

# **NETGEAR<sup>®</sup> ReadyNAS<sup>®</sup> and Acronis<sup>®</sup> Backup & Recovery<sup>™</sup> 10**

**Configuring ReadyNAS as an  
Acronis Backup & Recovery 10 Vault**

## Table of Contents

Contents .....	2
Concepts .....	3
Data Deduplication .....	3
Acronis Vaults .....	4
Components .....	4
Configuration Steps .....	5
Creating Acronis User & Share on ReadyNAS .....	5
Configuring Acronis Backup & Recovery 10 to Recognize ReadyNAS .....	8
Confirm Acronis Backup & Recovery 10 Can Access ReadyNAS .....	11
Conclusion .....	12

## Concepts

NETGEAR® ReadyNAS® storage delivers reliable, affordable and simple solutions for businesses seeking smart IT, not big IT. Midsize companies can now build solutions for nearly any size location or data store at a fraction of the cost of traditional monolithic vendors. The ReadyNAS storage platform is especially well suited for backup to disk solutions and can help reduce backup, restore and disaster recovery times to minutes.

NETGEAR ReadyNAS and Acronis Backup & Recovery 10 work together to provide easily accessible backups for quick recovery for server, workstations, and business data. This document describes the basic solution architecture and provides detailed setup and configuration steps for such a solution.

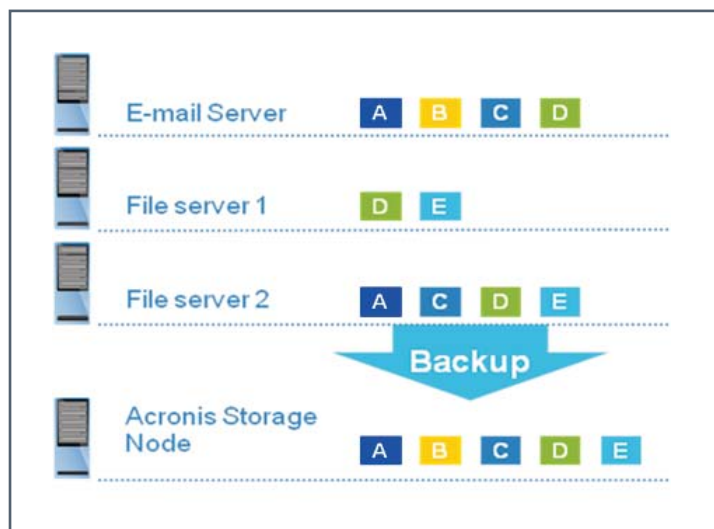
Acronis Backup & Recovery 10 uses ReadyNAS storage as a “vault” to store backups of data and systems. This vault can be configured as a centralized vault, which allows advanced features such as data deduplication or as a standard personal vault for simpler backups that can run without the need for a dedicated backup server.

## Data Deduplication

Deduplication works by monitoring data as it is written to storage, and removing any duplicate data blocks it finds during the backup process. Because system/data backups have large amounts of common (similar) data, deduplication can greatly decrease the amount of storage that is needed when backing up data.

File and block-level deduplication at the source or target eliminates redundant data, especially when copies of the same data exist on multiple systems. If a file or block is already in a location, only the link is saved instead of a second copy. In addition, the second copy is not transferred over the network, thus reducing network traffic. This applies to full, incremental and differential backups.

