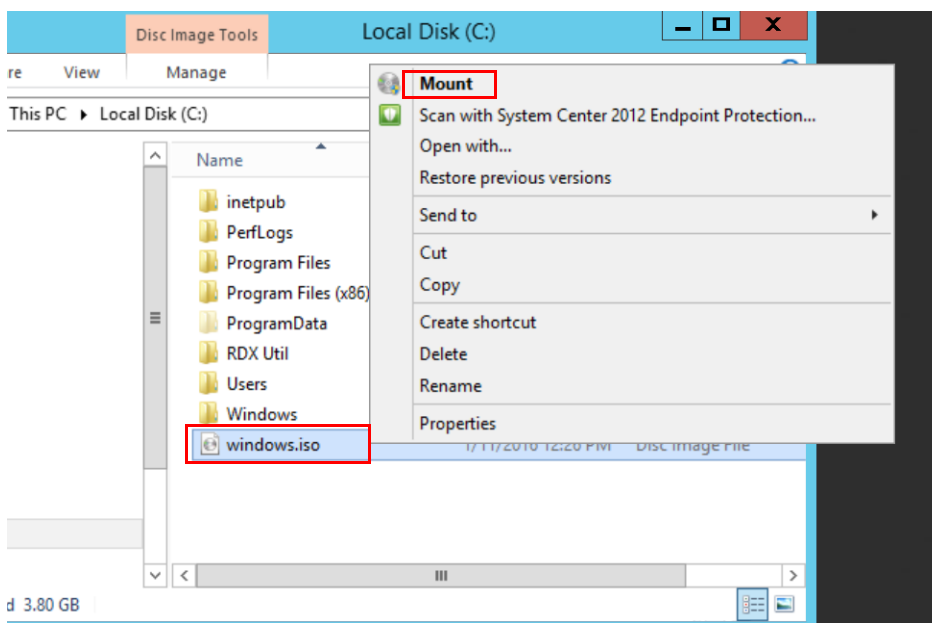


- Specify a destination on your **hard disk** to store the Windows ISO file.



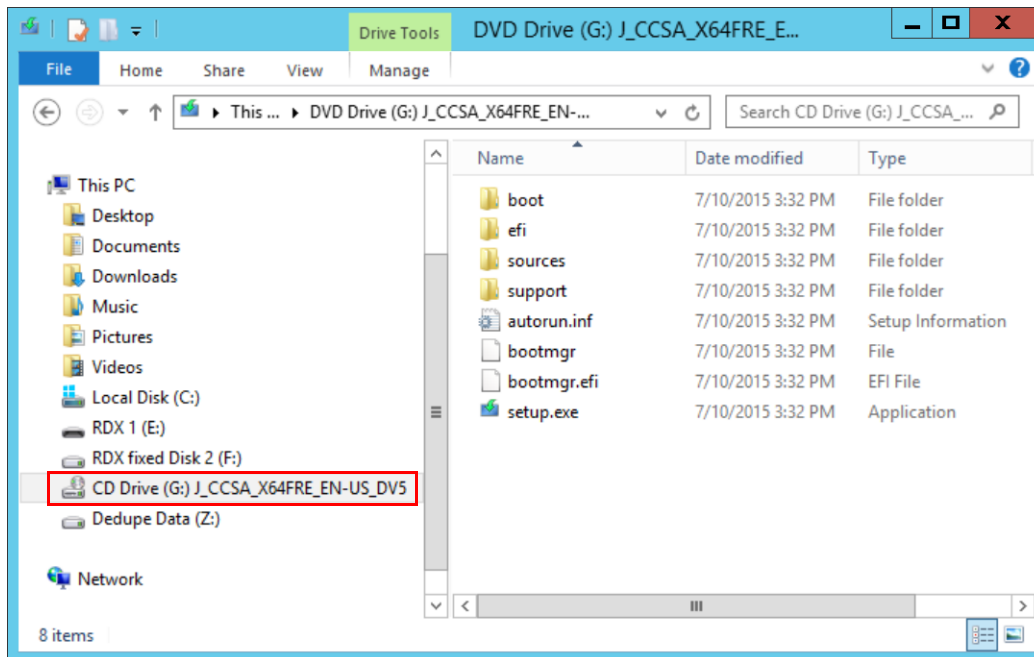
The ISO file starts downloading and might take a while.

- As soon as download has **finished**, click **Next**.
The ISO file is now stored onto the local disk of the server.
- Right-click the ISO file and select **Mount**.



Windows creates a virtual CD drive, which contains the boot files for starting the system and recovery process with the ISO file. You can now use this ISO file to create RDX boot media.

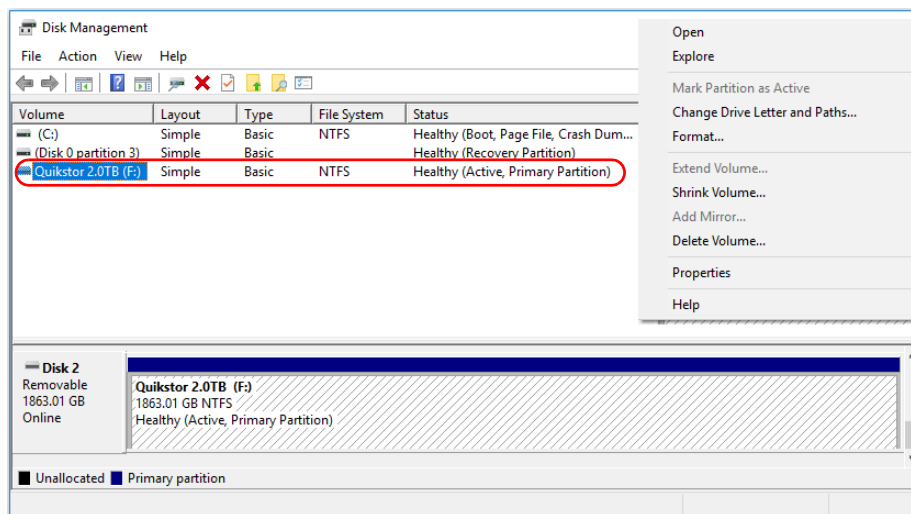
- Copy these **files** to an RDX media with a capacity of 2.0 TB or less.



