



## BackupChain v4 User Guide

In 2021, we are celebrating our **12<sup>th</sup> year** serving IT professionals and businesses of all sizes worldwide. We would like to thank all our customers for their trust, and our partners and team members for their relentless efforts and hard work that has been invested in making BackupChain a solid and reliable enterprise-grade backup tool without the enterprise price tag.

© Copyright FastNeuron Inc., All rights reserved.

BackupChain® is a registered trademark of FastNeuron Inc.

Visit <http://backupchain.com/UserGuide> to access the most recent copy of this user guide.

Table of Contents.....	3
BackupChain Backup Software Concepts .....	11
What can BackupChain do for my business? .....	19
Getting Started.....	25
Introducing BackupChain Backup Software Features.....	27
Restoring Disk Images to Physical Disks.....	123
Restoring Files .....	125
Tutorials .....	134
Troubleshooting.....	259
General Recommendations .....	259
Frequently Asked Questions .....	263

## Quick Start Guides in the User Manual

File-Level Backup (for file servers and other document backups, [page 46](#))

Disk backup (P2P, P2V, V2P, V2V) on [page 29](#) and [page 134](#)

Granular backup & Granular Restore for Virtual Machines ([page 156](#))

Automatic Hyper-V backup for Windows Server 2008 - 2019 & Windows 8 - 10 ([page 180](#))

Windows 10 Hyper-V VM Backup and Restore using the Professional Edition ([page 192](#))

Hyper-V backup, *file-based* for PCs and Servers ([page 166](#))

VMware backup ([page 209](#))

SQL Server backup ([page 218](#))

VirtualBox backup, Virtual Server, and other VM platforms ([page 223](#))

Secure FTP server setup ([page 230](#))

How to back up to remote servers and cloud servers ([page 236](#))

Centralized Management ([page 245](#)) and Step-by-Step Instructions on [page 249](#).

Restoring Disk Images to Physical Disk ([page 123](#))

## Table of Contents

### Contents

Table of Contents .....	3
BackupChain Backup Software Concepts .....	11
Sector-Level Disk Backup vs. File Backup vs. Virtual Machine Backup .....	11
Compression .....	12
Encryption .....	12
Deduplication (Delta Compression) .....	13
Backup Tasks .....	13
Scheduler: The Auto-Pilot .....	13
Network Folders.....	14
Domains and Workgroups .....	15
Windows User Accounts .....	15
Authentication .....	16
Common Network Connection Challenges .....	16
Network Drives Accessed via a Mapped Drive Letter .....	18
What can BackupChain do for my business? .....	19
Mitigate Risks of Data Loss .....	19
Protect Your Data Efficiently and Economically.....	20
Deduplicate and Save Space by Removing Redundancy .....	20
Incremental Backup .....	20
Run Backups while You Work .....	20
“Owning” your Own Data – No Technological Lock-In .....	21
Sector-Level Disk Image Backup (P2V, V2P, P2P, V2V) .....	21
Physical to Physical Disk Copy (P2P) / Disk Cloning .....	21
Physical Disk to Mounted Virtual Disk Copy: Disk to Disk Copy over LAN.....	21
Live VM Conversion (V2V).....	22
Physical to Virtual (P2V) and Virtual to Physical Conversion (V2P) .....	22
General File Backup .....	23
Virtual Machine Backup (Hyper-V, VMware, VirtualBox, CSV) .....	23
Database Backup.....	23

Set up Your Own Online Backup System .....	24
Getting Started.....	25
Minimum Requirements .....	25
Feature List.....	25
Installation Instructions .....	26
On Hyper-V Server 2008 R2 or Windows Server 2008 R2 Core Installations .....	27
On Hyper-V Server 2012 - 2019 or Windows Server 2012 -2019 Core Installations .....	27
On Windows 8, Windows 10, Windows Server 2012 - 2019 Installations.....	27
Introducing BackupChain Backup Software Features.....	27
Sector-Level Disk Backup Strategies .....	28
How Disk Backup Works .....	28
Important Note .....	28
Disk backup via disk copy.....	28
Disk backup via virtual disk conversion .....	28
Virtual to virtual disk backup .....	28
Virtual to physical (i.e. Disk restore).....	28
Remote disk backup via copy.....	28
Backing up Virtual Machines.....	29
Creating a New Disk Backup Task .....	29
Definition of terminology.....	29
Disk Cloning.....	29
Getting started .....	29
Disk to image backup (Copy physical disk to virtual disk image).....	31
Specifying the target file .....	33
Choosing a virtual disk target type .....	35
Physical to Physical Disk Copy (Disk to Disk: Sector level copy) .....	35
Important notice regarding disk to disk live backups .....	37
Automatic Cleanup of Old Virtual Disk Backups .....	38
Backing up Several Disks Simultaneously .....	39
Virtual Disk Conversion .....	40
Automatic cleanup .....	42
Image to Disk: Copy virtual disk image to physical disk.....	42

Disk Backup Verification .....	44
Creating a New Task.....	46
Selecting folders.....	47
Backing up Local Folders .....	48
Backing up a Network Folder .....	49
Backing Up Folders Stored Inside a Virtual Machine (Granular Backup).....	51
Backup Defaults .....	55
Recommended Settings .....	55
No File Processing .....	56
Custom Backup Settings.....	57
Selecting a Backup Target .....	58
Specifying an FTP Backup Target .....	59
Running your Backup .....	60
Where Do I Set Up a Schedule? .....	61
Disk Backup and Disk Converter .....	62
The BackupChain Monitor (Main Screen) .....	64
Context Menu .....	65
Open Log Viewer .....	65
Deleting Tasks .....	65
Cloning Tasks.....	66
Selecting Folders .....	67
Select Local Folders to Be Backed Up .....	67
Select Network Folders to Be Backed Up.....	67
Select Folders Stored Inside a Virtual Machine or Virtual Disk (Granular Backup) to Be Backed Up .....	69
Adding Individual Files to Backup Task .....	72
Adding Local Files.....	72
Adding Individual Network Files to Backup Task .....	73
Adding Files Stored Inside a Virtual Machine to Backup Task (Granular Backup) .....	75
Excluding Folders and Files .....	79
Adding Hyper-V Virtual Machines to Backup Tasks .....	80
Manual VM Selection.....	80
VM Backup Size Estimation.....	80