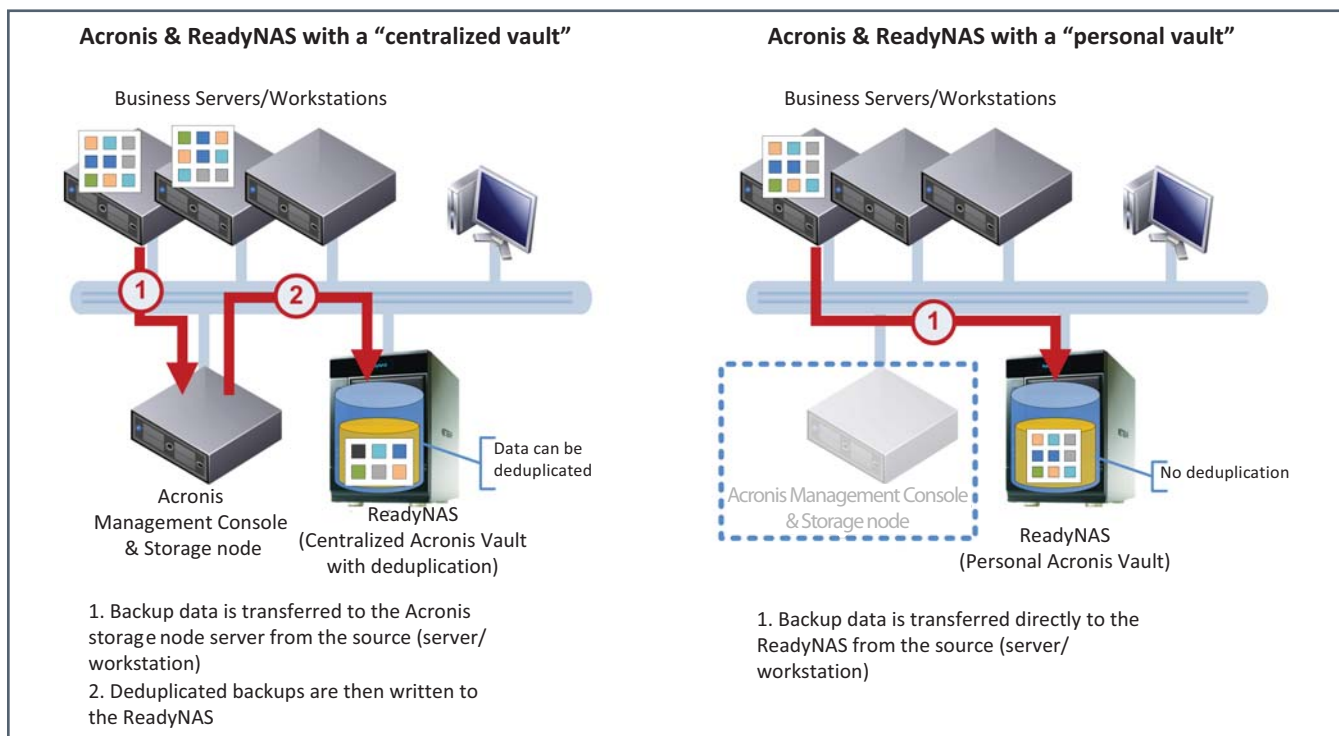
For example a 400GB backup might have 360GB of duplicate (redundant) data with other backups that have been run previously. In this case data deduplication could reduce the 400GB backup down to 40GB, providing a saving of 90%.



## Acronis Vaults

“Centralized Vaults” with deduplication enabled require a storage node server to exist on the network. The storage node server intercepts data between the backup source (servers/workstations) and the target (NETGEAR ReadyNAS) during the backup process. Any data that is not unique (duplicate data) is removed during this process to lessen the storage capacity required to store backups.

“Personal Vaults” do not require a storage node server, the source (servers/workstations) can write directly to ReadyNAS. This reduces the amount of hardware required to achieve a successful backup. Personal Vaults are convenient to configure but lack the advanced features such as deduplication.



## Components

The following components are required before attempting the below configuration steps.

- A Windows Server running Acronis Backup & Recovery 10 (this must include Acronis Backup & Recovery 10 Management Console and Acronis Backup & Recovery 10 Storage Node components)
- ReadyNAS Business Storage RAIDiator version 4.2.15 and above. This includes NVX, Pro, Pro2, Pro4, Pro6, 2100, 3100, 3200, 4200

## Configuration Steps

The following steps can be used as a guide for configuring a ReadyNAS as a deduplication vault for Acronis. This guide includes the step required to configure both a ReadyNAS and an Acronis Backup & Recovery 10 Server that are located on the same local area network.

### Creating Acronis User & Share on ReadyNAS

To prepare a ReadyNAS for Acronis backup we need to configure a dedicated share (CIFS) and create a user account with specific permission for writing backups to the share. Doing this will stop unauthorized users from accessing backup data.

