NETGEAR®

ReadyRECOVER™
Reviewer's Guide

Table of Contents

NETGEAR® CONTACT INFO

If you have any questions or technical issues, please contact your assigned NETGEAR® contacts for this review listed below.

Matt Pahnke
Senior Product Marketing Manager
Matt.Pahnke@netgear.com

Peter Chen
Senior Technical Marketing Engineer
(408) 890-3182
(408) 921-1689
Peter.Chen@netgear.com

PRODUCT CATEGORY

Switches	Wireless	Storage	Security

OVERVIEW

Thank you for taking the time to evaluate the ground breaking NETGEAR® ReadyRECOVER™. ReadyRECOVER is a complete backup and recovery appliance designed for small and medium-sized business. It is a joint solution between NETGEAR ReadyDATA™ and StorageCraft® ShadowProtect® that takes the unique advantages of each product and combines it into a backup solution with powerful, previously unseen capabilities. 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 independently be used to quickly and reliably restore files, folders or systems to any platform, physical or virtual.

READYRECOVER

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 backup is a space-efficient recovery point that never requires image chain management or consolidation. In addition, each backup captures the entire target system, the Windows operating system, all services, all applications, all settings and all data for fast full system recovery.

The ReadyRECOVER Advantage

- Every backup writes only changed data, forever!
    - ✓ Changes to live data are tracked at the block level
    - ✓ When a backup runs, only blocks of data that have changed since the last job are written
    - ✓ With less data to write for each backup job
    - ✓ Fewer cycles are consumed for maximum processing efficiency
    - ✓ Less capacity is required for maximum storage efficiency
    - ✓ Efficient backups mean lower overall IT costs
- Every backup is verified in real time, forever!
- Every backup is a full restore point, forever!

Solution Components

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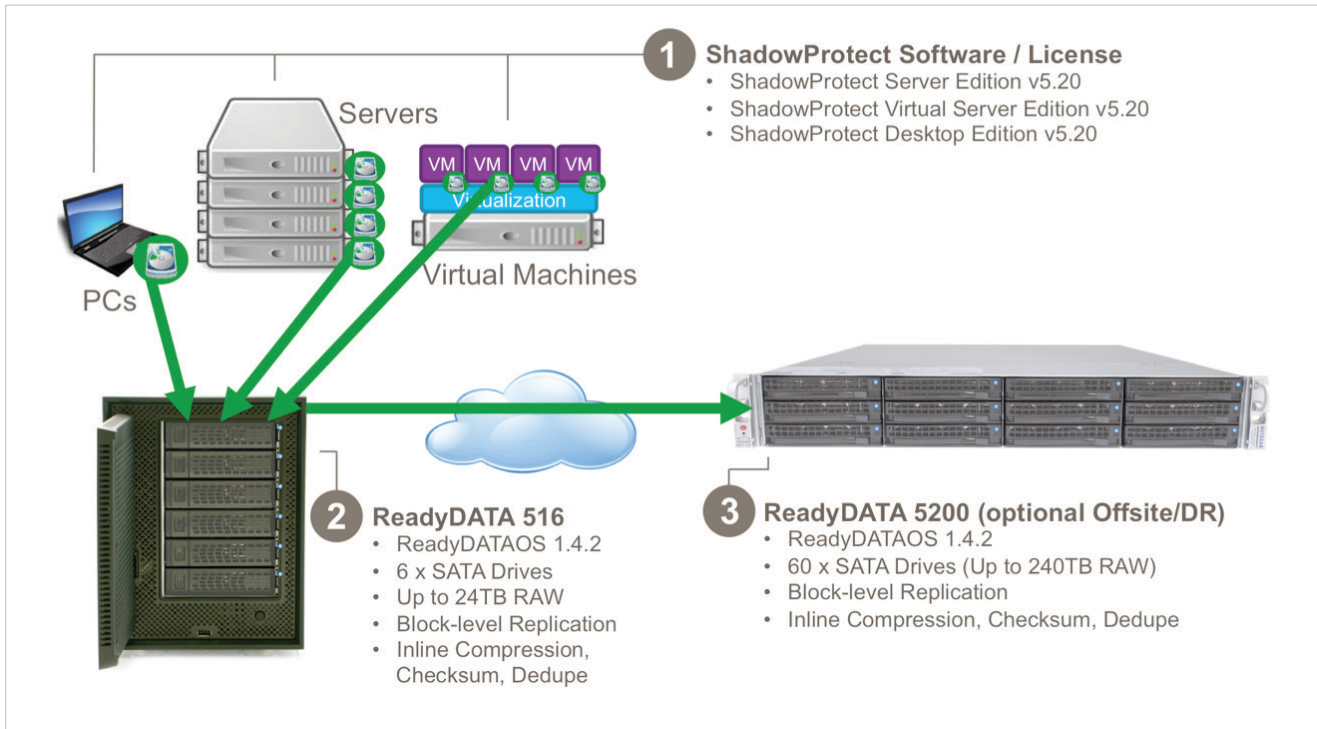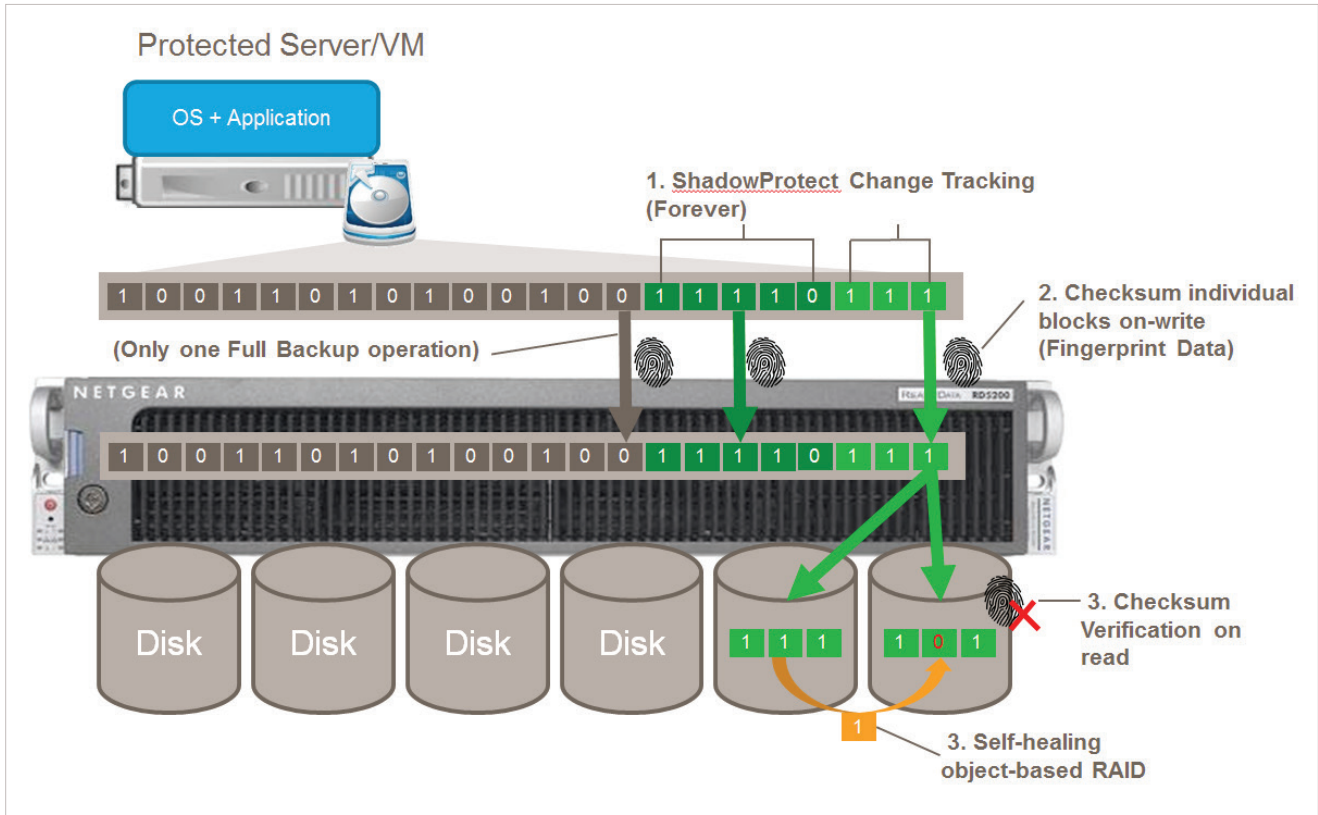

1. StorageCraft ShadowProtect Licenses and Software for each Server, VM, or Workstation to be protected. Minimum ShadowProtect software version must be 5.20.

2. ReadyDATA 5200 or ReadyDATA 516 running firmware ReadyDATAOS 1.4.2 or later with appropriately sized hard drives.

3. [Optional, but highly recommended] A second ReadyDATA in an offsite location for disaster recovery.

ReadyRECOVER Backup and Storage Architecture

ReadyRECOVER combines StorageCraft ShadowProtect backup software and NETGEAR ReadyDATA storage to deliver a unique backup and disaster recovery solution.
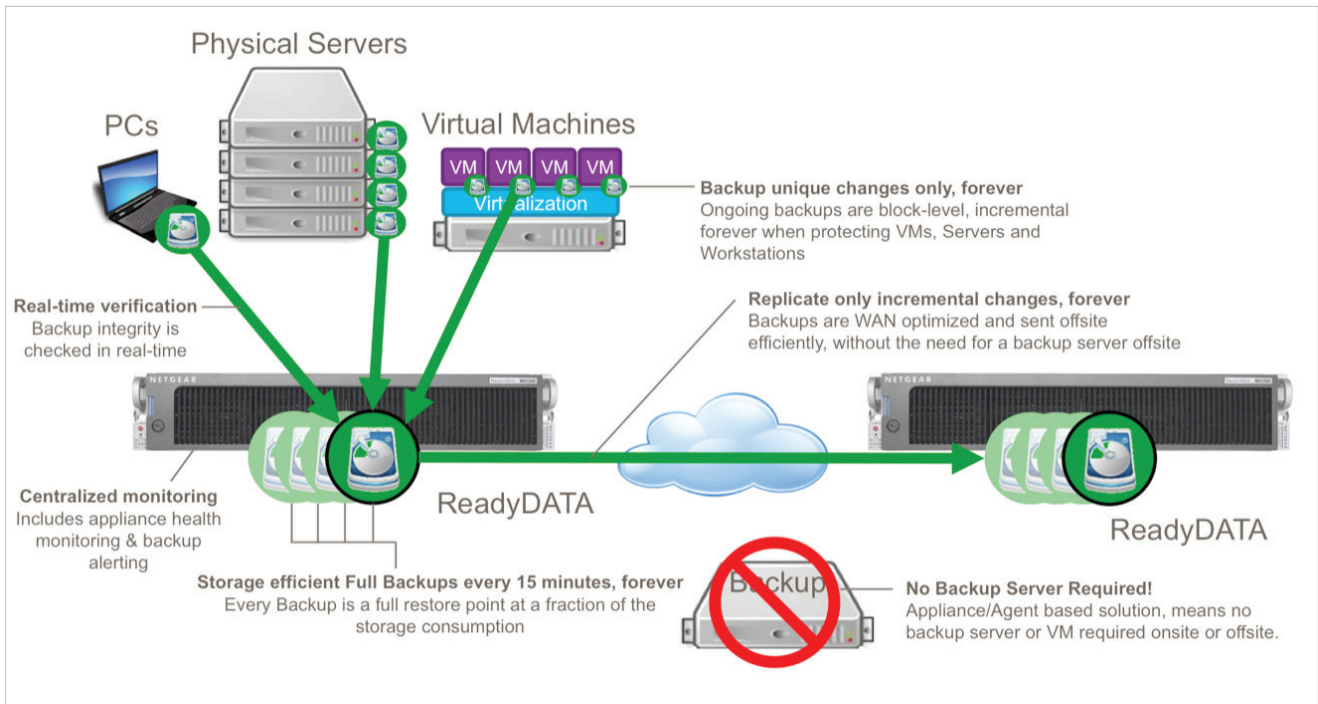
The following page depicts the ReadyRECOVER technical architecture, which shows holistic, end-to-end integrity.