Verify the RDX Media

Use Windows Disk Management to verify that the RDX media is ready to be used as Boot Media.

1. Right-click the **Start** button and open **Disk Management** to view the system disk storage of the RDX media selected.



2. Verify the following items:
 - The format is **NTFS**.
 - The **Status** shows that the partition is both **Active** and a **Primary Partition**.
 - A **drive letter** (at the end of the volume name) has been assigned.
 - The system BIOS is set to look for a **USB Boot disk** upon startup.

3. If needed, **repartition** the RDX media using the Command Prompt. New, unused media only needs to be set to Active.



CAUTION: ALL your User data will be LOST when the RDX media is repartitioned.

- a. From the Command Prompt (as Administrator), type “**DISKPART**” and press **Enter**.

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.16299.248]
(c) 2017 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>DISKPART
Microsoft DiskPart version 10.0.16299.15
Copyright (C) Microsoft Corporation.
On computer:

DISKPART> list disk

   Disk ###        Status       Size         Free        Dyn  Gpt
   -----        -
   Disk 0          Online            465 GB     1024 KB
   Disk 1          Online            465 GB     1024 KB
   Disk 2          Online            1863 GB          0 B
   Disk 3          No Media             0 B           0 B
   Disk 4          No Media             0 B           0 B

DISKPART> select disk 2
Disk 2 is now the selected disk.

DISKPART> clean
DiskPart succeeded in cleaning the disk.

DISKPART> create partition primary
DiskPart succeeded in creating the specified partition.

DISKPART> active
DiskPart marked the current partition as active.

DISKPART> format fs=ntfs label=Quikstor2.0TB quick
100 percent completed
DiskPart successfully formatted the volume.

DISKPART> assign
DiskPart successfully assigned the drive letter or mount point.