Automatic VM Selection Feature .....	81
Selecting a Backup Target .....	85
Local Drive Backup Targets .....	85
Network Folder Targets .....	85
FTP / FTPS Backup Targets .....	87
Advanced FTP Settings .....	87
Backup Configuration Depending on File Type (File Versioning / Cleanup Tab) .....	88
Limiting the Number of Backups (File Version History) .....	89
Enabling / Disabling Data Compression .....	90
Minimum File Age .....	90
Enabling Deduplication Depending on File Type .....	91
Delayed Deletion Periods Depending on File Type .....	91
File Backup Archive Period Depending on File Type .....	92
Example Interpretation of File Versioning / Cleanup table .....	92
How to Exclude a File Type from your Backup .....	94
How do I Backup Specific File Types Only? .....	95
Deduplication (Delta Compression) Settings .....	95
What is Incremental Deduplication? .....	96
What is Differential Deduplication? .....	96
Why and How to Create Intermittent Full Copies .....	96
Delta Block Size and its Meaning .....	97
How to Turn off Deduplication for all Files .....	97
How to Turn on Deduplication for Specific File Types .....	98
Schedule Settings .....	99
Continuous Backups .....	100
One-Time Backups .....	100
Daily Backups .....	100
Weekly Backups .....	100
Monthly Backups .....	101
The Options Tab .....	101
Task Settings .....	102
Locked File Handling .....	103

Sound Alert Settings.....	104
External Utilities.....	104
Access Control List .....	104
Task Chaining .....	105
The Compression Tab.....	106
The Verification Tab .....	107
Reverification of backup files.....	107
Coverage of Re-verification.....	108
Re-reading files actualizes sectors .....	108
Benefits of Verification and Reverification .....	108
The Speed Tab.....	110
Specifying Resource Allocation Limits / System Stress Prevention .....	110
Simultaneous File Backups.....	111
Background info on hard drives.....	111
Ethernet Background Info.....	112
When to use Simultaneous Backups.....	112
Folder Caches, Read-ahead, and Buffering Options .....	113
Enable Folder Cache.....	113
Write cache & read-ahead optimization.....	113
Minimal buffering .....	114
The BackupChain Log .....	115
Export Log as HTML.....	116
Log Archive.....	116
Skipped Files (Files Already Backed Up).....	117
Sending Your Log File to BackupChain Support .....	117
Log Archiving.....	117
Clearing and Refreshing the Log .....	118
Opening the Log in a Separate Window .....	118
Opening a Single Event in Log.....	118
Log Options .....	120
Customizable HTML Email Alerts .....	120
Progress Indication .....	122

Restoring Disk Images to Physical Disks.....	123
Restoring Files .....	125
Selecting a Backup Set .....	126
Restore Screen .....	127
Advanced Extraction Options .....	129
Restore Progress .....	131
Restoring a Single File .....	131
Tutorials .....	134
How to Set Up Sector-Level Disk Backups .....	134
How to Convert a Physical Machine to a Virtual Machine (P2V).....	134
Automatic cleanup of old virtual disk backups .....	137
Bootting the virtual disk as virtual machine (P2V) .....	138
Create a P2V VM in Hyper-V Server 2016.....	139
Changing VM Boot Settings .....	144
Create a P2V VM on VMware Workstation .....	146
Creating a P2V VM in VirtualBox.....	150
How to Restore a Disk: Copy a Virtual Disk to a Physical Disk (V2P) .....	152
Converting a Virtual Machine to a Physical Server (V2P) .....	154
Tips to prevent BSOD when booting on new hardware .....	154
Granular Backup and Restore .....	156
How to Configure a Granular Backup .....	157
How to use Granular Restore to Extract Individual Files from Virtual Machine Backups .....	160
Hyper-V Virtual Machine Backup and Restore .....	166
Hyper-V Live Backup Prerequisites .....	166
File-based Approach for Hyper-V Backup .....	167
Backup.....	167
Restoring Hyper-V VMs using the File-Based Method.....	174
Automated, Single-Click Hyper-V Backup .....	180
Sequential VM Backup vs. Multiple-VM Consistent Backup.....	184
Cluster Shared Volumes .....	184
Dealing With VM Migrations (Live, Manual, Automatic / CSV) .....	186
Restoring VMs.....	186

Starting the machine .....	191
Windows 10 Hyper-V Backup and Restore using the Professional Edition .....	192
Backup.....	192
Where are the VM files located? .....	194
Restoring Hyper-V VMs running on Windows 10 hosts using the Professional Edition .....	200
Replacing the original VM .....	204
Restoring a VM to a New Hyper-V Host or Side-by-Side with Original VM .....	205
Summary .....	207
VMware Virtual Machine Backup .....	209
Backup.....	209
Restore .....	211
Cold VMware Backups .....	216
Microsoft SQL Server Database Backup.....	218
Backup MDF and LDF Files .....	218
Restore .....	219
Backup Via SQL Server Script and then Deduplicate Using BackupChain.....	221
Restore using BAK files.....	222
VirtualBox Backup and Restore.....	223
Backup.....	223
Restore .....	224
How to Set up the Built-in FTP/FTPS Server .....	230
Server-side scanning database.....	230
Incremental and Differential Deduplication .....	230
Security Features .....	230
Reliability Features.....	230
Setting up the FTP Server.....	231
Adding FTP Users .....	232
Starting the FTP Server .....	234
Testing FTP Server Connectivity.....	234
Current Sessions.....	234
Helpful Hints .....	235
How to Back up to a Remote FTP Server .....	236