1. The StorageCraft ShadowProtect agent reliably tracks changes on the server/PC.

2. It sends changed data to ReadyDATA, where the data is immediately "fingerprinted" (checksummed) and redundant copies (mirror or parity) are written to ReadyDATA's object-based RAID.

3. The ShadowProtect agent reads data from ReadyDATA. Before the data is given to the agent, ReadyDATA confirms that the data is valid using the fingerprint (checksum). If the checksum proves the data to be valid, it is sent to the agent, which can trust the validity of the data. If the fingerprint (checksum) shows the data to be invalid, ReadyDATA automatically heals the data by using an alternate copy from one of the other disks in the system.

Protected Server/VM

OS + Application

1. ShadowProtect Change Tracking (Forever)

1 0 0 1 1 0 1 0 1 0 0 1 0 0 1 1 1 1 0 1 1 1

(Only one Full Backup operation)

2. Checksum individual blocks on-write (Fingerprint Data)

1 0 0 1 1 0 1 0 1 0 1 0 0 1 0 0 1 1 1 1 0 1 1 1

Disk   Disk   Disk   Disk   1 1 1   1 0 1

3. Checksum Verification on read

3. Self-healing object-based RAID

ReadyRECOVER Backup and Storage Architecture

Below is a diagram of the backup architecture for ReadyRECOVER.

Physical Servers

PCs

Virtual Machines

Backup unique changes only, forever
Ongoing backups are block-level, incremental forever when protecting VMs, Servers and Workstations

Real-time verification
Backup integrity is checked in real-time

Replicate only incremental changes, forever
Backups are WAN optimized and sent offsite efficiently, without the need for a backup server offsite

Centralized monitoring
Includes appliance health monitoring & backup alerting

ReadyDATA

ReadyDATA

Storage efficient Full Backups every 15 minutes, forever
Every Backup is a full restore point at a fraction of the storage consumption

No Backup Server Required!
Appliance/Agent based solution, means no backup server or VM required onsite or offsite.

To address common backup challenges, ReadyRECOVER offers:

1. Fast and frequent backups, using block-level incremental forever technology. After the first full backup, never again run a slow running full backup. Most backup software claims to include incremental forever technology, but do not truly deliver on "forever" and often require monthly or yearly full backups, with incremental backups in between.

2. Real-time verification on write, so that backups can run around the clock without the need for verification jobs or maintenance operations.

3. Centralized monitoring and alerting of backup tasks, agent health, storage consumption, and RAID/disk state.

4. WAN optimized replication means only unique backup data is ever replicated, delivering significant bandwidth savings.

5. Support for Windows-based Servers, Virtual Machines, Workstations and Laptops with support for all major Virtualization platforms including VMware, Hyper-V and XenServer. (**Note**: Guest OS must be Microsoft Windows, for more information visit http://www.netgear.com/ReadyRECOVER)

The ReadyRECOVER Restoration options
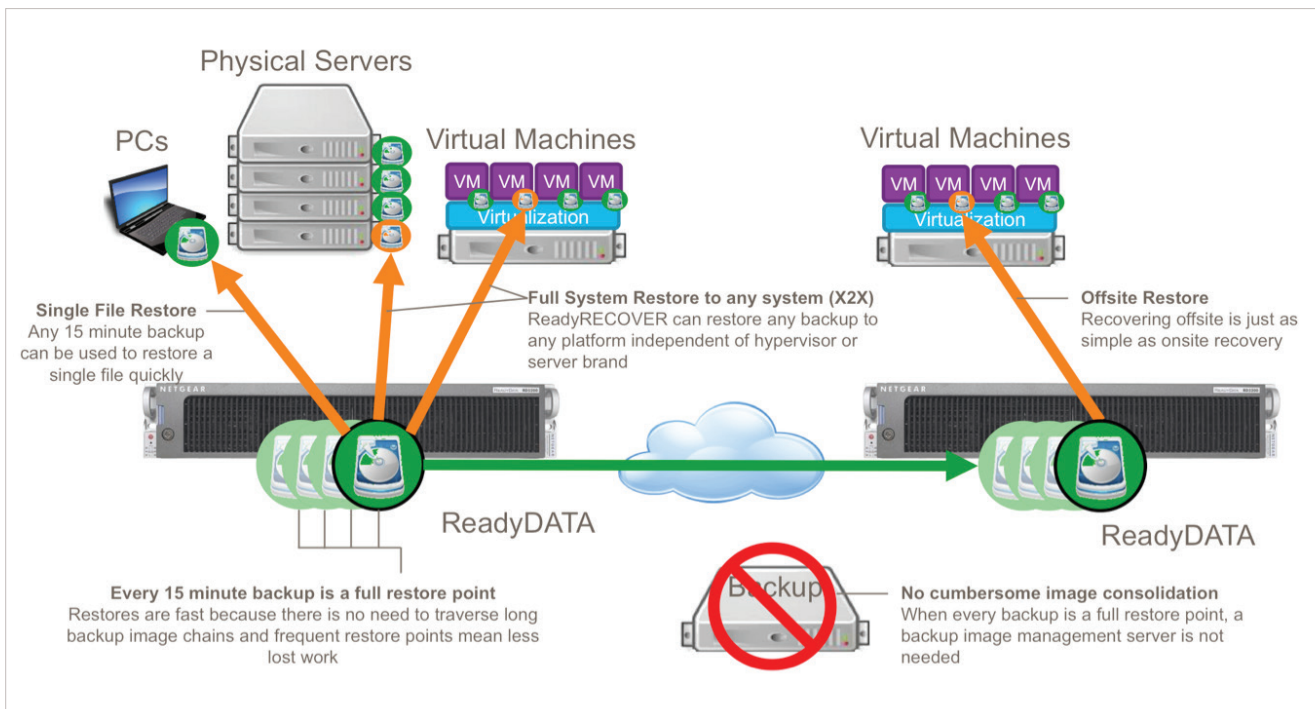
Restoration is the single most important part of any Backup and Disaster Recovery solution. For this reason, ReadyRECOVER focuses on real-world needs in a disaster situation, including:

1. **Single File Restore** – Any 15 minute backup can be mounted instantly and recovery of individual files.This capability means users don't have to wait to get important files or application data back in the event of corruption or human error.

2. **Hardware Independent Restore (HIR)** – Operating systems and applications can be restored onsite or offsite. More importantly, full systems can be restored to any hardware or virtualization platform (P2V, V2P, P2P, V2V) available at the time of disaster.

Block-level Deduplication & Inline Compression Savings

ReadyRECOVER employs a unique technique to deliver storage efficiency that saves space on disk and reduces bandwidth consumption when replicating backups offsite. These efficiencies are delivered by three complementary techniques:

1. **Change Tracking (Forever)**: Only newly changes blocks ever need to be send from the source system (backup client) to the ReadyDATA onsite or the ReadyDATA offsite
2. **Block-level Deduplication**: When each full backup image is written, common blocks from previous backups are not stored twice. Because only unique blocks are written, many independent full backup images can be stored, while minimizing capacity consumption.
3. **Inline Compression**: As data is written to ReadyDATA, it is compressed and checksummed in real-time.

Deduplication of backup data requires end-to-end data integrity at a block level because many backups may reference the same block. In ReadyRECOVER, inline checksumming is implemented to guarantee every block is correct when restoring. If a block is corrupt, it is silently repaired using checksums and object-based RAID technology built into ReadyDATA.

- **Reliable change tracking**: The StorageCraft backup agent (called ShadowProtect), can reliably track incremental sector changes on servers and PCs. StorageCraft started as a storage driver vendor in 2004. It has since created backup software with deep VSS integration and sector level change tracking using a Microsoft-certified driver in the Windows I/O stack. Every piece of data written (saved) on a PC or Server must pass through the StorageCraft driver, allowing it to track every change.
- **Data integrity forever**: ReadyDATA employs a next-generation file system that checksums all data inline. When new backup data is written, it is checksummed at the block level. When that data is read (for recovery), the checksum is verified. If the checksum indicates an issue, ReadyDATA uses self-healing RAID technology (object based RAID) to find a copy of the same data elsewhere on disk and repair the broken copy.
    - All storage devices that use RAID keep redundant data (extra copies) on disk. However, most of these devices do not checksum data and are unable to tell if the data being read back is valid. Additionally, they are unable to heal corrupted data.

For more information on ReadyDATA and ReadyRECOVER please visit:
http://www.netgear.com/business/products/storage/readydata/ and
http://www.netgear.com/business/products/storage/readydata/readyrecover.aspx

LICENSES

ReadyRECOVER is licensed per machine/VM. There are four types of ReadyRECOVER licenses depending on the type of machine you are trying to backup. Keep in mind you will also need ReadyDATA hardware and drives for ReadyRECOVER to work.

SKU	Product Name	Street Price (USD)
RRSERV01-10000S	Server Protection License	$979.99
RRVIRT01-10000S	Virtual Server Protection License	$369.99
RRSB01-10000S	Windows Small Business Server Protection License	$499.99
RRDESK01-10000S	PC & Desktop Protection License	$94.99
RRGRE01-10000S	ReadyRECOVER Granular Restore for Exchange License	$1799.99

TESTING & DEPLOYMENT

Implementation Steps:

To successfully deploy ReadyRECOVER, complete the following steps:

1. Configure ReadyDATA
2. Install ShadowProtect Backup Agent on clients systems
3. Create a backup job
4. Replicate backup data offsite for Disaster Recovery [Optional]

Configure ReadyDATA

The following high-level steps are required to deploy ReadyDATA in a supported ReadyRECOVER configuration. Following these steps will ensure the best possible results when deploying ReadyRECOVER.