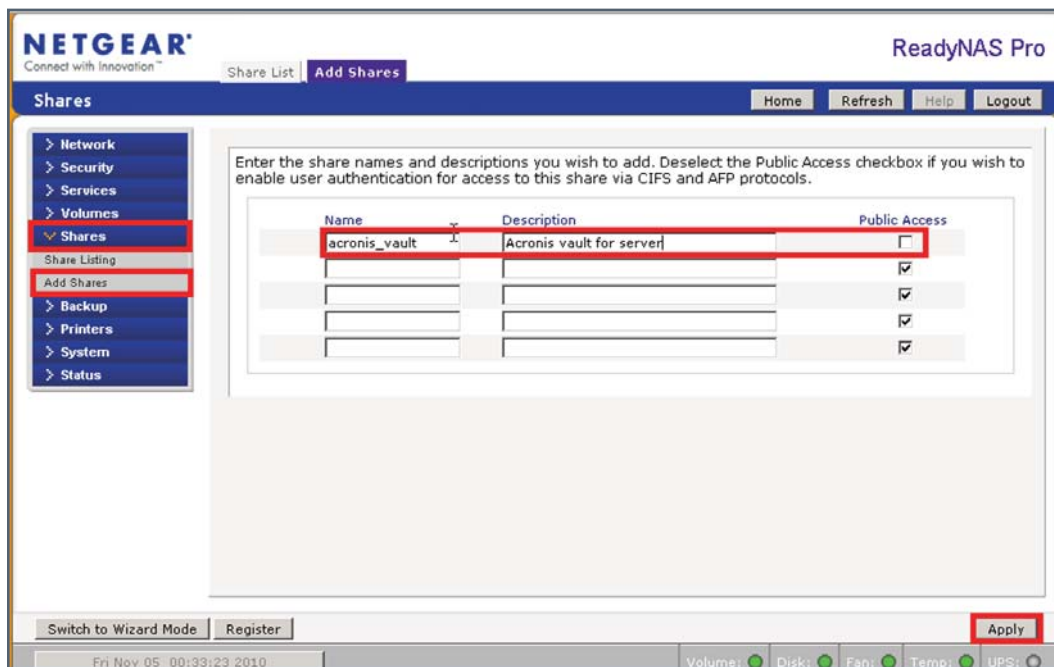
Log onto the Frontview management interface of the ReadyNAS you wish to use as a vault with Acronis (i.e. connect to <https://readynas/admin> from a web browser). Select the "Security" menu, and then select "User & Group Accounts". Enter a name for the account Acronis Backup & Recovery 10 will use to access the storage and a secure password. For this example we will use "acronis" as the user name. Click "apply" and the account will be created.

The screenshot shows the Netgear ReadyNAS Pro web interface. The 'Security' menu is selected, and the 'User & Group Accounts' sub-menu is active. The page displays instructions for adding user accounts and a table for entering account details. The first row of the table is filled with the following information:

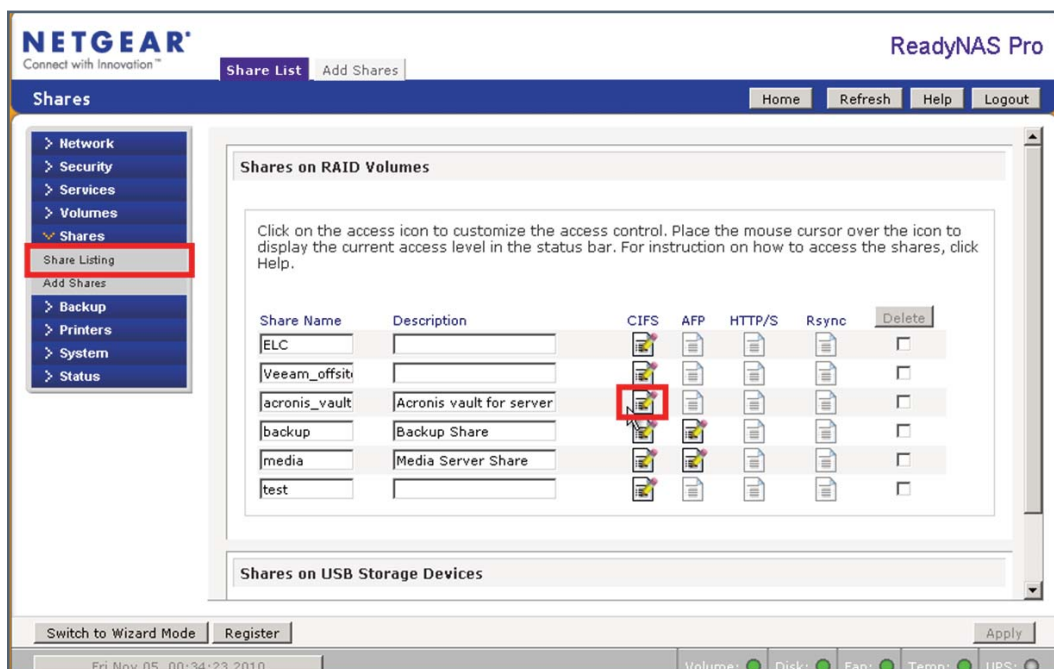
User	Email	UID	Primary Group	Password	Quota (MB)
acronis			users	*****	
			users		
			users		
			users		
			users		

The 'Apply' button at the bottom right of the interface is highlighted with a red box.

Select the "Shares" menu and click "Add Shares". Enter a name for the share you would like to use as the Acronis Backup & Recovery 10 vault (i.e. "acronis\_vault"). Uncheck the "Public Access" box to deny guest users from seeing the data that will be held in the Acronis vault.



Select the "Shares" menu again and then click on "Share Listing". The existing shares on the ReadyNAS will appear in the management console. Click on the CIFS icon next to the share that we created earlier (acronis\_vault).



In the permissions menu set the Default Access to "Disabled", this will deny any user accessing this share by default. Click the "Write-enabled users" option below and enter the name of the account (acronis) that was created for Acronis Backup & Recovery 10 to access the backup vault. Click "apply" and the new permissions will be set.

At this point the only user account that can access the new share is "acronis", this is important as it limits access to potentially confidential data.

The screenshot displays the Netgear ReadyNAS Pro web interface. The top navigation bar includes the Netgear logo, the text "Connect with Innovation™", and the product name "ReadyNAS Pro". Below this, there are tabs for "Share List" and "Add Shares", and a secondary navigation bar with "Home", "Refresh", "Help", and "Logout" buttons.

The main content area is titled "Shares" and features a left-hand sidebar with a tree view containing "Network", "Security", "Services", "Volumes", "Shares", "Share Listing", "Add Shares", "Backup", "Printers", "System", and "Status".

The central pane shows the configuration for a share named "acronis\_vault". At the top, there is a "Display Share List" button and a set of protocol tabs: "CIFS", "AFP", "HTTP/S", "Rsync", and "Advanced Options". The "Default Access" is set to "Disabled".

The "Share Access Restrictions" section contains the text: "Share access for the file protocol can be restricted using the access list(s) below." Below this, there are several checkboxes and input fields:

- Hosts allowed access: [input field]
- Read-only users: [input field]
- Read-only groups: [input field]
- Write-enabled users: [input field containing "acronis"]
- Write-enabled groups: [input field containing "acronis"]
- Allow guest access