FTP Backup Characteristics .....	238
How to Restore Files Stored on a Remote FTP Server .....	239
How to Set Up Your Own Online Remote Backup System.....	240
How to Install BackupChain on Windows Server 2008 Core or Hyper-V Server 2008 R2 .....	241
How to Install BackupChain on Windows Server 2016 / 2012 Core or Hyper-V Server 2016 / 2012... 242	
How to Change the BackupChain Service User.....	243
How to Set up Centralized Remote Management .....	245
Two Possible Connection Scenarios Combined .....	245
Inbound Connections .....	245
Outbound Connections .....	245
Example diagram showing a mixed-mode setup .....	245
When to use inbound and when outbound? .....	246
Typical use for outbound connections (master to slave).....	248
General Recommendations for Setting up Remote Management .....	248
Troubleshooting Remote Management Connectivity .....	249
Step By Step Instructions for Centralized Management.....	249
Setting up the Master Console .....	249
Adding a Slave Server.....	251
Setting up Inbound Connections (Master Receives Link from Slave) .....	253
Setting up Outbound Connections (Master Connects to Slave) .....	255
Managing Remote Servers .....	257
Restoring Files on Remote Servers .....	257
Managing Backups on Remote Servers.....	258
Troubleshooting.....	259
General Recommendations .....	259
RAM.....	259
System Settings.....	260
Windows System Restore and Other Backup Tools.....	260
Simultaneous Backups .....	260
Hyper-V Backups .....	260
Speed Settings.....	261
General Recommendations .....	261

Frequently Asked Questions .....	263
What is the FastNeuronDelta file extension? .....	263
What is the FastNeuronDate extension? .....	263
Will My Backups Run If I Log off? .....	263
How can I reduce RAM Usage? .....	263
Can I Rename a Task? .....	263
Can I Move the Backup Folder? .....	264
Can I Restore Several Backups Simultaneously? .....	264
Can I Backup Files in their Native Format? .....	264
How do I get a Full Backup Every Time the Backup Runs? .....	264
How can I Get all my Files Compressed using ZIP? .....	264
What is the Name of BackupChain's Background Service? .....	265
How Can I limit the Number of File Versions Retained in the Backup Folder? .....	265
How Can I Limit Bandwidth Usage? .....	266

## BackupChain Backup Software Concepts

If you handle and store important data on your computers, it is important for you to understand the following concepts related to data backup.

### Sector-Level Disk Backup vs. File Backup vs. Virtual Machine Backup

Sector-level disk backup is a process where the entire disk is being copied to another disk or a virtual disk, or a container file. Disk backup doesn't have to be aware of what's in the disk; disk backup is a sector-by-sector copy of a disk and includes whatever may be stored on disk, including hidden areas, encrypted files, file fragmentation, etc.

File backup is a process where the backup application processes each file or document separately. File backup offers many benefits over disk backup, such as file versioning, where the entire history of a document is available for restore. In addition, file backup can be tuned to quickly skip unchanged or unwanted files in the backup. BackupChain also offers a way to change how each type of file is processed (compression, encryption, deduplication, file history length, cleanup, etc.) depending on its file extension.

While disk backup is useful to take a backup of the Windows operating system in its entirety, it's not recommended as a replacement of file backups. Similarly, file backups alone can't restore the Windows operating system; hence, most IT administrators chose a hybrid backup strategy: A sector-level disk backup when the server or PC is fully installed with all applications and perhaps once or twice a year after that. File backups, on the other hand, are utilized to make sure all important documents are backed up as often as necessary to avoid losses. Since file backups skip quickly all unchanged portions of your file server structure, they can run several times a day without having an impact on your server's quality of service and without consuming excessive backup storage.

Virtual machine backup is a specialized backup process where backups of virtual machines are taken from the host without interrupting or otherwise interfering with the virtual machines on the host. The virtual machine backup process talks to the virtualization platform (for example, Hyper-V) to bring the VM into a consistent state before backup. It then takes a consistent file backup of all relevant VM files, which are then compressed, encrypted, and or deduplicated.

## Compression

Compression is a method by which the size of a file is reduced based on repetitive patterns within a file's content. For example, if certain words repeat many times inside a Microsoft Word Document, the compression program replaces each word with a much shorter code.

Some types of files usually do not contain repetitive patterns. For example, WAV, AVI, MP3, and other media or music files are usually not compressible because their content is random and not repetitive.

On the other hand, text files, program files, databases, and virtual machine image files, usually contain a good portion of blank space and repeated blocks; hence, it is recommended to compress such files.

BackupChain Backup Software is shipped with various presets so that it turns compression on and off automatically depending on the type of a file; however, you change the configuration and determine yourself whether you want to compress a given file type or not.

## Encryption

Encryption is a method that "randomizes" data to a point where it cannot be recognized. Symmetric cyphers are programs that use the same password and method to encrypt and decrypt information. If you decide to encrypt your files, BackupChain will use an AES256 symmetric cypher to encrypt your files. AES is an open international industry standard for data security and is considered one of the most secure and efficient algorithms for encryption (see

[http://en.wikipedia.org/wiki/Advanced\\_Encryption\\_Standard](http://en.wikipedia.org/wiki/Advanced_Encryption_Standard) for more information.)AES256 is also HIPAA compliant.

Without a password it is usually impossible to recover an encrypted file. Therefore if you forget your password there is no way to restore your backup files.

## Deduplication (Delta Compression)

Deduplication, also known as Delta Compression, is a method that compares a file to its previous contents. For example, if an *incremental* daily file backup is generated, BackupChain compares yesterday's copy with today's file contents to find the actual differences. Then, a delta file is generated that contains only the changes.

*Differential* deltas compare the changes that occurred between now and the *first* backup that was taken (also called "full delta" or "full copy").

Because delta files (the detected file content changes between backup cycles) may contain repetitive patterns, it makes sense to compress them as well. BackupChain is configured to compress delta files automatically to save even more space in your backup folder or device.

## Backup Tasks

A backup task is a group of items you wish to back up in one process. For example, you can configure BackupChain to back up your My Documents folder and your virtual machines at the same time.

Backup Tasks may be scheduled to run at predetermined times, such as every 30 minutes, every night at 10 PM, or weekly on Saturdays.

With BackupChain you can set up as many tasks as you need and run them simultaneously if necessary.

## Scheduler: The Auto-Pilot

A scheduler is a background process that starts backup tasks automatically when the trigger event occurs. BackupChain runs a scheduler as a Windows Service in the background; hence, you do not need to be logged on to Windows for backup tasks to start. As long as the computer is switched on, backups will start at the configured time intervals.