1. Connect to ReadyDATA
2. Create a volume for hosting backup data
3. Configure Networking & Set Hostname

4. Change Default Admin password (Mandatory for successful backups)
5. Configure Email Alerting

Detailed information about installing the ReadyDATA 5200 and 516 can be 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.

1. Connecting to ReadyDATA

ReadyDATA is fully administrable from a supported web browser. When ReadyDATA is powered on for the first time, all network interfaces will be set to DHCP to allow the system to obtain a valid IP address on the network. To discover the system IP address, check the DHCP logs on your DHCP server or download and run the NETGEAR "RAIDar" discovery utility. RAIDar can be downloaded at http://kb.netgear.com/app/answers/detail/a_id/20684/~/readynas-downloads.

Once the IP address is discovered, simply enter it into the address bar of a supported browser. The default username and password are "**admin**" and "**password**".

2. Create a volume for hosting backup data

ReadyDATA supports RAID levels 0, 1, 5, 6, 10, 50, and 60. For ReadyRECOVER configurations, it is recommend to use RAID5 for less than six disks configuration and RAID50 (medium performance profile) configurations in six disk solutions and larger.
In environments with large numbers of clients and where replication will be used, it is recommended to use RAID50.
To create the perform the following steps from the admin UI
1. Select the "**System**" Tab, then select "**Storage**"
2. Select all the drives you would like to include in the volume and click "**Create**"
3. Enter a name for the Volume, for example 'Backup'
4. Select Protection level, for example "RAID5" (**Note:** this will lead to RAID50 options) and click "**Create**"
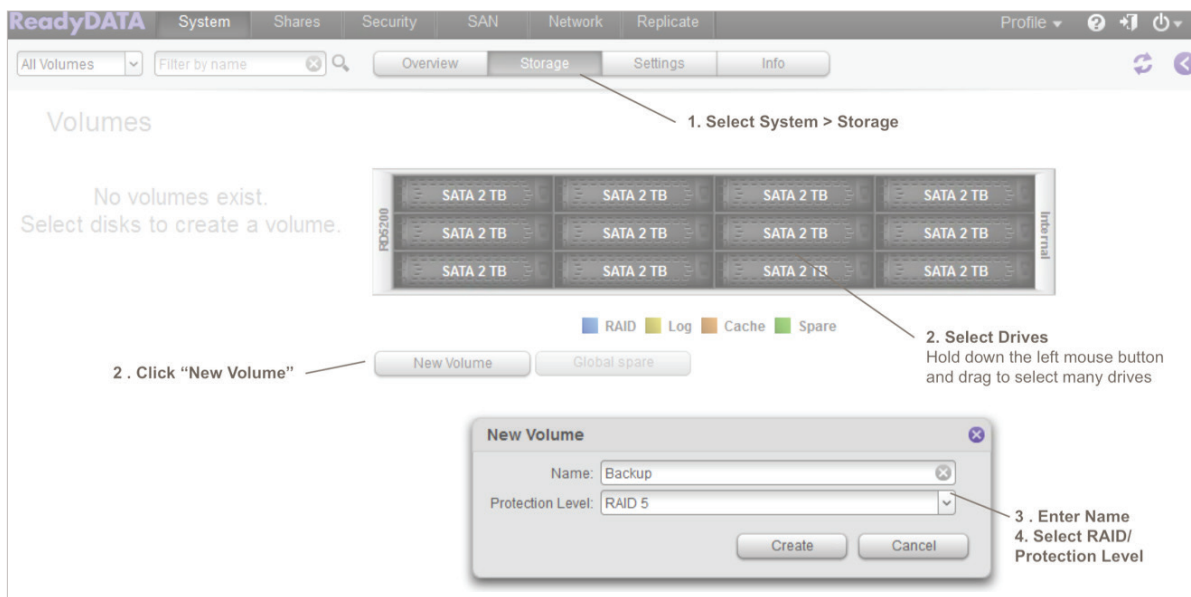
When selecting six or more drives, you will be prompted with multiple performance options. Selecting medium performance is recommended for ReadyRECOVER installations.
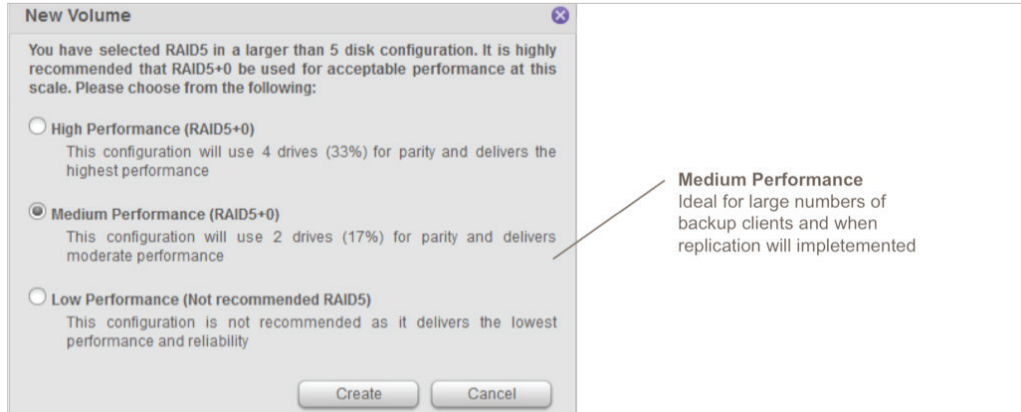
The new volume will be created instantly and is ready to store backups immediately. The ReadyDATA object-based RAID technology eliminates the need to format the drives and create parity at the time of volume creation. Parity is generated in real-time when backups are written to the system, which allows for instant volume creation. More importantly, object-based RAID silently repairs corrupted blocks in the event of on-disk corruption.
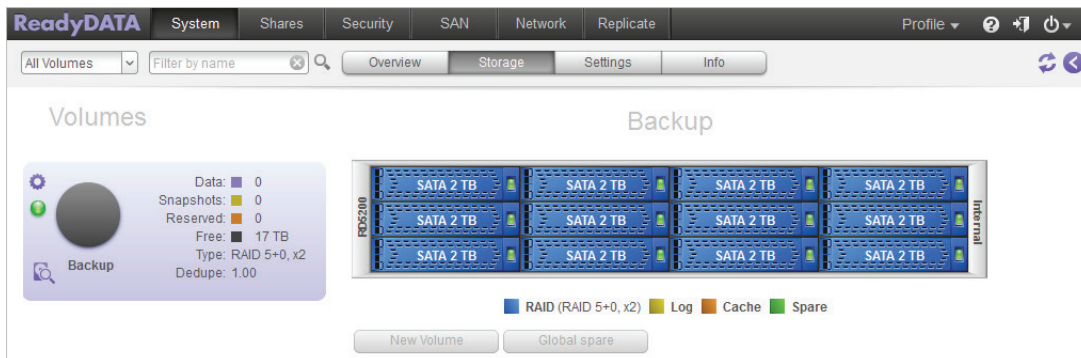
3. ReadyDATA Networking & Set Hostname

Network settings can be changed by logging into the administration console and selecting the "Network" tab. It is recommended that ReadyDATA be connected to the physical network using bonding (LACP) to ensure a reliable and durable connection for ongoing backups.

At a minimum, set a static IP address along with a valid subnet and gateway address so client systems always route to the same location.
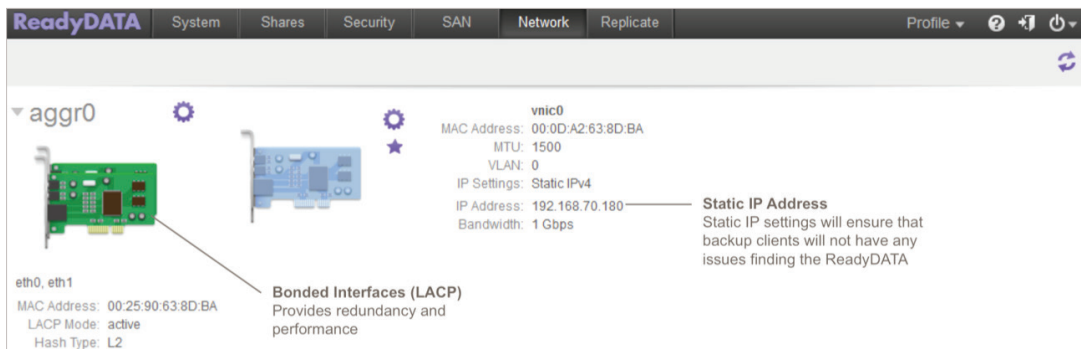
Note: LACP must be supported and configured on the attached switch before enabling bonding on ReadyDATA. Failure to configure switching correctly can cause the ReadyDATA device to become disconnected from the network.

Ensure that the time is set correctly on the ReadyDATA device and that the hostname is unique and recognizable for logging and alerting purposes. To do so:

1. Select the "**System**" Tab, then select the "**Overview**" tab
2. Click on the settings cog
3. Enter a new Hostname, for example "OnsiteB2D"
4. [Optional] If the time is incorrect, select the "**clock**" icon to update time and time zone settings
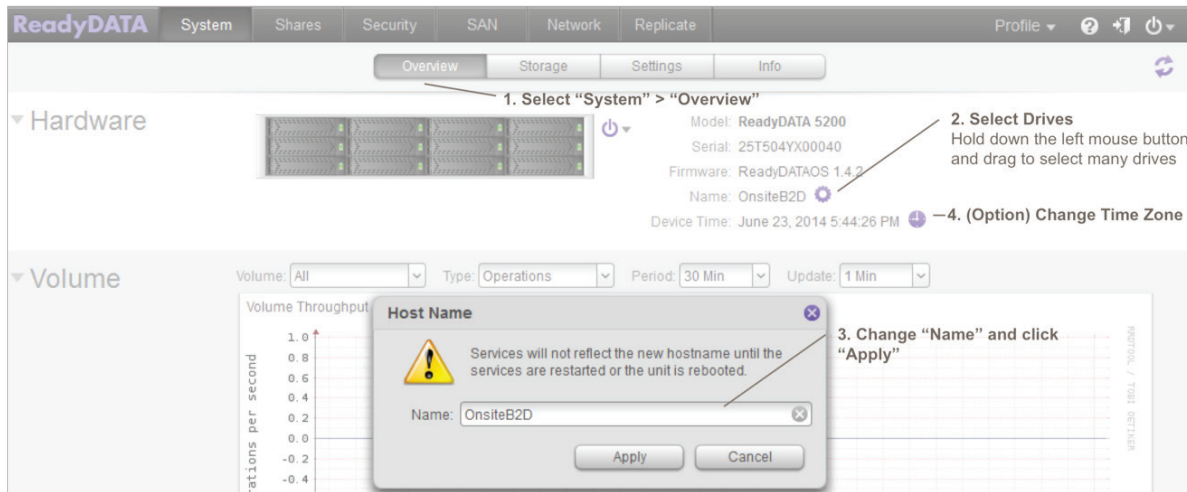
4. Change Admin Password (mandatory for successful backups)

In general, it is highly recommended that you change your admin password on ReadyDATA before storing any data on the system. In the case of ReadyRECOVER, it is mandatory to change the password before backup clients can successfully backup to the system.