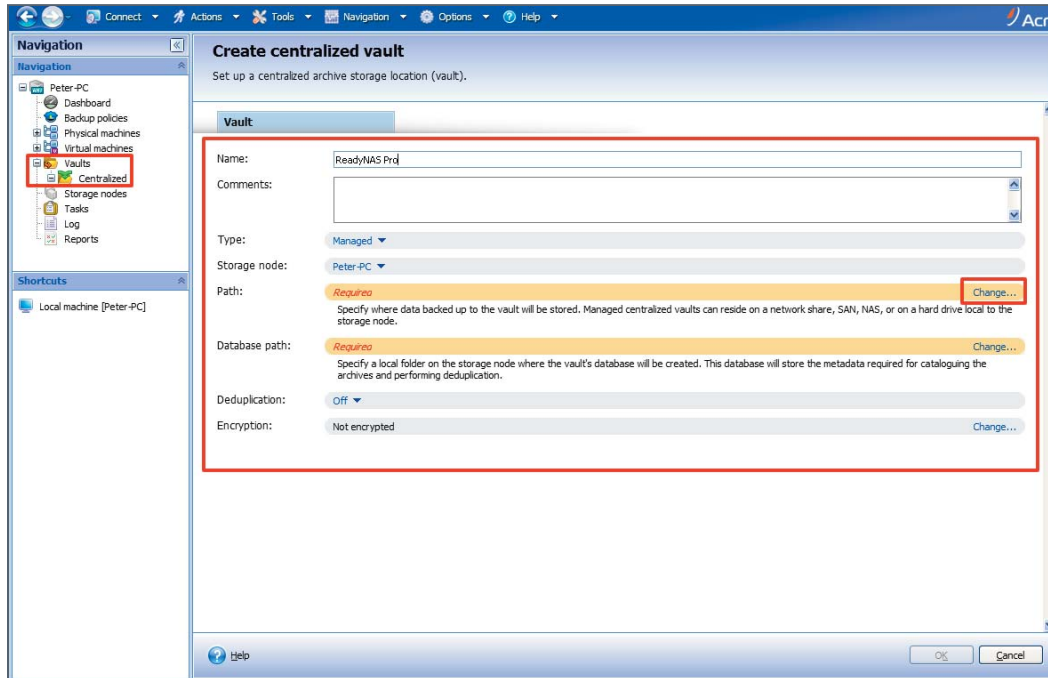
At the bottom right of the configuration area, there is an "Apply" button. The status bar at the very bottom shows system information: "Fri Nov 05 00:34:23 2010" and hardware status indicators for "Volume", "Disk", "Fan", "Temp", and "UPS".

## Configuring Acronis Backup & Recovery 10 to Recognize ReadyNAS

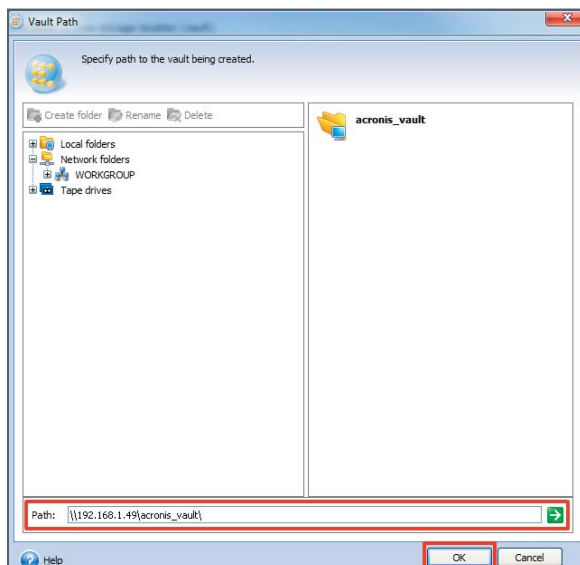
Now that we have created a “vault” share on ReadyNAS and created a user that can access the share, we can now configure Acronis Backup & Recovery 10 to recognize the ReadyNAS as a location for backups.

First, log into the Acronis Management Console of an existing Acronis Management Server. Expand the “Vaults” option from the navigation menu, then select “Centralized”, and click the “Add” button.

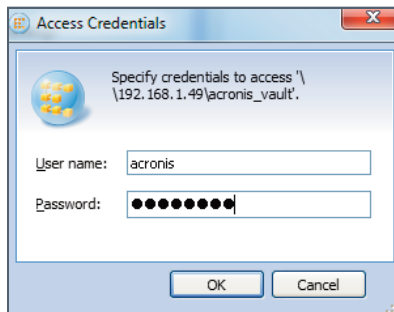
Enter a name for the new centralized vault. In this case we will name the vault after the ReadyNAS we are using (ReadyNAS Pro). Select “type” to be “Managed” and then click the “Change...” link located next to the “Path” option.