BackupChain's scheduler supports several types of schedules:

**Continuous:** Run a task at given intervals. For example, every X minutes, hours, days, or weeks. The task will be repeated indefinitely at specified intervals.

**Daily:** Run tasks every n days at a particular start time. For example, at 8 AM every third day, or 11PM every night.

**Weekly:** Run tasks on specific days every nth week. For example, you can set up a task to run on Mondays, Wednesdays, and Sundays at 9PM every second week.

**Monthly:** Run tasks on specific months, days of the month, and weeks of the month. Example #1: Run backups on every 2<sup>nd</sup> day of each month. Example #2: Run tasks every third Monday in January, March, and June.

## Network Folders

A network folder (or network share) is a data folder located on another computer connected through a private local area network (LAN) or VPN (virtual private network).

There are two ways to access network shares and both require authentication. Authentication is the transmission of a user name and password to the other computer before the remote computer grants access to its files.

One way to access the network folder is using a UNC path. This is the method supported by BackupChain and it's also the most flexible method. These are several examples of UNC paths and how they should be entered in BackupChain:

`\\computername\foldername`

`\\computername.domainname\foldername`

`\\<ip address>\folder` as in: `\\192.168.1.1\foldername`

When connecting to a network folder it's very important to let Windows know how to authenticate. The user name should be prefixed with the domain or server network name or address to make it clear how the authentication is to be made.

Examples for user names, instead of joe use: `joesdomain\joe` (in a domain setting)

OR

`192.1.3.5\joe` (in a workgroup or mixed setting to authenticate as user Joe created on server with address 192.1.3.5)

OR

Fileserver4\joe (in a workgroup or mixed setting to authenticate as user Joe created on server "fileserver4")

## Domains and Workgroups

A Windows Domain requires a Domain Controller, which is a computer that manages user accounts and their access permissions. Workstations and servers authenticate with domain controllers in order to obtain access to resources on the local network.

A workgroup is a decentralized network approach without a domain controller. In a workgroup, computers share resources when they belong to the same workgroup.

## Windows User Accounts

Microsoft Windows uses a user session concept to protect your computer and network from unauthorized access and damage resulting from malicious software, such as viruses.

Users may have restricted rights. For example, the built-in SYSTEM user has access to almost everything, while a guest user account may not be allowed to access certain folders on the computer. Similarly, you can share a folder to others on the network and specify which users can read and who is permitted to write and delete inside that folder.

Most people are not aware of it but your computer runs several user sessions simultaneously. Each Windows PC has a SYSTEM user and several other users with restricted access to files and network resources. BackupChain's background service, which actually runs the backups even when you are not logged on to Windows, runs in the session of the local system user.

Anti-virus programs and other services on your computer run in different user sessions, invisible to your personal user session. *It is important to know that network connections are not visible to other user sessions. **Mapped drives and network shares cannot be created and authenticated in one session and accessed by another.*** Hence, if you personally have access to a network folder, these access rights are private to your user session. Other user sessions, such as the local system user, do not have the same access permissions as you have. This was done that way for several reasons. First it protects your machine from virus damage and security breaches. Second, it allows several people to work simultaneously on one single computer (this is especially important for servers).

## Authentication

When connecting to a network drive it is important to understand how authentication works.

In Microsoft Windows, each computer may have several user accounts of its own and several users may be logged in to the same computer simultaneously. For example, you may be logged in physically as user “Sven” and system processes in the background may be using internal user accounts to run applications, such as “SYSTEM”. In addition, Windows Servers permit multiple administrators to work via Remote Desktop on the same server simultaneously, each with their own account and desktop screens.

Problems may arise when several users connect to the same remote server or when several similar user names exist. This is why you should use the following pattern to connect to a network share:

`\\servername.domainname\foldername`

And then log in using this use name pattern:

`Domainname\YourDomainUserName`

If connecting to a computer that isn't on a domain:

`\\ RemoteServerName \FolderName`

And use this user name pattern:

`RemoteServerName\UserNameOn RemoteServer`

This method ensures Microsoft Windows understands which user and which server you mean.

On a simple network without domains you can use a simpler login:

`\\servername\folder`

And log in with the user name.

## Common Network Connection Challenges

BackupChain runs backups in a background service called “BackupChain Service” and it is using the local system user session. **Note:** Backups do not run in the application visible to the user. Because the

background process uses the local system user, that user needs to authenticate separately with each network server used.

Your own user session may be connected to the network share but the local system user is a separate session which has its own set of network connections, different from yours. When you add a network share to BackupChain, it uses the login credentials you entered to authenticate with the other computer on the network.

**Note:** You cannot use two different users to connect to the same server on the network. Example: Say you have a server named *dataserver* and it contains two shares: *datafiles* and *musicfiles*. You can use Dataserver\user1 to connect to [\\dataserver\datafiles](#) and [\\dataserver\musicfiles](#)