To change the admin password:

1. Click on the "**Profile**" menu on the top right of the administration console
2. Select "**Change Admin Password**"
3. Complete the form with a new admin password and recovery question/answers

5. Configure Email Alerting

To receive email alerts about ReadyRECOVER backup client failures, hardware status, and storage volume health from the ReadyDATA device, email alerting must be configured. To enable email alerting:

1. Click "**System**" and then "**Settings**"
2. In the Alerts sections, click to "**+**" button to add an email recipient
3. Fill out SMTP settings with valid settings from your mail server/service
4. Click the "**Apply**" button
5. Click "**Send Test Message**" and verify
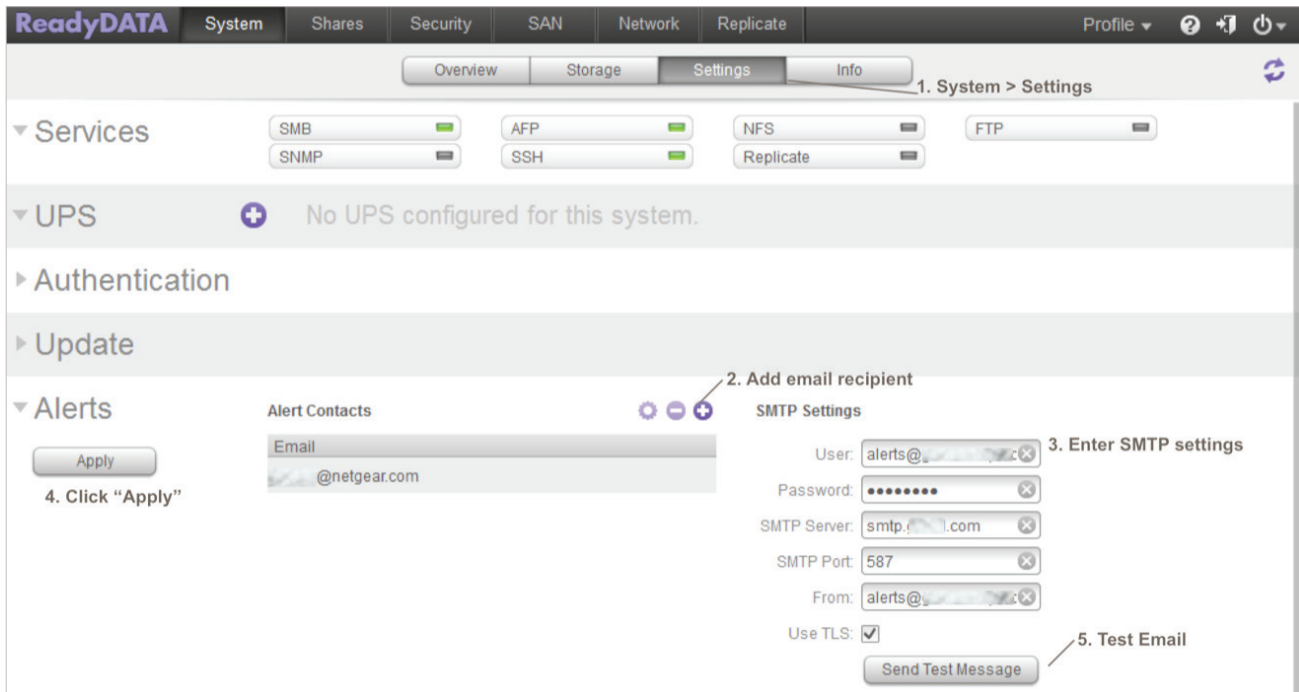
Congratulations! Your ReadyDATA is ready to receive ReadyRECOVER backups from clients on the network.

Install ShadowProtect Backup Agent on clients systems

Before you can configure backup on any Microsoft Windows-based system, you must install the ShadowProtect agent. The agent can be downloaded from the NETGEAR ReadyRECOVER product page at: http://www.netgear.com/readyrecover. Once the agent is installed, the client system will need to be rebooted.

Create a backup job

From the Windows start menu, select "**ShadowProtect**". To create a backup job, click "**Create a job**" and the backup wizard will begin.
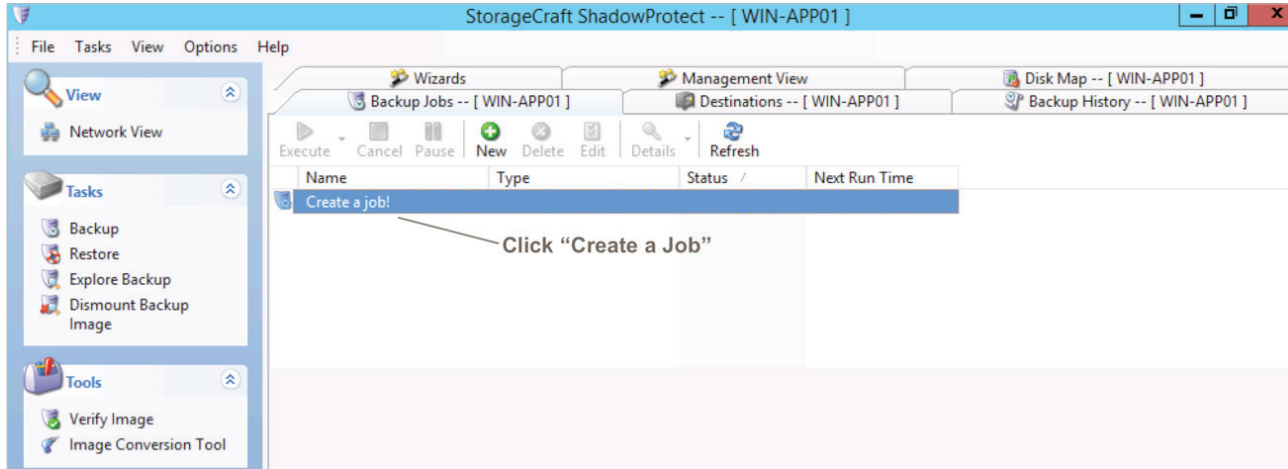
Click "**Next**" to start the Backup Wizard
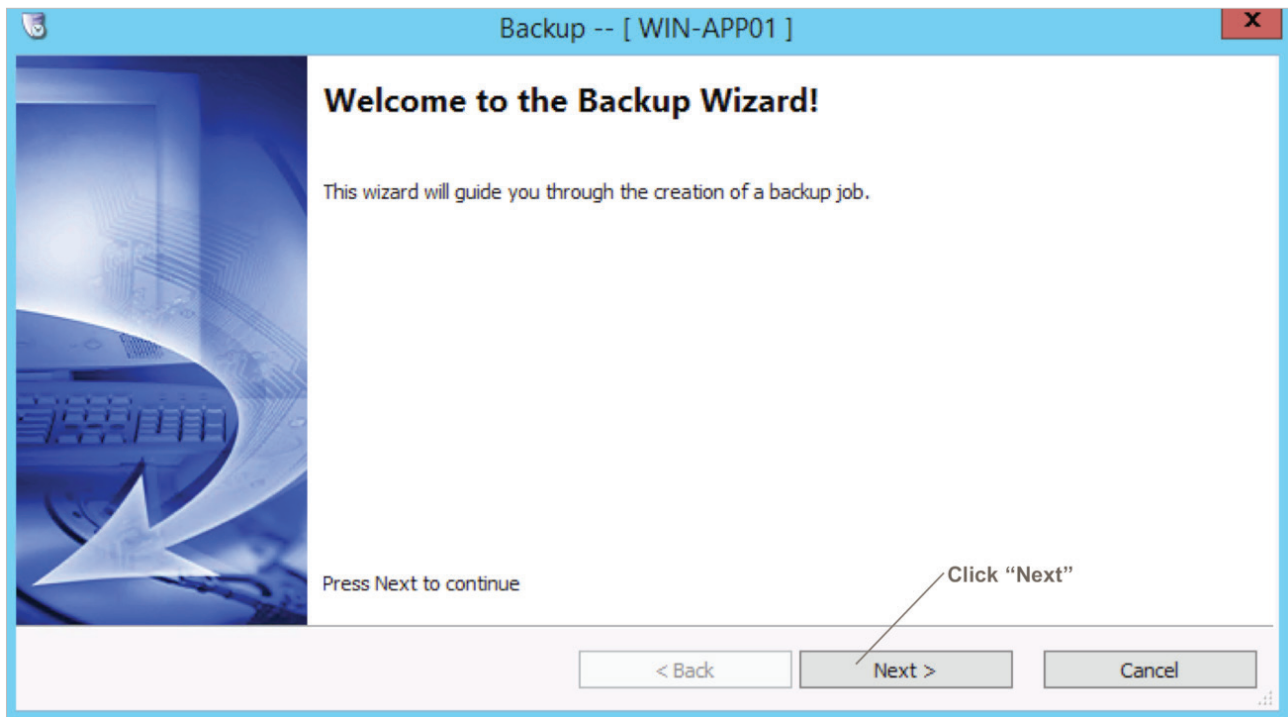
From the volume list, select the volumes you would like to protect. Typically, the volumes with assigned drive letters are all that are required.
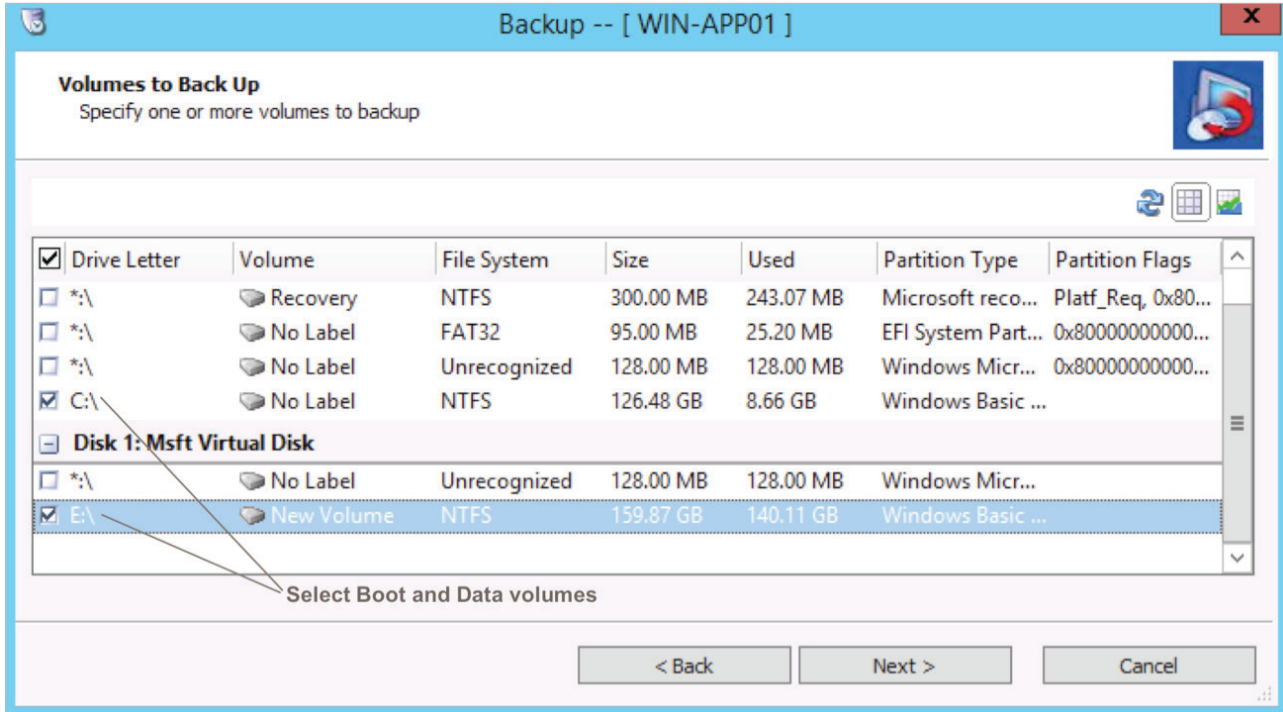
From the dropdown list, choose "**Network Locations**" (**Note:** do not click "Browse…")