DISKPART> exit
Leaving DiskPart...
C:\WINDOWS\system32>

```

- b. Use following **commands** in the order shown:

<code>DISKPART> list disk</code>	This list shows the disk choices
<code>DISKPART> select disk 2</code>	This selects the RDX QuikStor disk target number 2
<code>DISKPART> clean</code>	This erases the disk target
<code>DISKPART> create partition primary</code>	This creates the partition
<code>DISKPART> active</code>	The boot sector is now active
<code>DISKPART> format fs=ntfs label=Quikstor2.0TB quick</code>	Quick Formats and labels the disk Volume
<code>DISKPART> assign</code>	This assigns the drive letter to the disk Volume
<code>DISKPART> exit</code>	This exits the diskpart tool

- c. Review the RDX media with Windows Disk Manager to confirm you have an **Active** drive with a **Primary Partition**.

The RDX media is now ready for the boot files to be created with the **Media Creation Tool**.

4

Set up Windows Backup

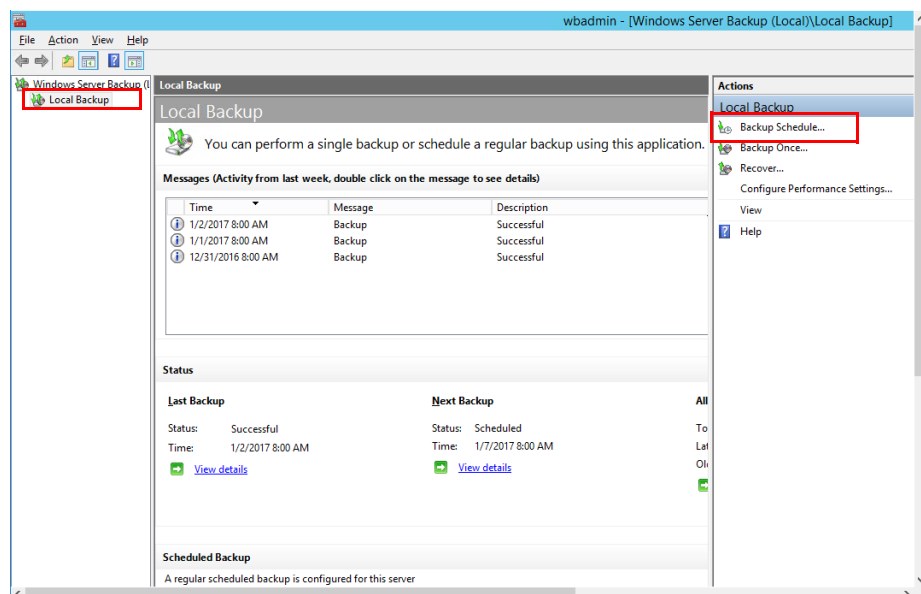
Use Windows Server Backup to configure and schedule backups of your RDX QuikStor.

NOTE: Windows Desktop OS System Image Backup (SIB) solution is deprecated by Microsoft. Microsoft recommends using third-party backup tools to properly backup the RDX QuikStor system. For more information, see:

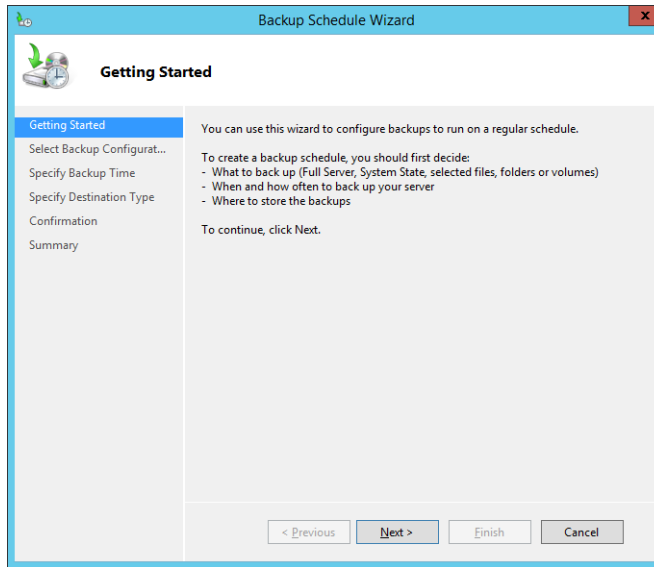
<https://docs.microsoft.com/en-us/windows/deployment/planning/windows-10-1709-removed-features>

Server OS Backup Configuration

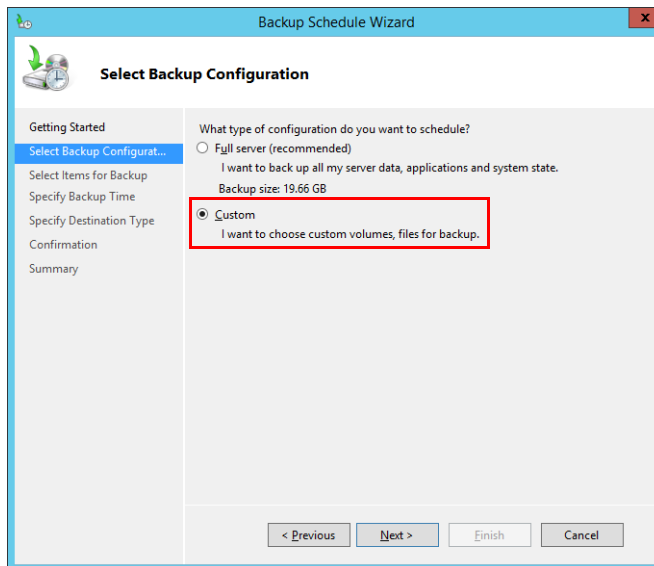
1. From the Windows Start screen, start **Windows Server Backup**.