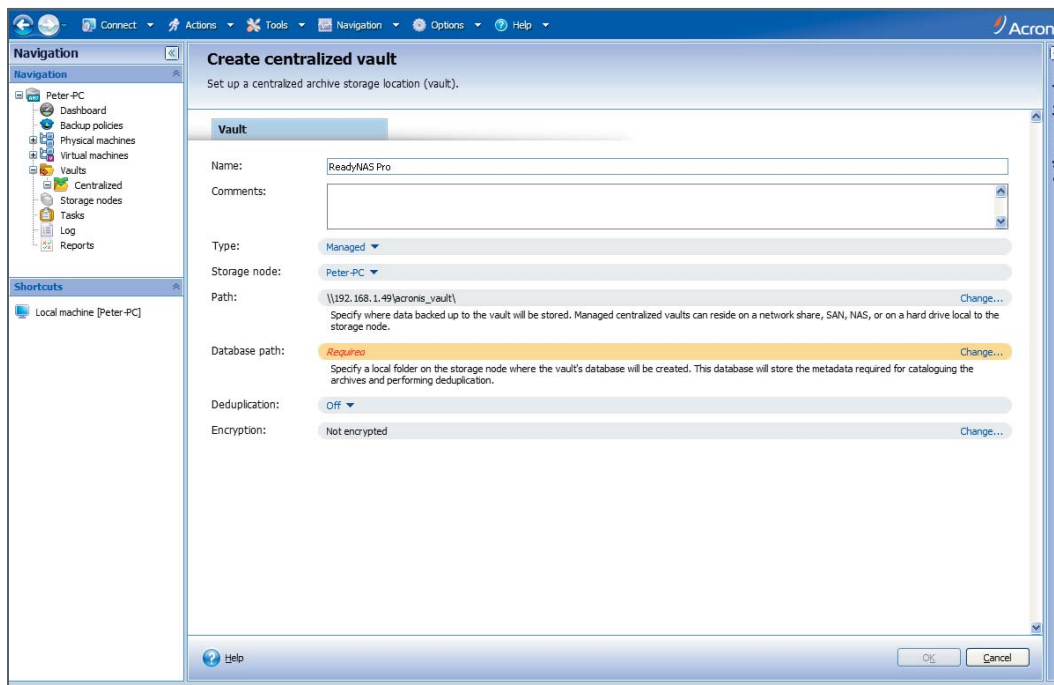
Enter the full network path to the ReadyNAS that will be used as the “vault” storage, this will include the network address and the share name created earlier. In this example the path would be “\\192.168.1.49\acronis\_vault”.