![NETGEAR ReadyRECOVER]
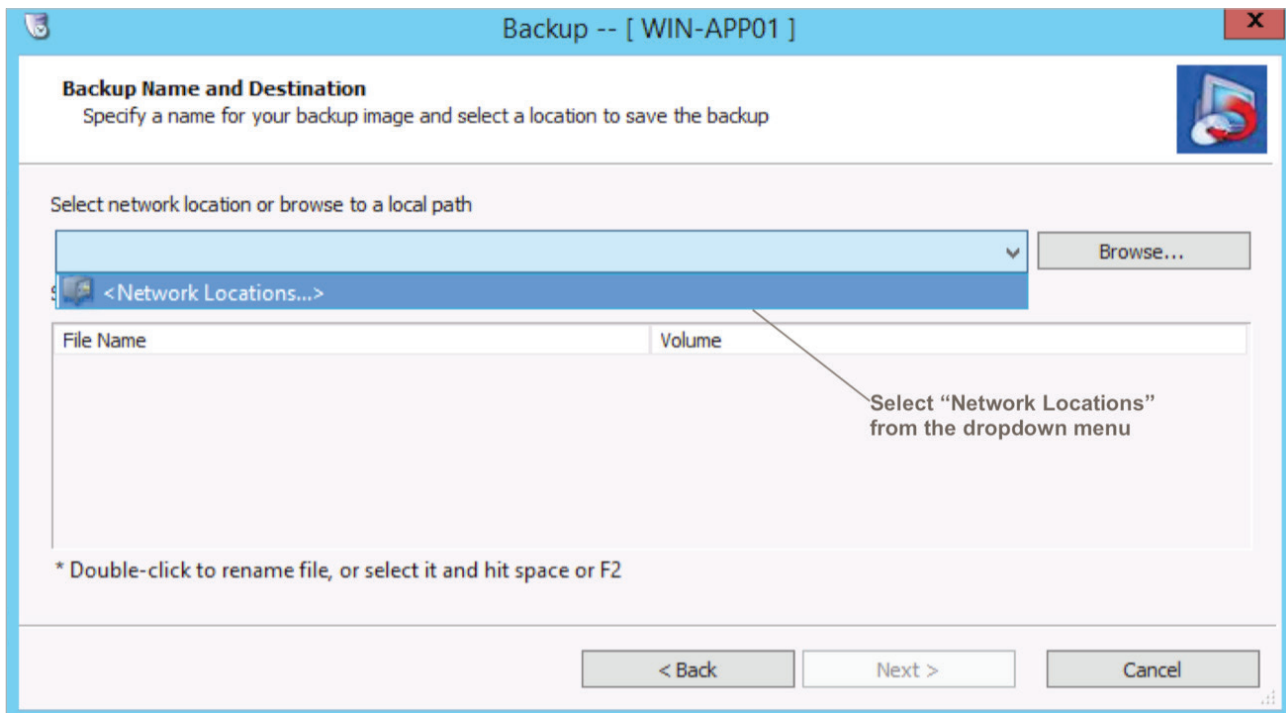
Fill out the fields in the Destination step.

1. Select "**NETGEAR ReadyDATA**" as the "**Destination Type**"

2. Enter a name for the "**New Destination Share**" (default is set to hostname)

3. Enter the IP Address for the ReadyDATA

4. Enter the admin password for the ReadyDATA and click "**Connect**"

5. Once connected, select a volume from the ReadyDATA

6. Select which ReadyDATA account you would like to use when the backup process access the storage. By default, this will be the ReadyDATA admin account. By selecting "**new/existing**", an alternate ReadyDATA account can be used for granular access control.