If you did not install Windows Server Backup, install it first. Press Win + R and type “wbadmin.msc” to open Windows Server Backup. Or, you can click Start, select Administrative Tools, and click Windows Server Backup.
2. With **Local Backup** selected, from the **Actions** area on the right, choose **Backup Schedule**.



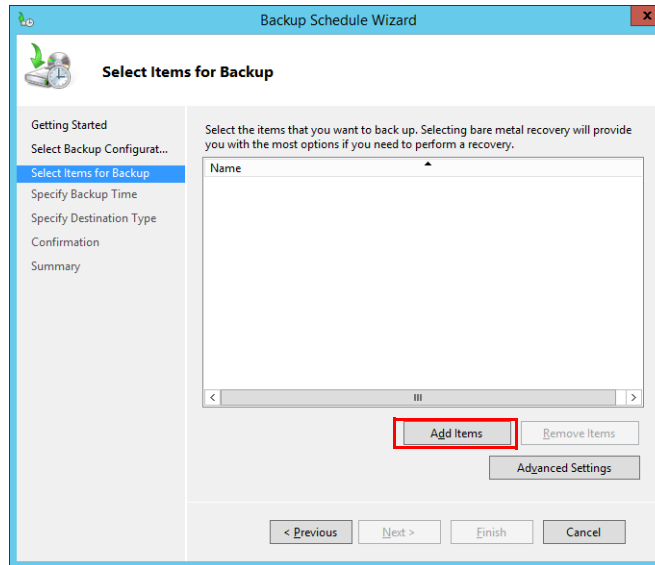
3. At the **Getting Started** window, review the scheduling process and click **Next**.



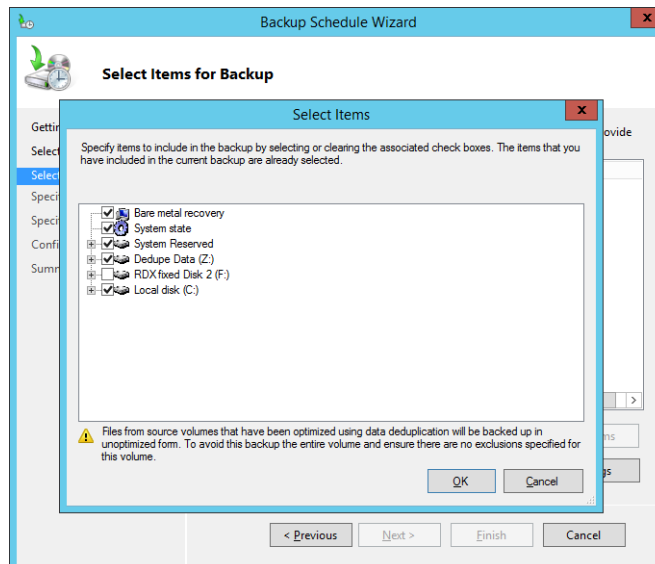
4. At **Select Backup Configuration**, select **Custom** and click **Next**.



- At **Select Items for Backup**, click **Add Items**.



- In the **Select Items** popup, check the **items and drives** you want to back up.

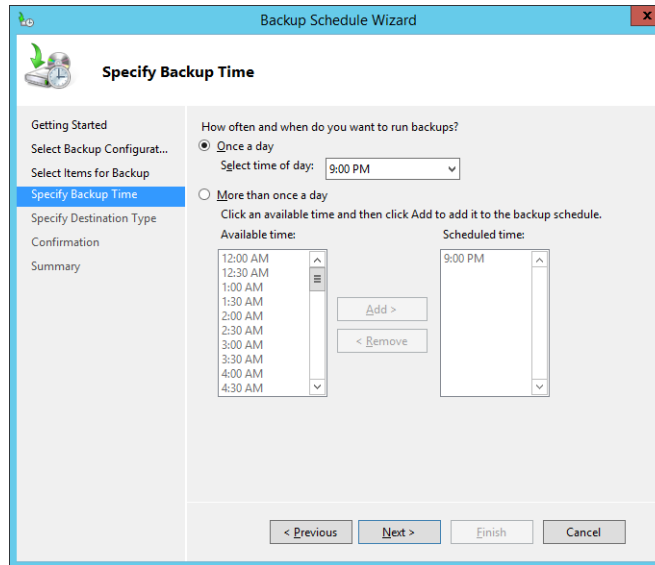


In this example, we selected bare metal recovery to be able to set up our server from scratch in the event of a system crash.

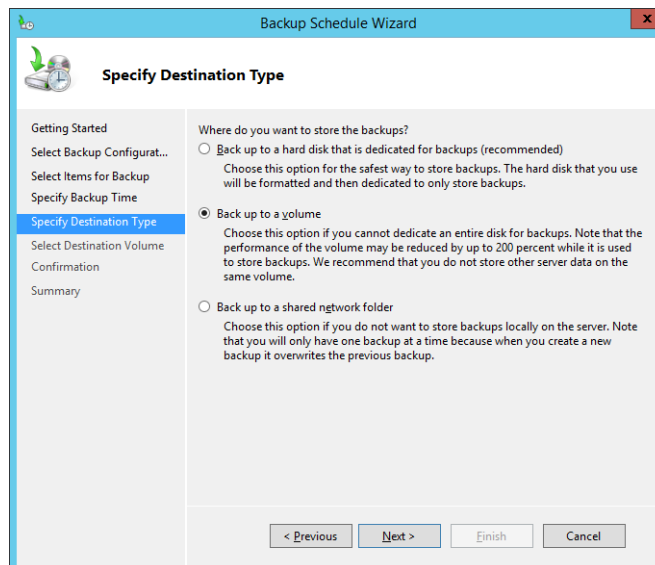
In addition, **System State**, **System Reserved**, and **Local Disk (C:)** is automatically selected. We also selected the **deduplicated volume (Z:)**.

- Click **OK** to accept the selections and click **Next** to continue.

- At **Specify Backup Time**, select on option and click **Next**.

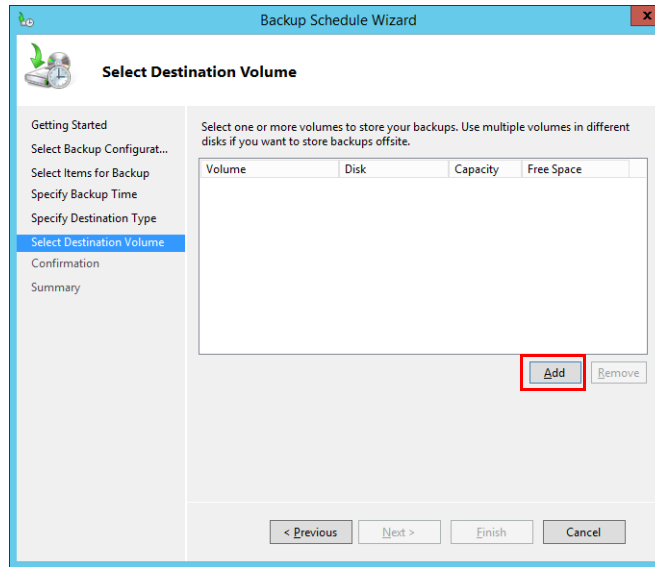


- At **Specify Destination Type**, select either **Back up to a hard disk that is dedicated for backups** or **Back up to a volume**, and click **Next**.

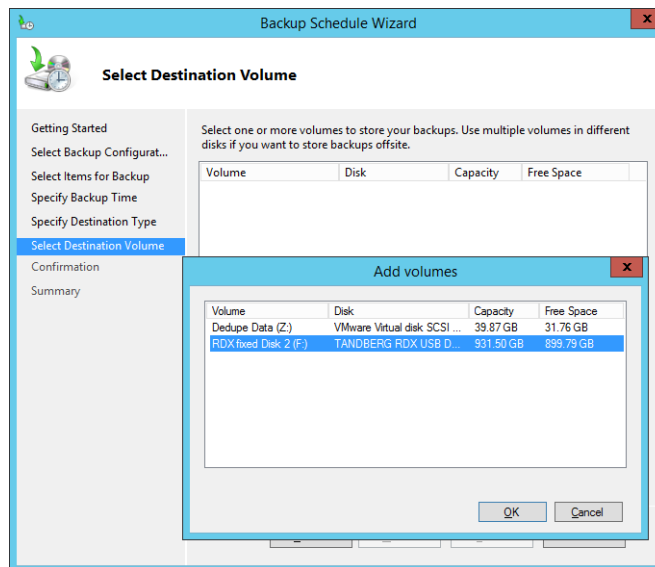


We recommend **Back up to a volume** to keep the drive letter and to be able to display the data.