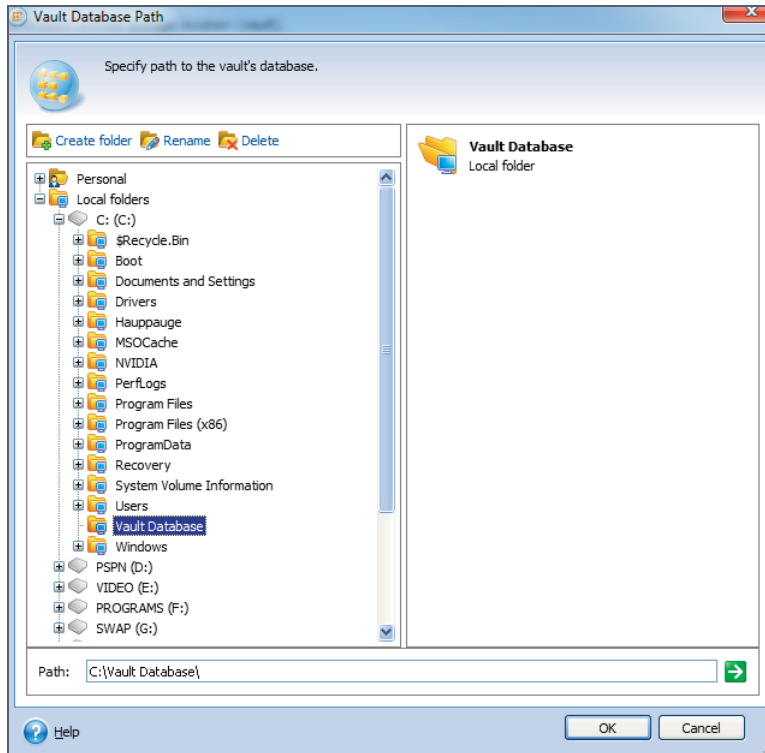


Click the green arrow and Acronis Backup & Recovery 10 will then prompt for the username and password that is required to access this location on the ReadyNAS. Enter the username (acronis) and password that was created earlier and click "OK".

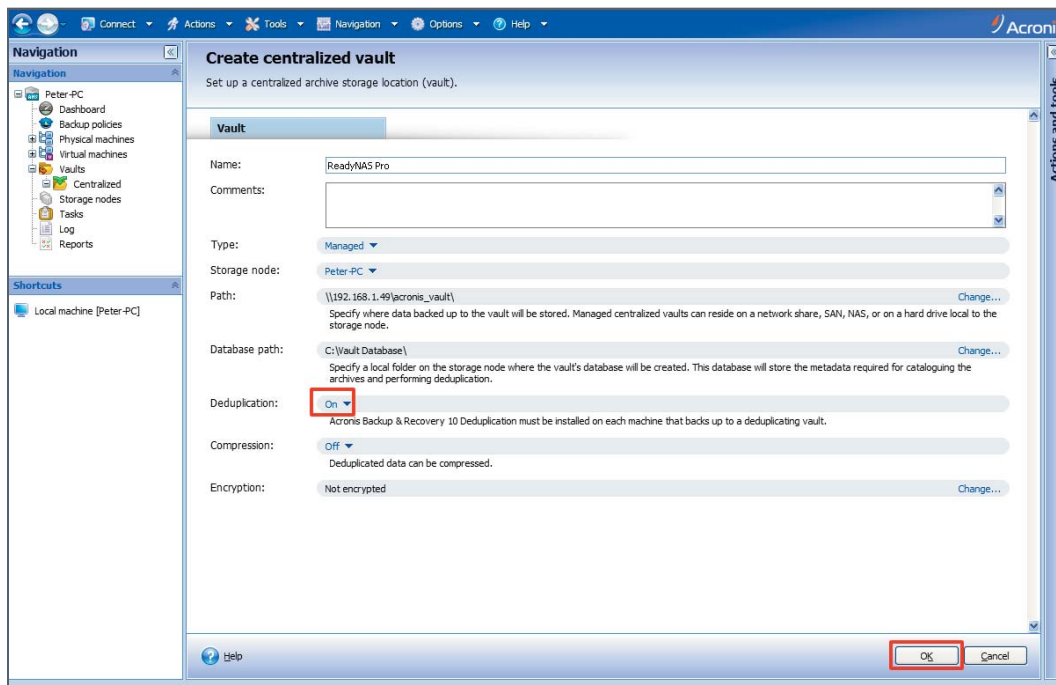


Before we can enable deduplication, we must specify a location for the vault's database. The database is used to hold deduplication information about data that is created during backup. Click the "Change..." link next to the "Database path" option and select a folder on the backup server to locate the database. The Database needs to be located somewhere on the storage node that will be managing this vault.





Now that the ReadyNAS is selected as the path for this “vault”, we can now choose advanced options. This includes the option for compression, deduplication, and encryption. For best results on deduplication, keep compression disabled. When the advanced options are selected we then click “Ok” to apply them. At this point the ReadyNAS is now acting as an Acronis Backup & Recovery 10 “vault” with deduplication capabilities.



## Confirm Acronis Backup & Recovery 10 can Access ReadyNAS

To confirm that Acronis Backup & Recovery 10 has recognized the new storage you can select "ReadyNAS Pro" from the list of "Centralized" vaults located in the navigation menu. If the configuration was successful you will notice Acronis Backup & Recovery 10 will be able to report the amount of available storage with the ReadyNAS and also advanced information such as deduplication ratio.