7. Click "**OK**" to continue

On the Backup Name and Destination step, you may customize the name of the individual backup image files that are created each time the backup runs. It is recommended to leave the default names.
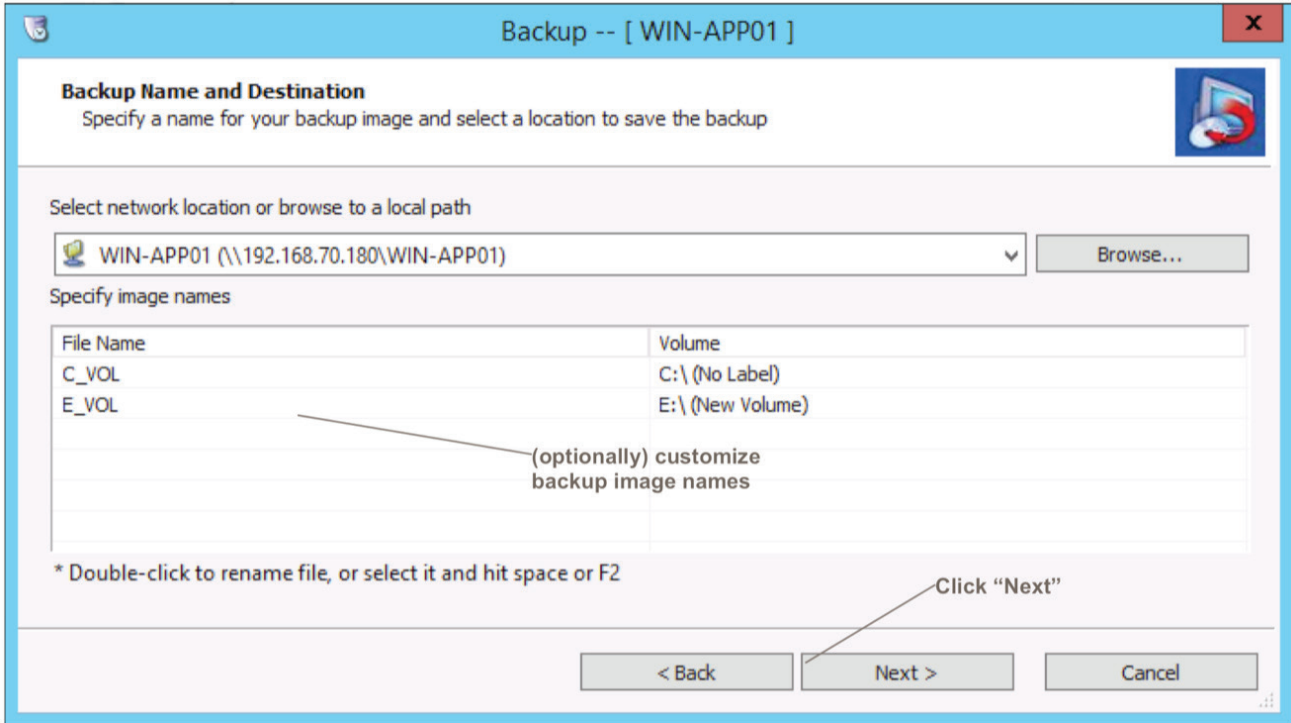
From the scheduler, select which days as well as the time range you would like backups to occur. Backups can run continuously by selecting a time in "**Start taking backups at this time**" one second after the time in "**Stop taking backups at this time**".
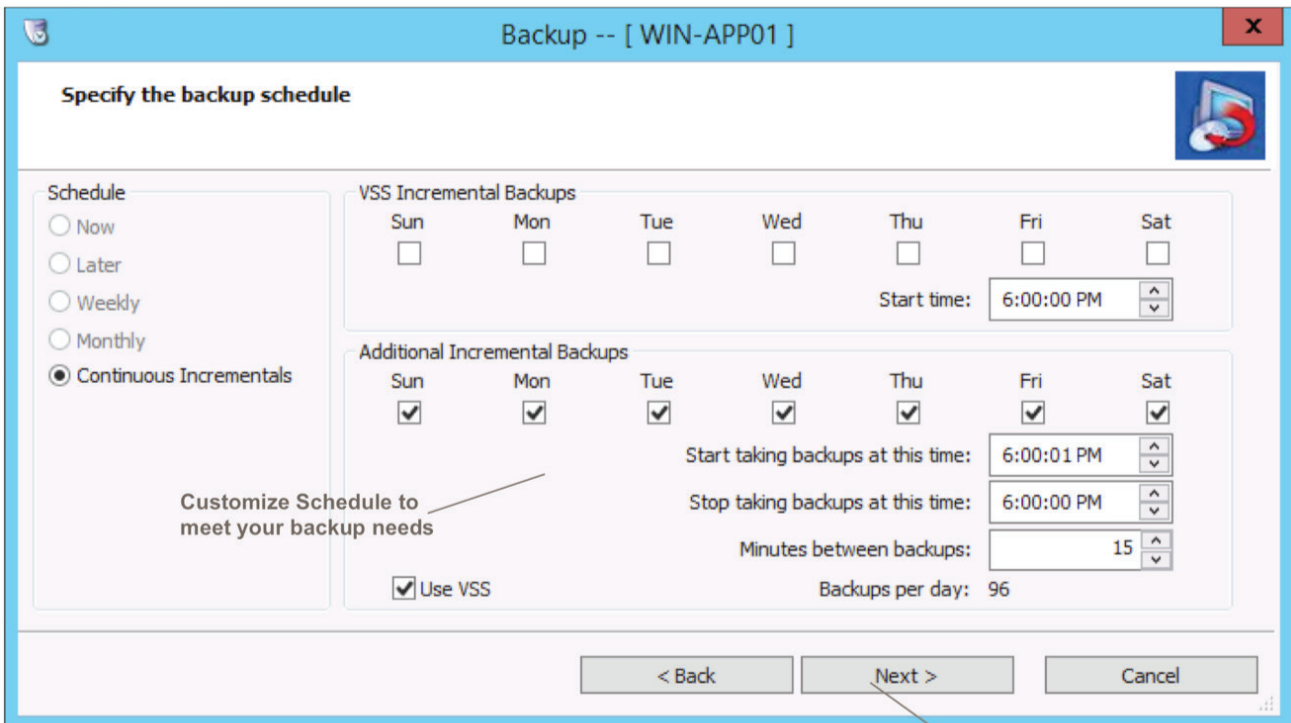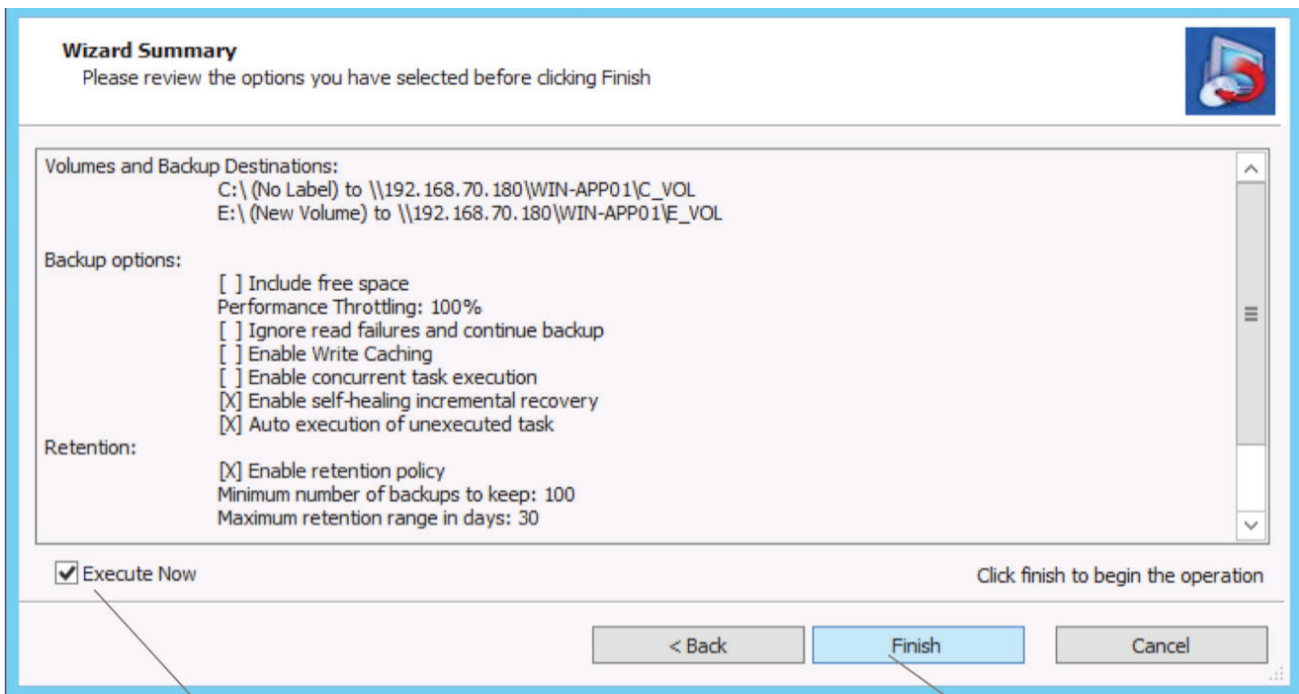
From the "**Retention**" tab select the minimum number of backups to keep and the Maximum range (in days) of backups to keep. Retention will automatically consolidate aging backups into less granular restore points that span the defined backup range as per the "Retention policy rules" below.
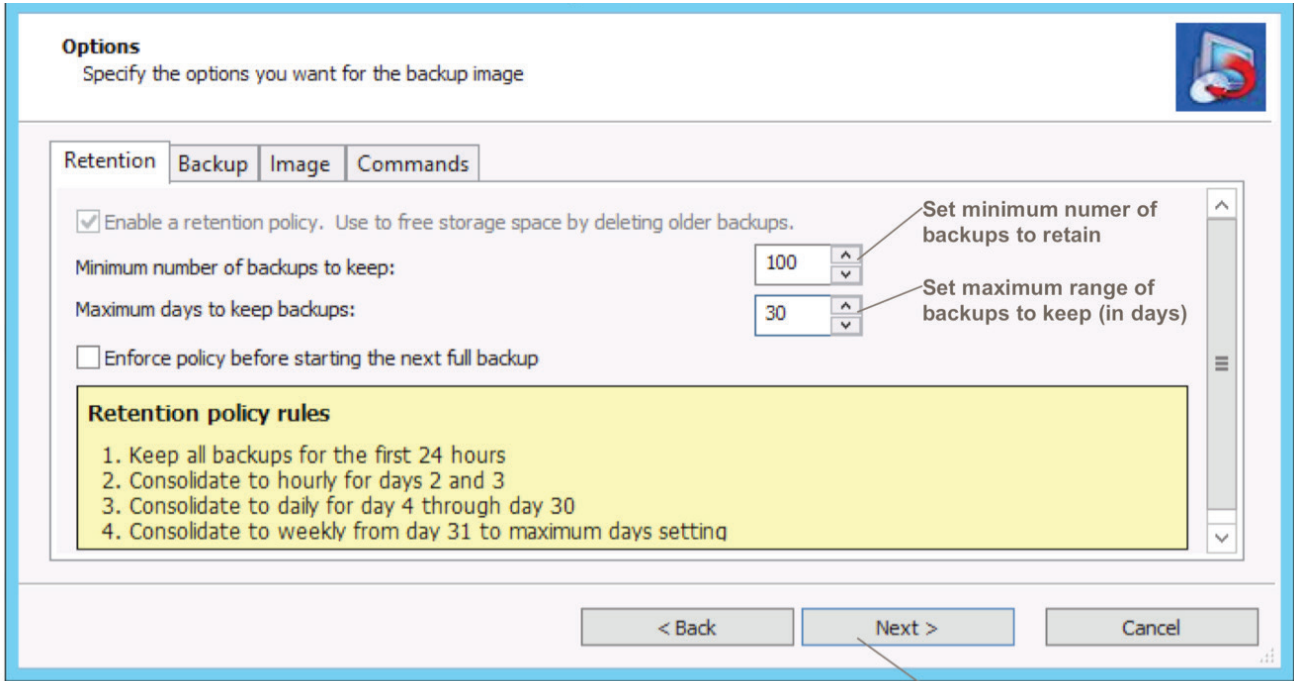
Confirm all the settings on the summary screen and optionally select "Execute Now" to run the first backup.

The first backup job will start and show progress in the "Backup Jobs" tab. You may close the client and the Backup will continue as a background operation.
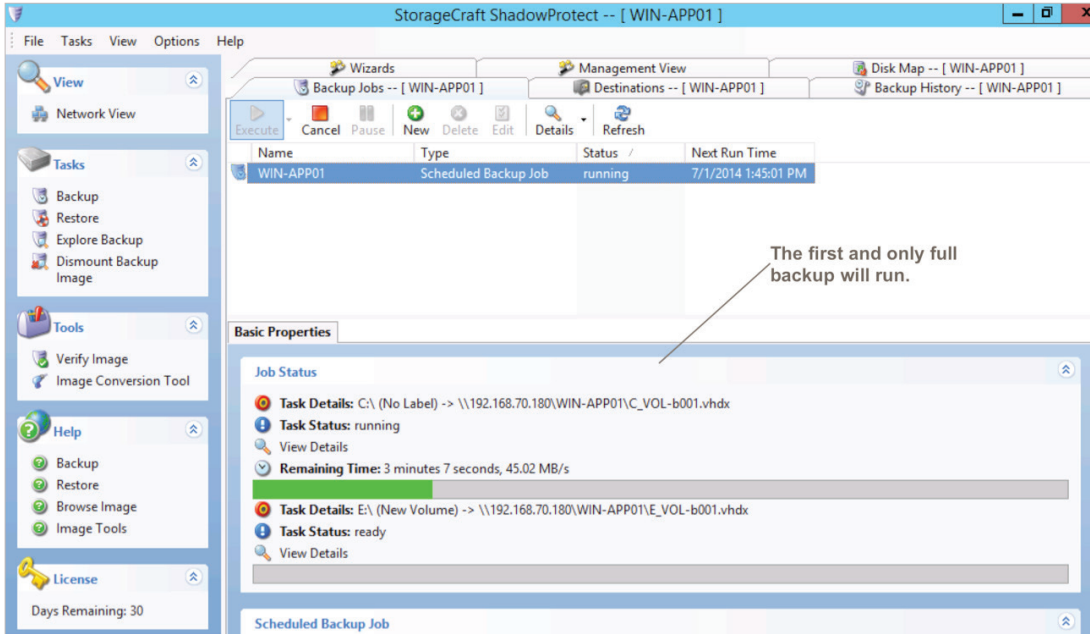
View Backup Sets on ReadyDATA