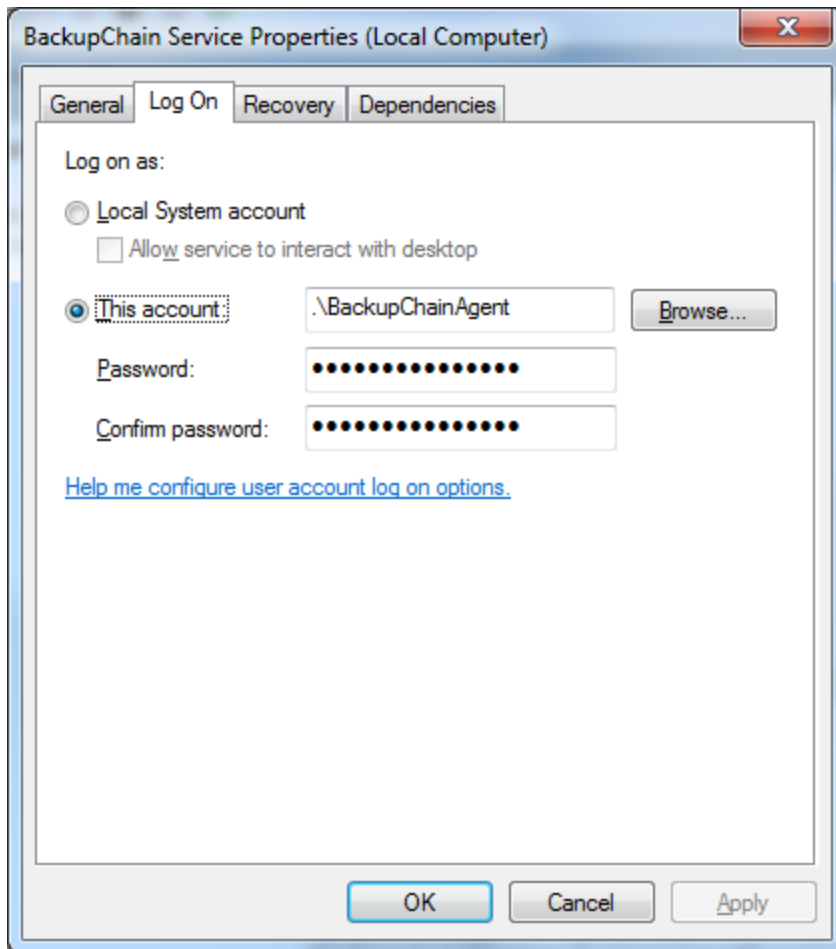
You cannot connect two users to connect from one PC to one server:

Dataserver\user1 to connect to \\dataserver\datafiles

And Dataserver\user2 to connect to \\dataserver\musicfiles

**Note:** The above limitation is a Microsoft Windows limitation and applies across all user sessions on your computer. Hence you need to give the BackupChain the same user credentials that you use personally in your user session. You cannot connect two different users to the same remote server simultaneously.

An alternative is not to use the local system user for BackupChain's background service. Open the Service Manager or Services from the Control Panel using the Windows Start menu. Look for the service called "BackupChain Service" and open its properties (see screenshot below). Navigate to the Log On tab and change the user from local system account to a local administrator or a domain administrator. If you are on a domain, that user needs to be a local admin and also have permissions on the remote server. If you want to change the user for BackupChain's background service you have to select a local administrator user.



### Network Drives Accessed via a Mapped Drive Letter

**Do not use mapped drives** in BackupChain. In fact, BackupChain will not show mapped drives in the folder and file selection screens. The reasons have been stated in the previous section.

**Mapped drives are user session specific.** BackupChain's background service runs as local system user and does not have access to the mapped drives you use personally when you log in using your own user name.

Instead you need to provide a UNC path to the network share with user name and password, see section above. You may also need to change the Windows user for the BackupChain's background service as described in the previous section.

## What can BackupChain do for my business?

BackupChain Backup Software is specifically designed for small to medium sized companies and offers you a multitude of configuration options so you can fully control your backup processes and the characteristics of your backup data.

### Mitigate Risks of Data Loss

Naturally the main function of backup software is to prevent data loss as much as possible. You need to have a good sense of all common risks of data loss because most forms of data loss are preventable.

These are some typical causes of data loss:

- Fire.
- Storms.
- Floods.
- Software faults and errors, including the operating system.
- Accidental deletion by users.
- Hard drive faults: head crash, deterioration, etc. The expected lifetime of hard drives is usually under two years.
- Virus, ransomware, and malware damage.
- Static discharge. For example on days with low humidity below 40% and carpets installed in the office. Vacuum cleaners and other devices may be statically charged as well. Be aware of this when near a computer.
- Humidity levels and condensation. Ideal levels should be kept between 40% and 60%. High humidity levels can cause condensation. Dry levels can damage electronic parts.
- Electric shock caused by lightning strike to exterior structures in the vicinity of the building or power lines.
- Electric surge caused by lightning or defect electric appliances connected in the same office or household.
- Water damage. Fire sprinklers, flooding, or other leaks.
- Temperature. Do not expose computers to temperatures below 15 degrees Celsius (60 degrees Fahrenheit) or above 27 degrees Celsius (80 degrees Fahrenheit) because electronic parts may overheat. Low temperatures may lead to condensation.
- Mechanic shock. For example, a notebook may be dropped or a desktop may be struck accidentally while the hard drives are spinning.
- Magnetic fields. Magnetic fields caused by older TV sets or wiring can damage the sensitive plates inside hard drives or electronic components on motherboards.

- Incomplete data transport. For example data is copied to a new computer and users may not notice that the transfer was not complete.

## Protect Your Data Efficiently and Economically

Using BackupChain you can plan your backups and thereby save time, money, storage space, and bandwidth. In addition, the built-in FTP server and client features allow you to set up your own remote backup system.

## Deduplicate and Save Space by Removing Redundancy

The deduplication (delta compression) technology offered by BackupChain offers incremental and differential backups at the file level and is optimized to work with very large file sizes (> 1TB).

The deduplication process works as follows: first, a compressed full file copy is generated. At the next cycle, BackupChain compares the current file to its previous version in the backup store. It extracts the changes and creates an incremental delta file. Differential backups always compare the current file to its most recent full copy in the backup store.

## Incremental Backup

Incremental backup may also mean that only changed files are backed up. BackupChain skips files automatically if they haven't changed since the last backup. Incremental backup may also refer to 'deduplication', also known as delta compression. See previous section on how BackupChain performs deduplication on a file basis.

## Run Backups while You Work

BackupChain runs in the background and can process locked or exclusively opened files as well. For example, BackupChain can back up your Word document while you are writing it and back up databases and virtual machines while they are running without service interruptions.

## **“Owning” your Own Data – No Technological Lock-In**

Many other tools lock you in technologically to their software. Once you make a backup, so-called container files are produced in the backup store. These container files are usually in a proprietary format that cannot be opened using standard tools; hence, even if you have backup you may not be able to get access to your own data unless you use the software that generated it.