The screenshot shows the Acronis Backup & Recovery 10 interface. The main window displays the configuration for a 'ReadyNAS Pro' vault. The vault is identified as a 'Centralized managed vault' and is connected to the user 'Peter@Peter-PC'. The storage capacity is shown as 'Free: 1.360 TB'. The interface also displays a table for archives and a list of actions.

Archive name	Owner	Machine	Created	Occupied...	Backups	Comments
There are no items to show in this view.						

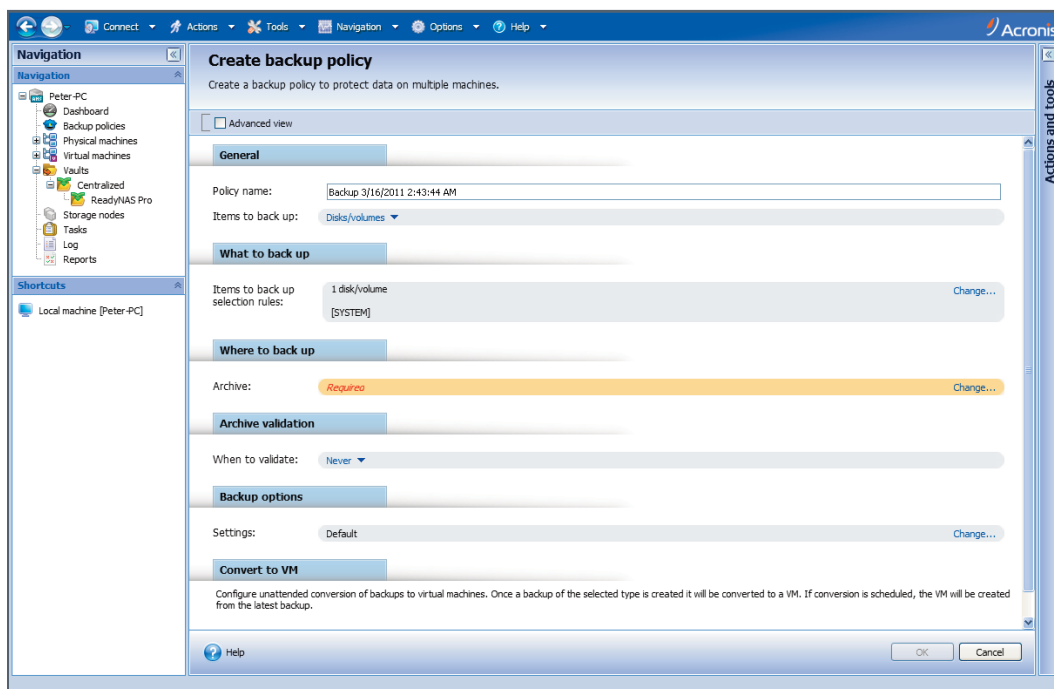
## Conclusion

Now that the ReadyNAS and Acronis Backup & Recovery 10 are configured to work together, backup jobs and policies can be created from within Acronis Backup & Recovery 10. The policies can be configured to use the ReadyNAS storage as a deduplicated vault, by selecting the "ReadyNAS Pro" in the "Where to back up" option when configuring backup policies.

Backup policies can be configured to protect large amounts of servers and workstations within a customer network and send all backup data to a ReadyNAS.

There are many different configuration options within a backup policy - this provides flexibility to protect systems in a way that suits the business.

Configuring ReadyNAS to work as an Acronis Backup & Recovery 10 vault provides a reliable, affordable, and simple way to efficiently backup business data in a smart IT environment.



NETGEAR, the NETGEAR logo, Connect with Innovation and ReadyNAS are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Acronis®, Acronis® Backup & Recovery™, Acronis Compute with Confidence, and the Acronis logo are trademarks and/or registered trademarks of Acronis Inc. in the United States and/or other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Information is subject to change without notice. © 2011 NETGEAR, Inc. All rights reserved.