To see existing backups and storage consumption metrics, open the ReadyDATA UI in a supported web browser (https://{IP Address}) and select the "**Shares**" tab.
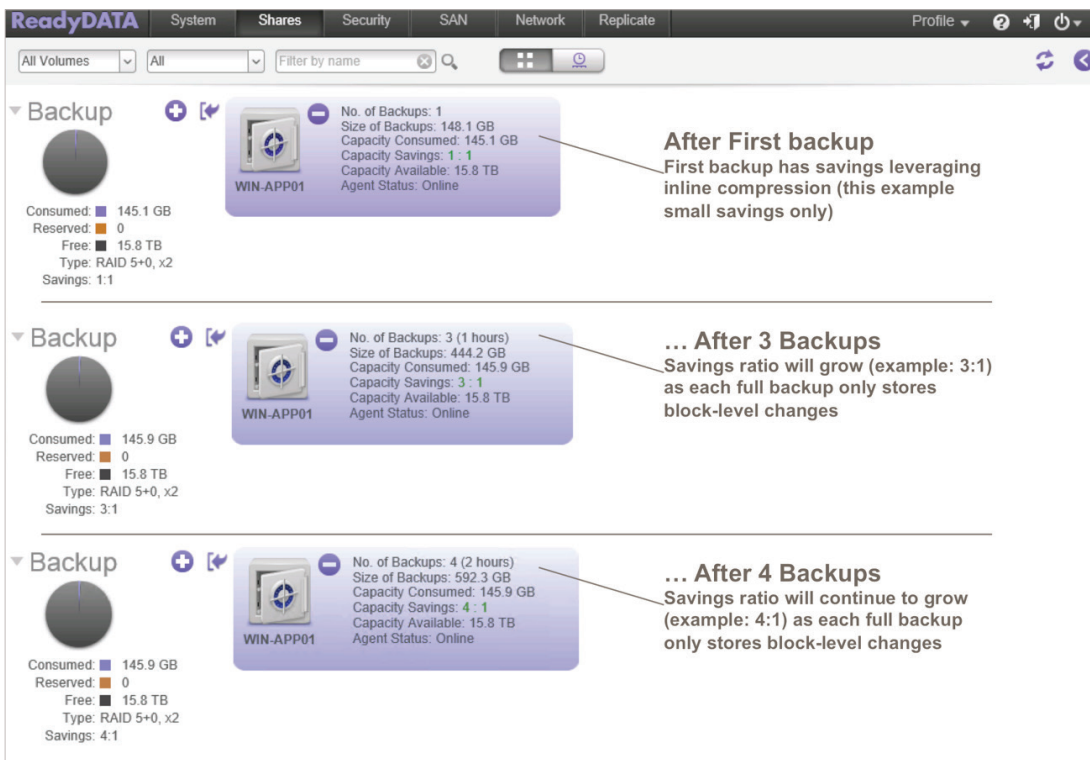
First Backup Savings - Storage savings on the first backup operation will be based on inline compression at the block-level. These savings vary based on the data type of the source server/client.

Ongoing Backup Savings – The ongoing savings will increase as more backups occur. Each backup stores only block changes, while keeping fully independent backup images.

Replicate backup data offsite for Disaster Recovery [Optional]

To offer additional protection against disaster, ReadyDATA offers the ability to replicate ReadyRECOVER backups offsite to a secondary ReadyDATA system.

One of the largest deployment considerations when setting up offsite data replication is the ongoing WAN bandwidth requirement. The best way to deliver fast and effective offsite replication is to reduce the amount of data being replicated. Combining ReadyRECOVER block-level change tracking with ReadyDATA replication will maximize WAN bandwidth efficiency when replicating backups to an offsite location. Much like the backup process itself, ongoing replication will only ever need to send incremental block-level changes after the first successful full replication cycle (forever).
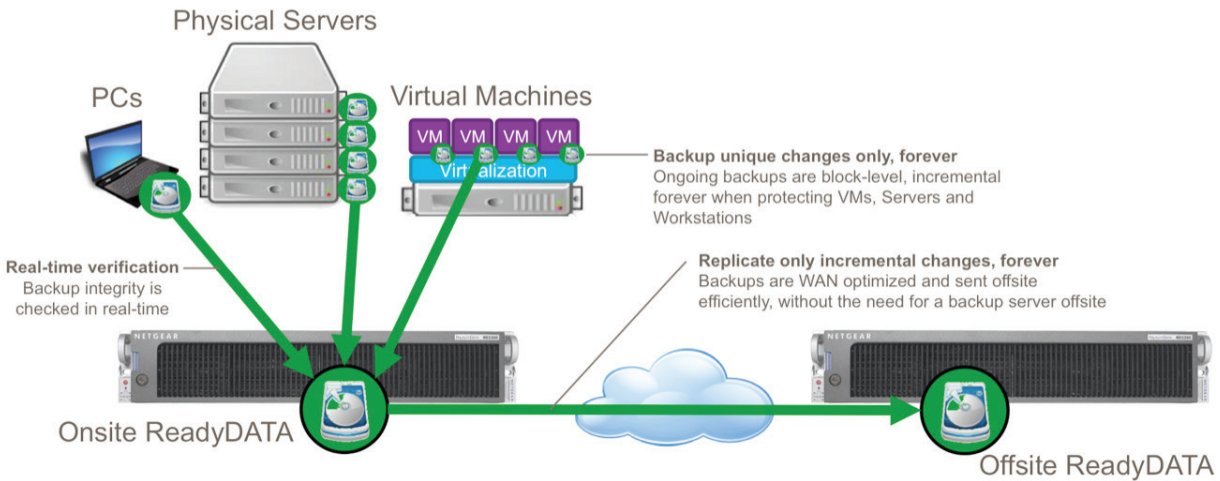
To configure replication of a Backup Set to a secondary location, you will need to have deployed a secondary system in the desired location, enabled replication services on that system, and copied the replication certificate key from the secondary system to the primary system. The certificate key can be found in the ReadyDATA administration console (Replicate Tab > Certificates).

Steps to configure replication of ReadyRECOVER Backups:

1. Connect to the onsite ReadyDATA with a supported web browser
2. Select the "**Replicate**" tab for the top menu
3. Click the "**New Job**" button
4. Give the replication job a unique and descriptive name
5. Expand the source system and select the source Backup Set
6. Enter the IP Address of the destination system. (Note: this address must be accessible from the source system. For WAN replication, port forwarding through firewalls on the remote site may be need.)
   – For an alternative option that does not require manual port forwarding, ReadyDATA's cloud-managed replication can be used. Please reference the ReadyDATA OS Software Manual for setup instructions. This document is available on the resource CD that came with your ReadyDATA. You can also obtain these manuals by clicking the **?** icon in the ReadyDATA dashboard.
7. Select the "**Access key**" (Certificate) from the dropdown list and click "**Connect**"
8. Select a volume from the remote ReadyDATA as a destination for replication
9. Click the "**Next**" button to continue the wizard
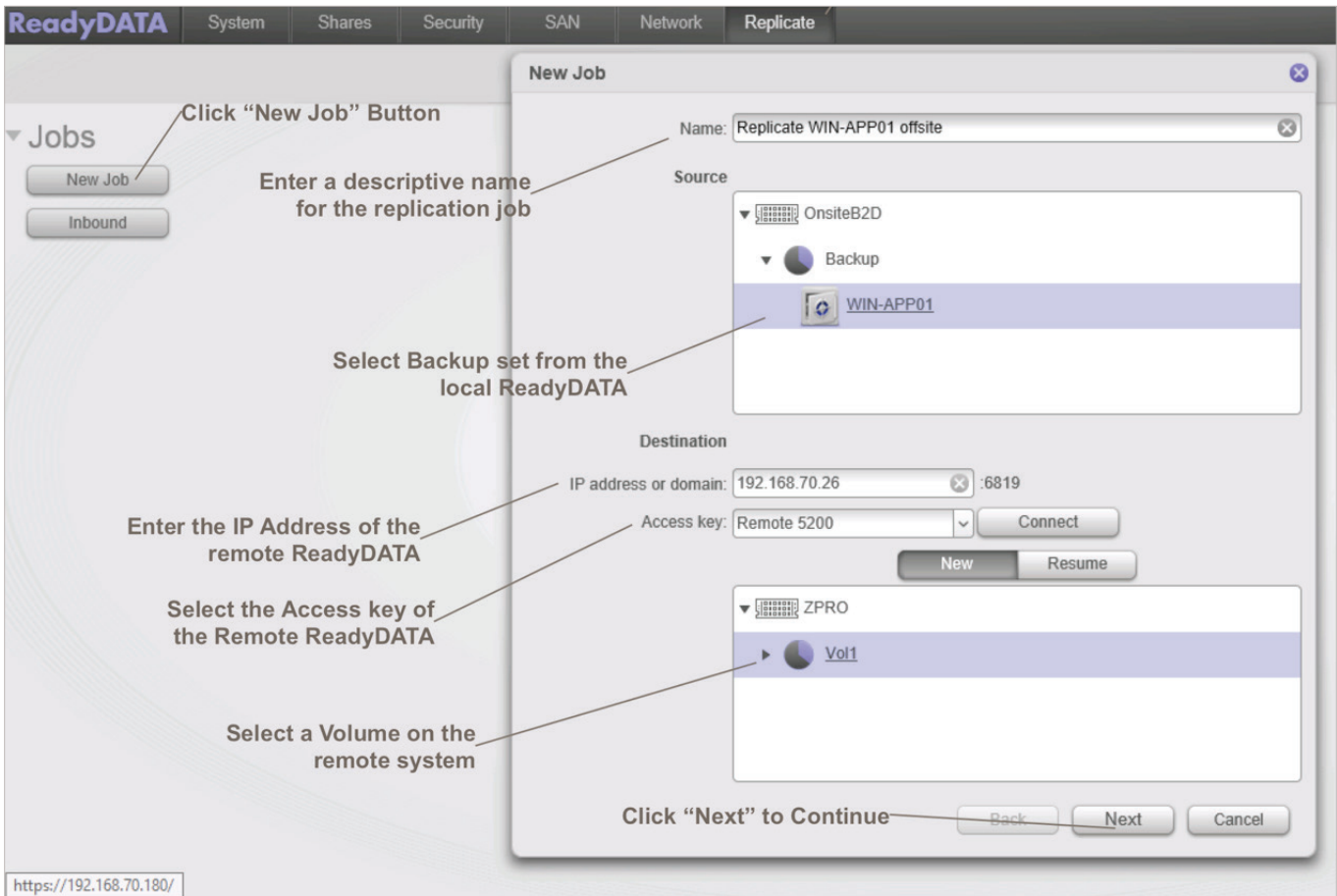
1. Enter a unique name for the remote Backup Set
2. [Optional] When replicating over a public network or limited bandwidth connection, it is recommended to select "Compression"
3. Click the "Next" button to continue

Select the frequency of the replication. This is an important decision based on recovery requirements and environmental factors such as connectivity between ReadyDATA systems.

Periodic replication is recommended for ReadyRECOVER installations. Replication can be scheduled on an hourly basis to meet aggressive recovery point objectives (RPOs) at offsite locations. However, for environments with restricted bandwidth, it is recommended to schedule periodic replication outside of business hours.