10. At **Select Destination Volume**, choose your volume:

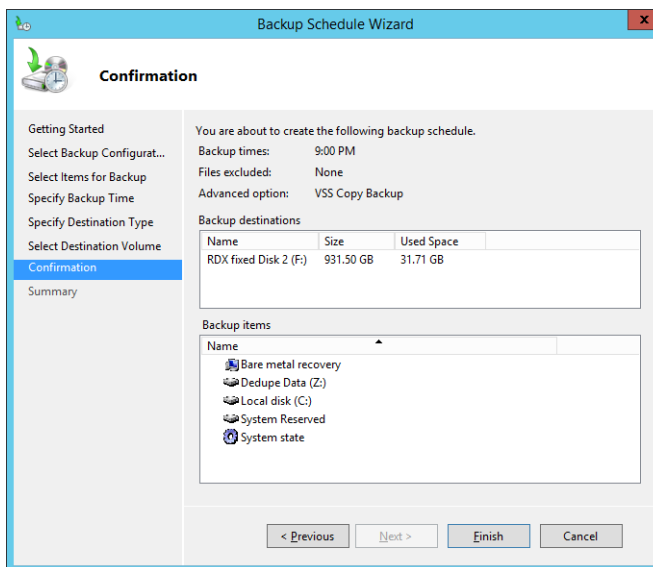


- a. At the **Add Volumes** popup, choose the RDX QuikStor **volume** as the backup destination.

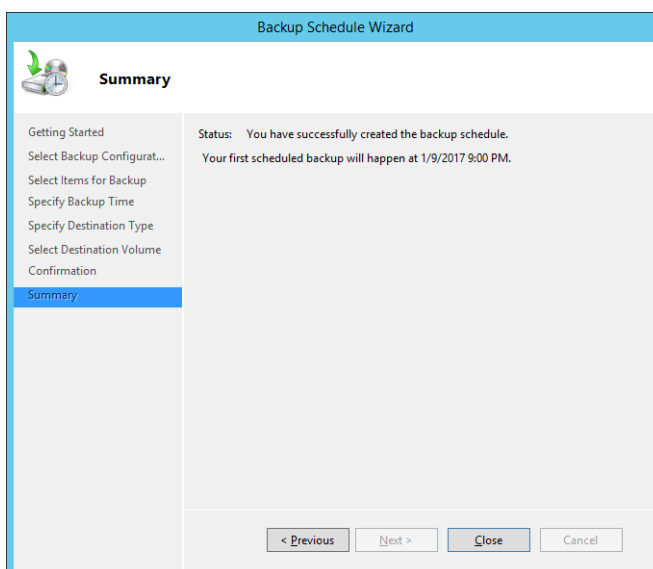


- b. Click **OK**.
- c. Click **Next**.

11. At the **Confirmation** window, click **Finish** to confirm your settings.



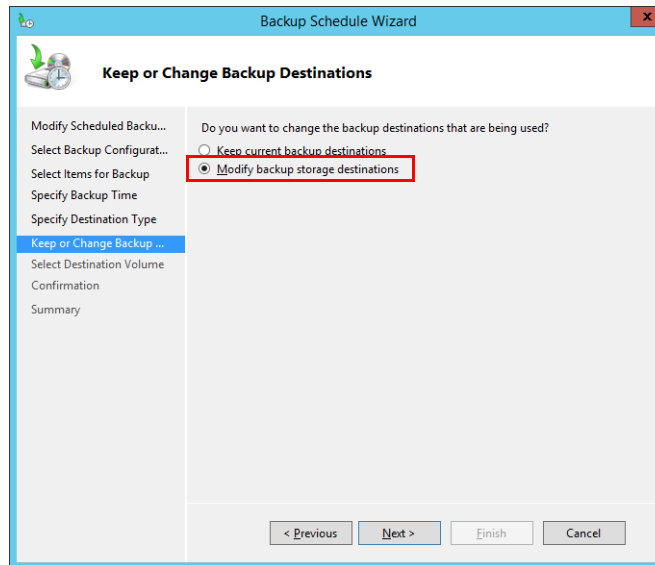
The backup schedule is created and the **Summary** window is displayed acknowledging your settings.



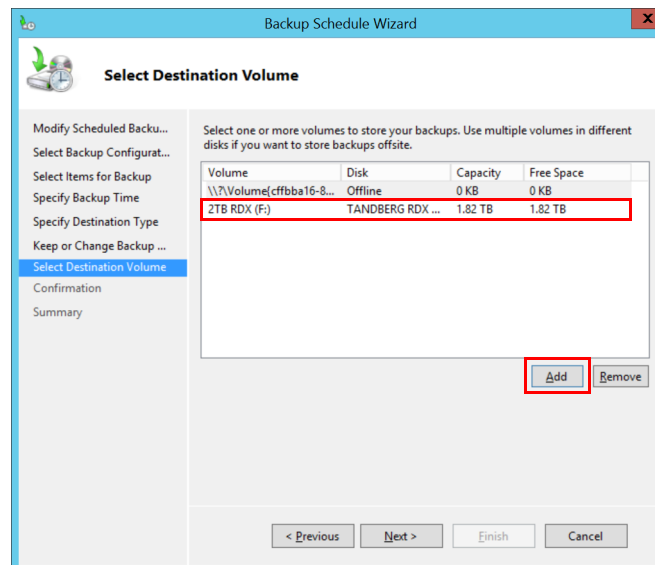
Using Media Rotation

We highly recommend using media rotation to have multiple backup copies and to store at least one copy off-site. For each cartridge you want to include in the rotation, repeat the above steps in [Server OS Backup Configuration](#). Be sure you have inserted the appropriate media into the RDX QuikStor before you start. Also, be aware that there is now an additional step (**Keep or Change Backup Destinations**) that must be configured.

1. While still in the **Backup Schedule Wizard**, at the **Keep or Change Backup Destinations** option, select **Modify backup storage destinations** and click **Next**.



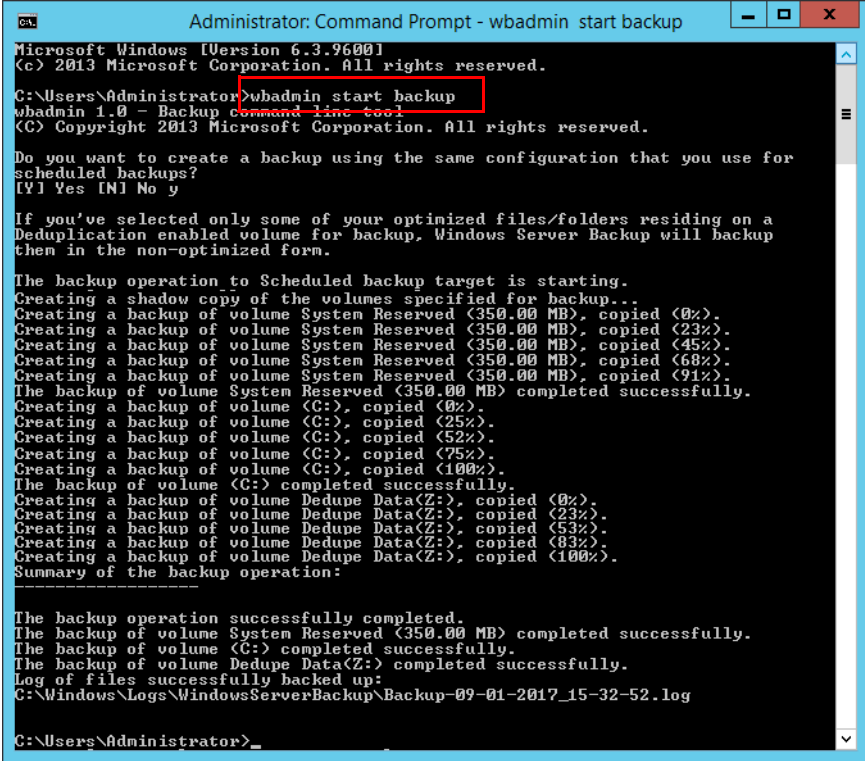
2. At **Select Destination Volume**, choose your RDX QuikStor volume and click **Add**.



3. Proceed through the **remaining screens** accepting defaults until finished.

Running a Backup Outside the Schedule

You can manually run an unscheduled backup by issuing a “`wbadmin start backup`” command in the command line interface.