BackupChain does not use container files. BackupChain replicates the exact folder structure from the original folder to the backup media. It uses open-standard file formats, such as ZIP or 7Z files which can be opened on any computer without BackupChain. The only exception is the “FastNeuronDelta” format which is BackupChain’s proprietary file format for incremental / deduplicated file backup. This format is necessary because there is no open standard for deduplication; however, you can fully configure how, if, and when to use each file format to match your specific in-house backup requirements.

## **Sector-Level Disk Image Backup (P2V, V2P, P2P, V2V)**

Sector-level disk image backup in BackupChain offers several advantages. Physical disks can be copied to either physical disks or virtual disks and vice versa. The supported formats are VHD, VHDX, VDI, and VMDK. The resulting physical to virtual (P2V) or virtual to physical (V2P) conversions are bootable as VMs or physical machines in most circumstances. Virtual disks may be mounted to Windows (VHD, VHDX, depending on Windows version) or you can use the BackupChain tool to access disk images and restore files individually without restoring the entire disk image.

### **Physical to Physical Disk Copy (P2P) / Disk Cloning**

Copying physical disks to physical disks on a schedule allows you to always have an independent boot disk or data disk available when the original disks fail.

- Copy RAID array disk contents to a single disk, which can be simply plugged in or brought online (via Windows Disk Management) when needed. Or the disk can be plugged into another server at any time.
- Copy the system disk or data disk to another disk. Unlike a typical mirror RAID you now have some reaction time in case of a virus attack or accidental deletion. Also the disk can be placed offline or physically removed from the server for additional safety and security, for example to protect against ransomware or theft.

See the section “Create a new disk backup task” on page 29 for detailed how-to instructions.

### **Physical Disk to Mounted Virtual Disk Copy: Disk to Disk Copy over LAN**

Physical disk to a virtual disk appearing as physical can be achieved over the network:

Create VHDs on target server and share the VHD files using a network share. Mount the VHDs on the other server where you plan to run the backup via Disk Management. They now appear as “real” physical disks even though they are VHDs stored on a network server.

Then create a physical disk to disk copy task in BackupChain to copy each disk to its own target disk. In case of a disaster the disks are immediately accessible on the target server or any other server over the network. The VHDs can be attached to VMs if need be (and booted) or simply attach them via Disk Management to any computer you want to access files immediately.

See the section “Create a new disk backup task” on page 29 for detailed how-to instructions.

### Live VM Conversion (V2V)

Another unique feature in BackupChain is its ability to back up live virtual machines into a different virtual disk format, while running and without interruptions. You could for example, convert a VM from VMware Workstation to Hyper-V or VirtualBox and vice versa.

See the section “Create a new disk backup task” on page 29 for detailed how-to instructions.

### Physical to Virtual (P2V) and Virtual to Physical Conversion (V2P)

A virtual disk can be converted and copied to a physical disk and vice versa.

See the section “Create a new disk backup task” on page 29 for detailed how-to instructions.

## General File Backup

File backup is more than just a simple file copy. BackupChain can be configured to keep track of file histories so you can go back in time and restore old versions of a file.

In addition, BackupChain uses VSS technologies to obtain valid, consistent, and reliable live copies of files when these files are in use. Copying files by hand does not provide a consistent view of the files and folders being copied. Some application or another user may be modifying, moving, adding, deleting files while the folder is being copied. The result of a manual copy is hence not guaranteed to contain exactly the same information as when the copy began. BackupChain, on the other hand, uses a snapshot mechanism to guarantee that all files and folders are copied exactly and consistently to the target media, as they were when the backup commenced, even if the backup job takes a long time and other users have since modified the files being backed up.

BackupChain can be configured to process files depending on their type. For example, you may wish to ZIP compress Microsoft Word files and keep the last 100 versions of each document, but in the same task you may want to deduplicate VMDK files with compression and set a file version limit of only three copies.

Files may be backed up to a network share, an external drive, a local drive, or an FTP / FTPS server.

## Virtual Machine Backup (Hyper-V, VMware, VirtualBox, CSV)

BackupChain's tools are optimized to perform live virtual machine backups using Hyper-V (including Cluster Shared Volumes), VMware, VirtualBox, and other platforms that are VSS compliant.

For Hyper-V, BackupChain offers a single-click and restore feature which configures itself automatically. For other platforms, such as VMware, simply point BackupChain to the folder containing the virtual machine files.

An important part of virtual machine backup is deduplication (delta compression). Instead of generating full virtual machine copies, BackupChain detects the changes that occurred between backup cycles and extracts and compresses them into a delta file. Using this technology a daily backup is usually only 1 to 5% of its original size.

Another important strength of BackupChain is its quick processing ability, which can be configured to use all available CPU cores during deduplication.

## Database Backup

Databases contain a lot of redundancy; therefore, data compression and deduplication are very effective means to back up database files.

BackupChain's delta compression feature performs a quick scan and generates delta files of each database every time it backs them up. This is the fastest and most economical way to back up database container files.

## Set up Your Own Online Backup System

One of BackupChain's unique features is its built-in FTP / FTPS server. An FTP server is needed to receive backup files from other computers over the Internet.

Many customers use BackupChain to connect their office and home computers or connect two servers in different offices. The idea is to back up one computer's files to the other and vice versa. That way you don't need to have a backup store or pay for online storage because each computer uses the other as its backup store.

In addition, you can set up a centralized backup server and have workstations back up to that centralized server locally or over the Internet.

Alternatively you can use a compatible standard FTP server on the Internet that is hosted by a third party.

Many online backup hosting services have switched to BackupChain. Using BackupChain at the client site as well as the receiving end eliminates most incompatibility problems that other solutions involve. Contact FastNeuron sales or support for more information if you plan to deploy BackupChain in a large scale environment.