Once you have selected an appropriate replication frequency, press the "**Next**" Button to continue.
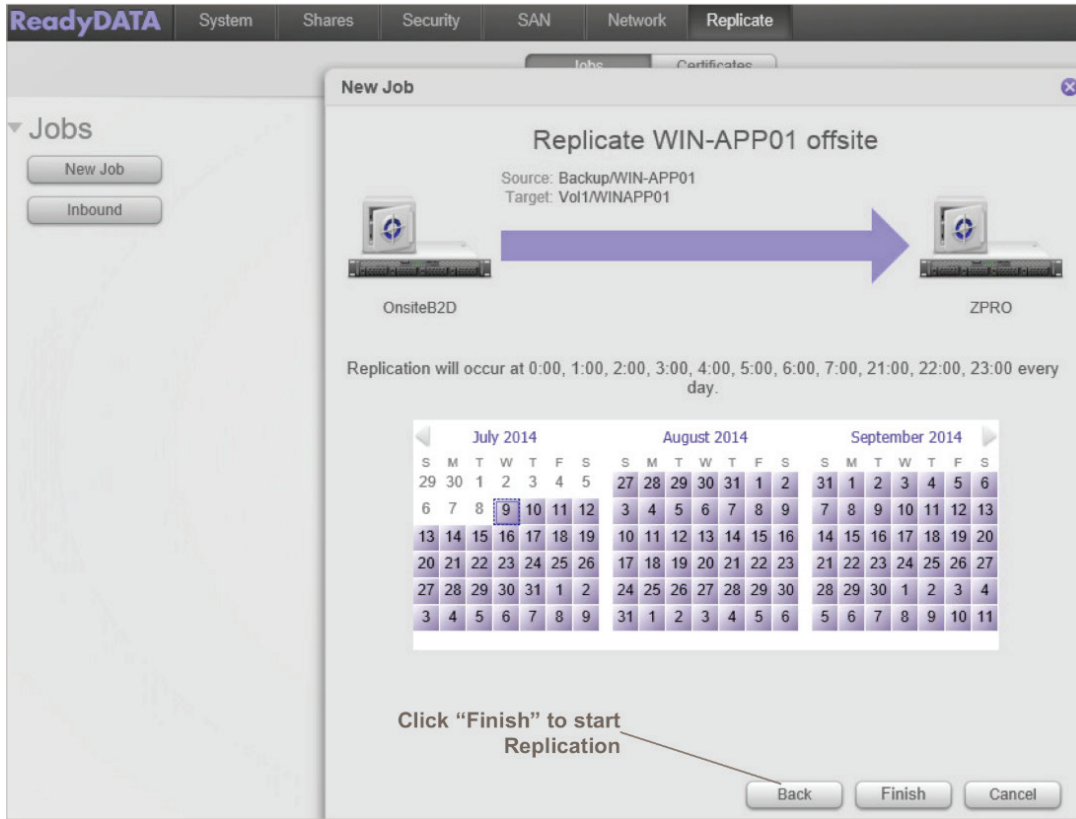

Once the wizard is complete, the replication job is ready to run its first replication cycle.

Performing a single file restore

ReadyRECOVER allows you to recover entire operating system in case of a hardware failure, disaster, or data corruption. However, smaller recovery tasks are far more frequent. One of the most common recovery situations in a server environment is the need to restore a single file that may have been changed or deleted.
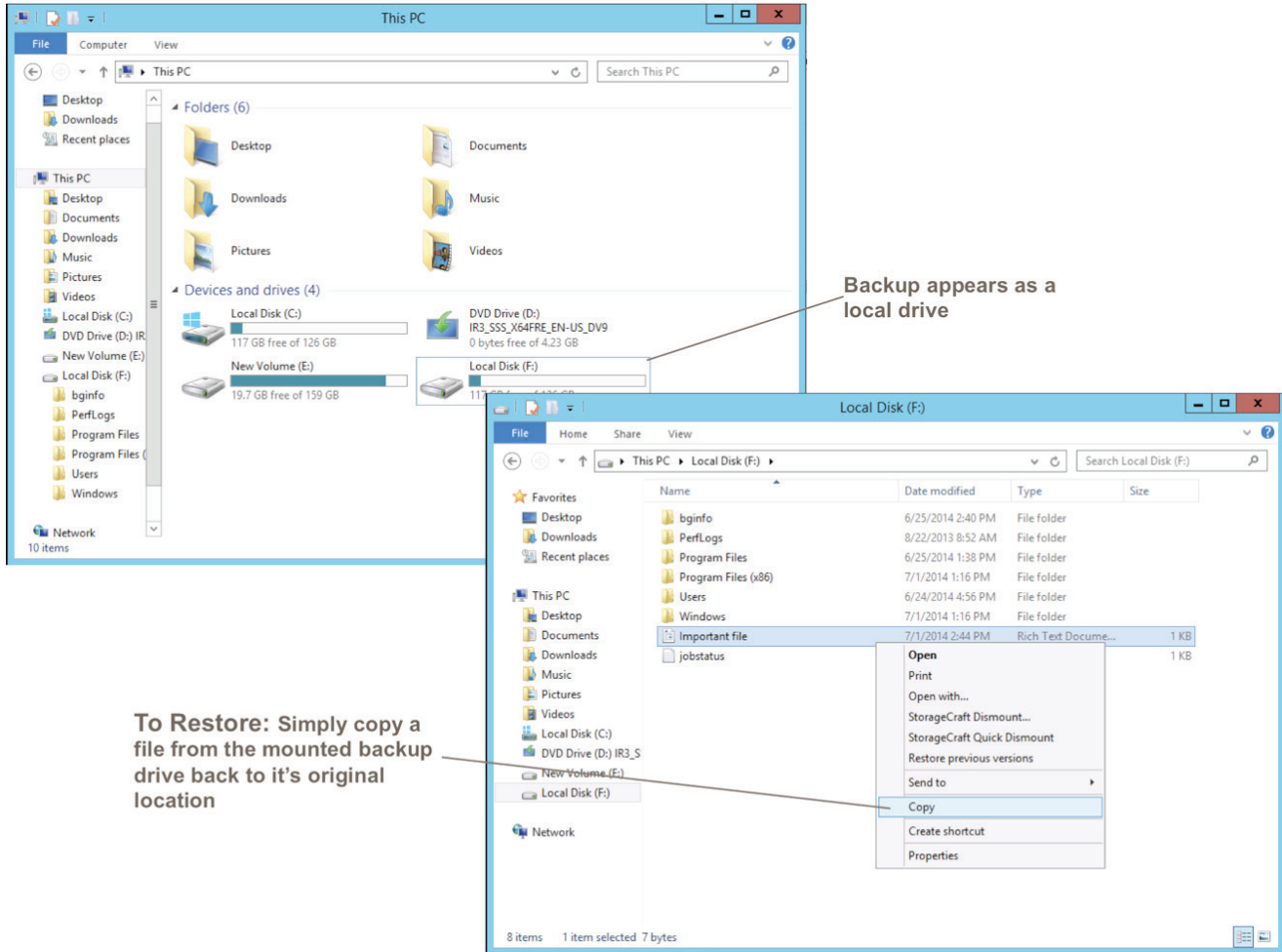
ReadyRECOVER provides a simple and reliable way to recover any file from any previous backup.
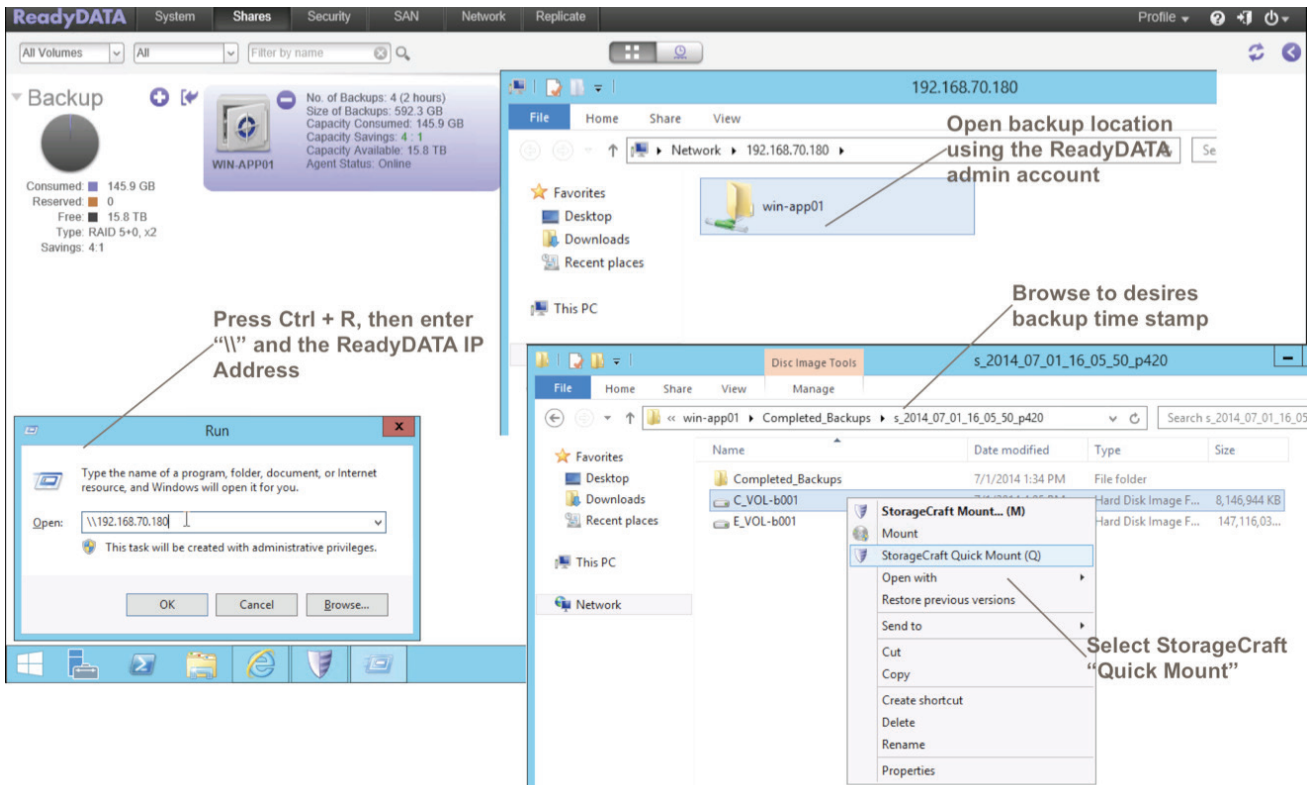
Recovery Steps

1. Connect to the desktop of any system that has the ShadowProtect agent installed

2. Press the Ctrl + R to bring up the Windows Run menu

3. Enter the UNC path for the ReadyDATA that hosts the ReadyRECOVER backups (\\{IP Address})

4. Open the backup share with the same name as your Backup Set

5. Browse through the "Competed_Backups" folder to the time stamped folder which contains the desired backup

6. Right click on the backup image file of the volume that contains the file you wish to restore. Select "**StorageCraft Quick Mount**".

A copy of the whole volume that is being protected by ReadyRECOVER will be mounted as a local drive on the system. Simply browse through the newly mounted volume and copy any files that need to be restored back to their original location.

Backup appears as a local drive

To Restore: Simply copy a file from the mounted backup drive back to it's original location

Congratulations! You have successfully recovered files. Detailed information about full system recovery, often called "bare metal recovery", can be found in the ReadyRECOVER User Manual, which is available on the ReadyRECOVER product page at: http://www.netgear.com/readyrecover