```
Administrator: Command Prompt - wbadmin start backup
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>wbadmin start backup
wbadmin 1.0 - Backup Command Line Tool
(C) Copyright 2013 Microsoft Corporation. All rights reserved.

Do you want to create a backup using the same configuration that you use for
scheduled backups?
[Y] Yes [N] No y

If you've selected only some of your optimized files/folders residing on a
Deduplication enabled volume for backup, Windows Server Backup will backup
them in the non-optimized form.

The backup operation to Scheduled backup target is starting.
Creating a shadow copy of the volumes specified for backup..
Creating a backup of volume System Reserved (350.00 MB), copied (0%).
Creating a backup of volume System Reserved (350.00 MB), copied (23%).
Creating a backup of volume System Reserved (350.00 MB), copied (45%).
Creating a backup of volume System Reserved (350.00 MB), copied (68%).
Creating a backup of volume System Reserved (350.00 MB), copied (91%).
The backup of volume System Reserved (350.00 MB) completed successfully.
Creating a backup of volume (C:), copied (0%).
Creating a backup of volume (C:), copied (25%).
Creating a backup of volume (C:), copied (52%).
Creating a backup of volume (C:), copied (75%).
Creating a backup of volume (C:), copied (100%).
The backup of volume (C:) completed successfully.
Creating a backup of volume Dedupe Data(Z:), copied (0%).
Creating a backup of volume Dedupe Data(Z:), copied (23%).
Creating a backup of volume Dedupe Data(Z:), copied (53%).
Creating a backup of volume Dedupe Data(Z:), copied (83%).
Creating a backup of volume Dedupe Data(Z:), copied (100%).
Summary of the backup operation:

The backup operation successfully completed.
The backup of volume System Reserved (350.00 MB) completed successfully.
The backup of volume (C:) completed successfully.
The backup of volume Dedupe Data(Z:) completed successfully.
Log of files successfully backed up:
C:\Windows\Logs\WindowsServerBackup\Backup-09-01-2017_15-32-52.log