## Getting Started

### Minimum Requirements

- A Microsoft Windows PC or Server with 1GB RAM.
- Ensure at least 512 MB RAM are available for optimum performance.
- Supported Workstation Operating Systems: Microsoft XP, Vista, Windows 7, Windows 8, and Windows 10.
- Supported Server Operating Systems: Windows Server 2003, Windows Server 2008 R1 / R2 incl. Core Installations, and Hyper-V Server 2008 R2. Windows Server 2012 / R2, its Core installations, Hyper-V Server 2012 R2, Windows Server 2016 and Hyper-V Server 2016, Windows Server 2019 and Hyper-V Server 2019.
- A .Net framework installation is almost never necessary. BackupChain can run on .Net Framework 2.0 (already included in Vista, Windows 7, and Windows Server 2008); .Net Framework 2.0 SP2 is recommended if only .Net 2.0 is installed, but not required. .Net Framework 4 is also supported (preinstalled in Windows 8, 10, Windows Server 2012 – 2019) and a separate .Net 2.0 or 3.5 installation is not required. BackupChain can run on either or both framework versions. A .Net Framework installation is hence not required in all current cases, except from Core installations of Windows that do not have any .Net runtime installed. For more information for Windows Core .Net installation, visit <http://backupchain.com/dotnet>
- System drives should have at least 10% free space available or 5 GB (This is not for BackupChain but to ensure enough resources are available during the backup process).

### Feature List

- Live Virtual Machine Backup
- Live disk backup (physical to physical disks, physical to virtual disks, virtual disk to physical, and virtual to virtual disk)
- Optional secure login requirement to prevent unauthorized access to backup settings
- Ability to remotely control other instances of BackupChain via a centralized console view
- Configurable file backup settings per type.
- Live database backups
- Verification of sector-level disk backups at file and sector level
- Verification of file level backups, stored locally and at remote sites
- Parallel, multitasked file backup also available within a single task.
- Parallel backup job execution (Backup Concurrency).
- Configurable CPU core usage (1 to all CPU cores).

- Configurable retention period in time periods and also in number of backup versions.
- Delayed deletion: configurable time to retain files that have been deleted at the source.
- Quick and economic incremental and differential backups.
- Continuous Server Backup and Protection.
- Efficient Locked File Handling via VSS.
- Built-in FTP and FTPS Server (secured and encrypted FTP over TLS).
- Remote Backups using built-in FTP / FTPS Server.
- In-file Delta Compression / deduplication create smaller backups and minimize bandwidth requirements.
- Fully Configurable File Versioning based on file types.
- Advanced Scheduler.
- Email Alerts.
- Capable of backing up millions of files of any size.
- FTP / FTPS backups.
- Network to disk, disk to network, and network to network backups.
- Granular backup (backup files stored inside VMs from the host)
- Granular restore (restore files from VM disk images and physical disk images without having to restore the entire disk)
- Military-strength encryption AES 256 (FIPS and HIPAA compliant).
- Unattended mode runs in a Windows service.
- Backup concurrency: Start several backups at the same time.
- Full CPU utilization (limit to one CPU core is possible).
- Unicode file name handling: all languages supported.
- Support for ultra-long file names (32768 characters long), even when creating ZIP files and using FTP.
- Support for files larger than 4GB even with ZIP compression (64-bit file sizes are possible).
- Selective file restore of old file versions; search for old versions via date and time filter.
- All Windows Server Editions (2003 to 2016) and Workstations XP, Vista, Windows 7, Windows 8, and Windows 10 are supported.
- Support for Hyper-V Server 2008 / R2 and Windows Server 2008 / R2 Core installations.
- Support for Hyper-V Server 2012 / R2 and Windows Server 2012 / R2 Core installations.
- Support for Hyper-V Server 2016 and Windows Server 2016 Core installations.
- Support for Hyper-V Server 2019 and Windows Server 2019 Core installations.
- Restores file folder structure as of time of backup.

## Installation Instructions

You need administrator rights in order to install BackupChain.

Download the BackupChain package <http://backupchain.com/BackupChainSetup.zip>  
and run it as administrator.

### **On Hyper-V Server 2008 R2 or Windows Server 2008 R2 Core Installations**

From the command line execute the following commands to install the .Net Framework 2.0:

```
start /w ocsetup NetFx2-ServerCore
```

```
start /w ocsetup NetFx2-ServerCore-WOW64
```

If the above lines do not work with your Hyper-V OS version, try these:

```
DISM.exe /online /enable-feature /featurename:NetFx2-ServerCore
```

```
DISM.exe /online /enable-feature /featurename:NetFx2-ServerCore-WOW64
```

Then change directory to the folder containing BackupChainSetup.exe (available from our download page) and run:

```
BackupChainSetup.exe
```

To start BackupChain after installation, run: C:\Program Files\FastNeuron  
Inc\BackupChain\BackupChain.exe

### **On Hyper-V Server 2012 - 2019 or Windows Server 2012 -2019 Core Installations**

The .Net Framework v4 is already preinstalled; there is no need to install anything.

To start the BackupChain Monitor after installation, run: C:\Program Files\FastNeuron  
Inc\BackupChain\BackupChain.exe

### **On Windows 8, Windows 10, Windows Server 2012 - 2019 Installations**

The .Net Framework v4 is already preinstalled; there is no need to install anything.

## **Introducing BackupChain Backup Software Features**

This section describes each feature step-by-step to give you a complete tour of the product.

## Sector-Level Disk Backup Strategies

Disk backup can be done in very many combinations of strategies and each strategy offers its own pros and cons.

**How Disk Backup Works:** A consistent view of the disk contents is obtained by VSS. VSS also ensures that services prepare for live backup and prepare their data structures on disk so that the resulting disk image is application-consistent as well as crash-consistent.

**Important Note:** VSS cannot ensure consistency of non-Windows partitions and disks and offline disks. For example, if you attach a physical disk directly into a VM, that disk cannot be backed up from the host; instead, it must be backed up from inside the VM.

**Disk backup via disk copy:** By setting up a live disk to disk copy task you can clone a physical disk to another and have it ready to boot or access when disaster strikes. You will have to use a disk of the same exact size or larger than the original. This strategy also works with RAID disks that may be implemented using several disks combined. For example a three disk stripe array can be copied to a single disk with sufficient capacity. The clone can then be booted alone if the RAID fails.

Make sure your boot settings are configured to force booting from the “correct” disk. Once you have several bootable disks in the server, the BIOS might use the “wrong” one next time you boot.