C:\Users\Administrator>
```

Use BitLocker to Encrypt Your RDX QuikStor

BitLocker is a full volume encryption feature included with Microsoft Windows versions starting with Windows Vista. It is designed to protect data by providing encryption for entire volumes. By default, it uses the AES encryption algorithm in cipher block chaining or XTS mode with a 128-bit or 256-bit key. CBC is not used over the whole disk; it is applied to each individual sector.

When using BitLocker with System Image Backup, it is only necessary to know the key/passphrase. It is recommended that BitLocker be set to auto unlock.


See [Appendix A, “BitLocker Encryption,”](#) for more information.

5

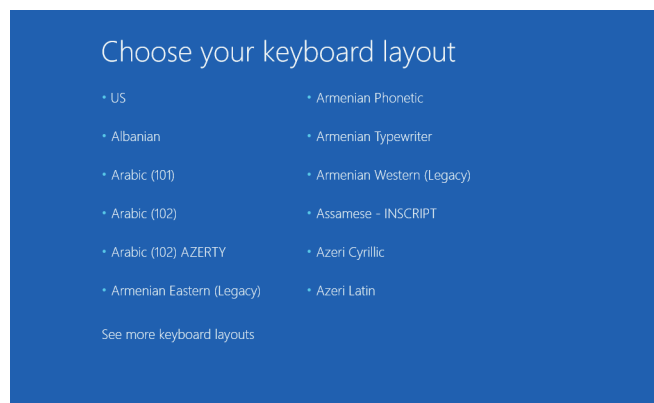
Bare Metal Recovery of a Server

A full server recovery can be done using Bare Metal Recovery (BMR) and Windows Backup.

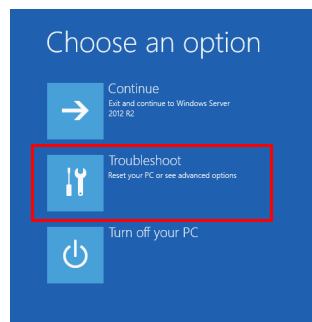
Server Restoration

 **CAUTION:** Verify that the Bare Metal Recovery (BMR) RDX media has the write-protect switch in the On position to prevent infection from the network or server.

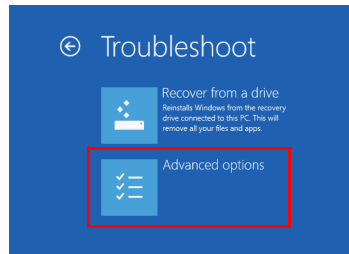
1. Attach a Fixed-Disk Mode RDX QuikStor to the failed server and load the appropriate BMR cartridge with the previously-created system image and the backup files.
2. Power on your **server**.
3. Choose your **keyboard layout** from the ISO file options.



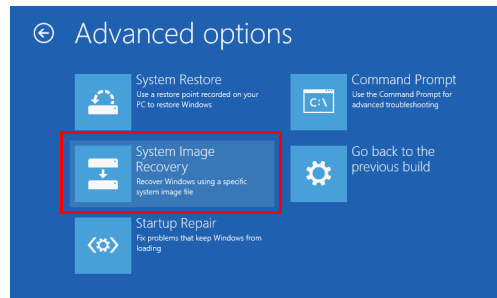
4. After the failed server has booted, choose **Troubleshoot**.



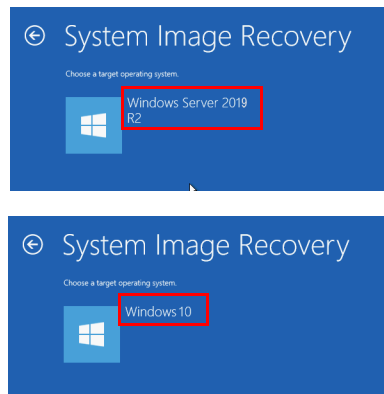
- At the **Troubleshoot** options, choose **Advanced options**.



- At **Advanced options**, choose **System Image Recovery**.

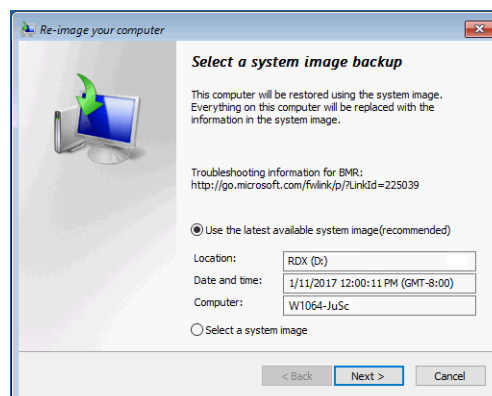


- At **System Image Recovery**, choose the **target operating system**.



For example, for a server you might choose **Windows Server 2019**, and for a desktop you might choose **Windows 10**.

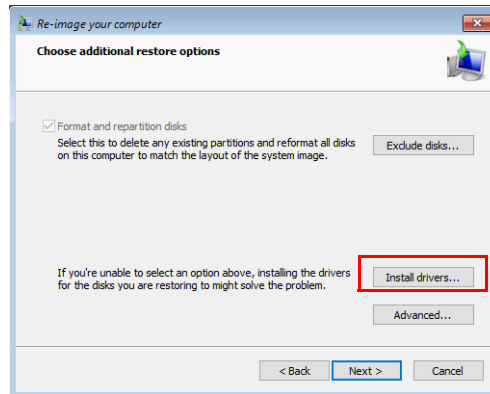
- Once the BMR procedure finds the system images on the RDX QuikStor volume, choose the **appropriate image** and click **Next**.



If you need to recover from a virus or ransomware attack, select a system image which was created before the attack happened.

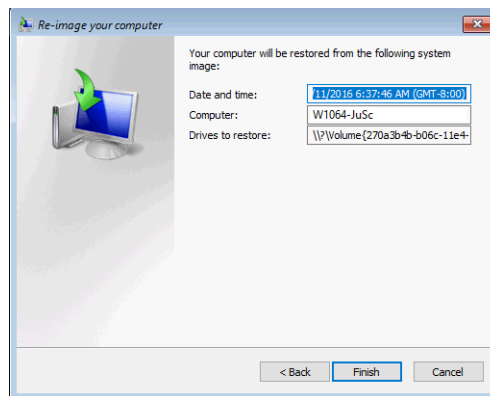
Otherwise, choose **Use the latest available system image**.

9. At the **Choose additional restore options** screen, if you want to install additional drives such as a RAID driver, click **Install Drivers** and follow the instructions.



10. Click **Next** to complete the restore.

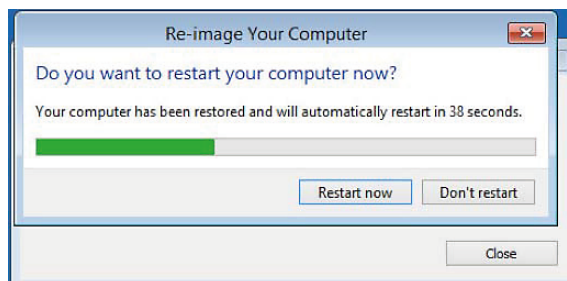
11. At the summary window, click **Finish**.



As the data is restored to the system, a progress bar is displayed.



12. Once the system is restored, it can be restarted by clicking **Restart Now**.



After the restart, your system is up and running. Additional tasks may be performed to complete the recovery.

A

BitLocker Encryption

NOTE: The chapter only applies to systems running a version of Windows server OS.

Data on a lost or stolen computer is vulnerable to unauthorized access, either by running a software-attack tool against it or by transferring the computer's hard disk to a different computer. BitLocker helps mitigate unauthorized data access by enhancing file and system protections. BitLocker also helps render data inaccessible when computers protected by BitLocker are decommissioned or recycled.

There are two additional tools in the Remote Server Administration Tools, which you can use to manage BitLocker.

- **BitLocker Recovery Password Viewer** – This tool enables you to locate and view BitLocker Drive Encryption recovery passwords that have been backed up to Active Directory Domain Services (ADDS). You can use this tool to help recover data that is stored on a drive that has been encrypted by using BitLocker.
- **BitLocker Drive Encryption Tools** – These tools include the command-line tools, `manage-bde` and `repair-bde`, and the BitLocker cmdlets for Windows PowerShell. Both `manage-bde` and the BitLocker cmdlets can be used to perform any task that can be accomplished through the BitLocker control panel, and they are appropriate to use for automated deployments and other scripting scenarios. `Repair-bde` is provided for disaster recovery scenarios in which a BitLocker protected drive cannot be unlocked normally or by using the recovery console.



CAUTION: Because an installed version of Windows is needed to access and decrypt a BitLocker encrypted media, that media cannot be used to do a Bare Metal Restore.

System Requirements

Enabling BitLocker requires that you save a startup key on a removable device, such as a USB flash drive.

The hard disk must be partitioned with at least two drives:

- The operating system drive (or boot drive) contains the operating system and its support files. It must be formatted with the NTFS file system.
- The system drive contains the files that are needed to load Windows after the firmware has prepared the system hardware. BitLocker is not enabled on this drive. For BitLocker to work, the system drive must not be encrypted, must differ from the operating system drive and must be formatted with either the FAT32 file system on computers that use UEFI-based firmware or with the NTFS file system on computers that use BIOS firmware. We recommend that system drive be at least 350 MB in size. After BitLocker is turned on, it should have around 250 MB of free space.

When installing the BitLocker optional component on a server, you will also need to install the Enhanced Storage feature, which is used to support hardware encrypted drives.

Using BitLocker to Encrypt Volumes

BitLocker provides full volume encryption (FVE) for removable data volumes. To support fully encrypted operating system volumes, BitLocker uses an unencrypted system volume for the files required to boot, decrypt, and load the operating system. This volume is automatically created during a new installation of both client and server operating systems.

Encrypting Volumes using the BitLocker Control Panel

Encrypting volumes with the BitLocker control panel is how many users will utilize BitLocker.

1. Click **Start**.
2. Type **bitlocker** in the search box.
3. Click the **Manage BitLocker** option when it is displayed.

The name of the BitLocker control panel is BitLocker Drive Encryption. Only formatted volumes with assigned drive letters will appear properly in the BitLocker control panel applet.

To start encryption for a volume, select Turn on BitLocker for the appropriate drive to initialize the BitLocker Drive Encryption Wizard. BitLocker Drive Encryption Wizard options vary based on volume type (operating system volume or data volume).

Data Volume Encryption

1. Select **Turn on BitLocker** within the control panel to begin the BitLocker Drive Encryption wizard.
2. Select the desired **authentication method** and click **Next**.
 - Password
 - Smart card
 - Automatically unlock this drive
Disabled by default, this option unlocks the data volume without user input when the operating system volume is unlocked.
3. Choose the storage option for the automatically generated **recovery key** and click **Next**.

You should store the recovery key by one of the following ways:

- Printing it.
- Saving it on removable media.
- Saving it as a file in a network folder, on your OneDrive, or on another drive of your computer that you are not encrypting.

You cannot save the recovery key to the root directory of a non-removable drive and cannot be stored on the encrypted volume. You cannot save the recovery key for a removable data drive (such as a USB flash drive) on removable media.

Ideally, you should store the recovery key separate from your computer. After you create a recovery key, you can use the BitLocker control panel to make additional copies.

4. Select an option for **encryption** (used disk space only encryption or full drive encryption).

If the volume being encrypted is new or empty, it is recommended that used space only encryption is selected.

5. At the final confirmation screen, select **Start encrypting** to begin the encryption.

Encryption status displays in the notification area or within the BitLocker control panel.

NOTE: For complete details about using BitLocker to encrypt volumes, refer to <https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-basic-deployment>.

Symbols

> (menu flow indicator) 4

A

alert definitions 4

B

backup scheduling 20
Backup to Cloud vs. RDX QuikStor 8
Backup to External USB Disks vs. RDX QuikStor 8
Backup to NAS vs. RDX QuikStor 9
Backup to Tape vs. RDX QuikStor 9
Bare Metal Recovery (BMR) 28
Bootable Recovery Cartridge 13

C

configure and schedule backups 20
conventions, typographical 4

F

failed server restore 28
Fixed-Disk mode 10, 12

K

Keep or Change Backup Destinations 25

M

manual backup 27
media rotation 25
menu flow indicator 4
Microsoft Media Creation Tool 13

O

organization of this eBook 3

P

product documentation 3

R

RAID driver install during BMR 30
ransomware 30
RDX Manager software 10
RDX QuikStor advantages 7
RDX QuikStor vs. Backup to Cloud 8
RDX QuikStor vs. Backup to External USB Disks 8
RDX QuikStor vs. Backup to NAS 9
RDX QuikStor vs. Backup to Tape 9
RDX QuikStor vs. other solutions 8
RDX recovery cartridge 13

S

server restoration 28
system image on the RDX QuikStor volume 29

T

Technical Support 4
typographical conventions 4

U

unscheduled backup, running 27

V

verify the RDX media 17
virus attack 30

W

Windows Backup Utility 7