**Disk backup via virtual disk conversion:** BackupChain can create a virtual disk (formats: VHD, VHDX, VMDK, and VDI) from a physical disk. You can use this strategy to create a bootable virtual disk that can be mounted to a virtual machine and booted at any time. VHDs and VHDX may be used to boot directly from if added to the Windows boot configuration via bcdedit.exe

**Virtual to virtual disk backup:** Say you have a VM running Hyper-V. On your backup server you have VMware Workstation. You can convert the Hyper-V VM live and without interruptions into a VMDK, which you store on your backup server. There you can boot the VMDK any time you want. BackupChain can convert any VM from and to Hyper-V, VirtualBox, VMware Workstation / Server, and Virtual PC in all combinations.

**Virtual to physical (i.e. Disk restore):** You can copy the contents of a virtual disk back to a physical disk and boot from it with a physical machine. By backing up your physical disks to virtual disks and restoring from virtual disk to physical, you have basically implemented a traditional backup scheme where the virtual disk is the backup medium.

**Remote disk backup via copy:** Mounted virtual disks are offered in Windows 7 and Server 2008 and later. You can mount VHDs that sit on a network share on your LAN somewhere. These virtual disks appear in Windows like a real physical drive. In BackupChain you can set up a task to copy the server’s disks to the mounted disks on a schedule. In case of a disaster, these VHDs can be mounted anywhere

on the LAN as physical disks and you can access data from them directly. Alternatively you could attach these VHDs to a virtual machine and boot immediately.

## Backing up Virtual Machines

Please refer to the Tutorial section on page 134 onwards. The sections below discuss general features, such as email alerts, scheduler, etc.

## Creating a New Disk Backup Task

This section explains how to back up, copy, or convert **entire disks** using a “disk to image backup” task. If you want to back up file server documents, virtual machines, or databases, please refer to the next section: “Create a New Task” on page 46.

### Definition of terminology

This manual uses the terms “conversion”, backup, and copy interchangeably. Physical disks are converted to other physical disks or virtual disks. A conversion is similar to a copy and can be used as a backup image file that you can use to restore the entire system from. Copying from disk to disk may include additional operations beyond the straight copy and is hence more of a conversion than a true copy.

### Disk Cloning

Windows requires all mounted physical disks to have unique identifiers. Copying disks on a live system, hence, requires that the “copy” must be assigned a new identity before it can be mounted. BackupChain takes care of this issue so that Windows permits the original and the “clone” to coexist side-by-side without clashes. However, BackupChain performs some modifications on the target disk in order to achieve this. If you are using a 3<sup>rd</sup>-party boot loader, other than the standard Windows boot loader, the cloned disk might, if it is a Windows operating system boot disk, not boot correctly.

### Getting started

To create a new disk backup task, click “New Task” from the main window, select “disk to image backup” and enter a task name:

**Create a New Backup Task Wizard -- BackupChain**

Select Backup Type | Help | Disk Imaging | Finished

**Welcome to BackupChain's Backup Task Wizard!**

This wizard guides you through the main functions of BackupChain and assists you in setting up a backup task. Backup tasks store all your settings for future use. Tasks may be scheduled or may be run manually whenever you need to run a backup. Once saved, you may fine-tune your backup task later in the Main Screen, where all features of BackupChain are available.

Create Task on Server: **backupchain-PC**

Enter a Task Name:

Please select the purpose of this backup task:

**I want to back up documents and file server data...**

☐ **File-Level Backup**  
(File Server and Version Backup.  
Use for file server data, documents, etc.  
Files are placed individually in backup folder.  
Do not use for VMs)

**I want to back up virtual machines...**

☐ **Hyper-V Backup (Server)**    ☐ **Hyper-V Backup (Client)**    ☐ **VMware Backup**    ☐ **VirtualBox Backup**  
(Automatic or Granular Backup)    (File-based, recommended only for Windows 8-10 + Pro Edition)    (VMware Workstation, Player, VMware Server backup)

**I want to back up the Windows boot disk or sector-level backup...**

☒ **Disk to Image Backup (Sector-Level)**    ☐ **Disk Cloning (Sector-Level)**    ☐ **Restore Disk Image Backup (Sector-Level)**  
(Sector-based backup of a physical disk into a disk image file. This is usually only done to back up operating system disks)    (Sector-based copy of a physical disk to another physical disk. This can be used for Windows operating system boot disks as well as data disks)    (Restore a disk image file to a physical disk)

**I want to convert physical and virtual machines / disks...**

☐ **P2V**    ☐ **V2P**    ☐ **V2V**  
(Physical disk to virtual disk conversion)    (Virtual disk to physical disk conversion)    (Virtual disk format conversion)

**Other backup task types:**

☐ **SQL Server Backup**    ☐ **Universal Backup**  
(Backup SQL Server and MSDE Databases)    (Backup all VSS aware services. Use only if no other backup type suits)

**Go Back**    **Next Step**

Then click “Next Step” and have a read through the various helpful hints that appear. Then click “Next” again to reach the following screen:

bc Create a New Backup Task Wizard -- BackupChain

Select Backup Type Help Disk Imaging Finished

Below select the source disk and target disk. If you want to back up several disks simultaneously, click "Add Disk" to add additional backup steps.  
For P2V, V2P, and V2V conversions, simply select the source disk type and target disk type to set up the kind of conversion you need.

Disk Step #1 [Hide Settings](#)

Disk Selection Options

Backup Type  
Selected Backup Type: Disk to Image: Copy physical disk to virtual disk image (P2V)

Source Disk  
Selected Source Physical Disk:  Select

Target Disk Image File  
Target File:  Browse

Virtual Disk Format  
☐ VHD (≤ 2TB)
 ☒ VHDX (≤ 64TB)
 ☐ VMDK (≤ 2TB)
 ☐ VDI (≤ 2TB)

Virtual Disk Type  
☐ Same as Original
 ☐ Pre-allocated, Fixed Size
 ☐ Pre-allocated, Sparse
 ☒ Dynamically Expanding

☐ Apply universal boot settings

Add Disk Help Refresh

Go Back Next Step

In the above screen you need to choose the type of backup ("disk to image" is preselected above), then the physical source disk and the target file for your backup image.

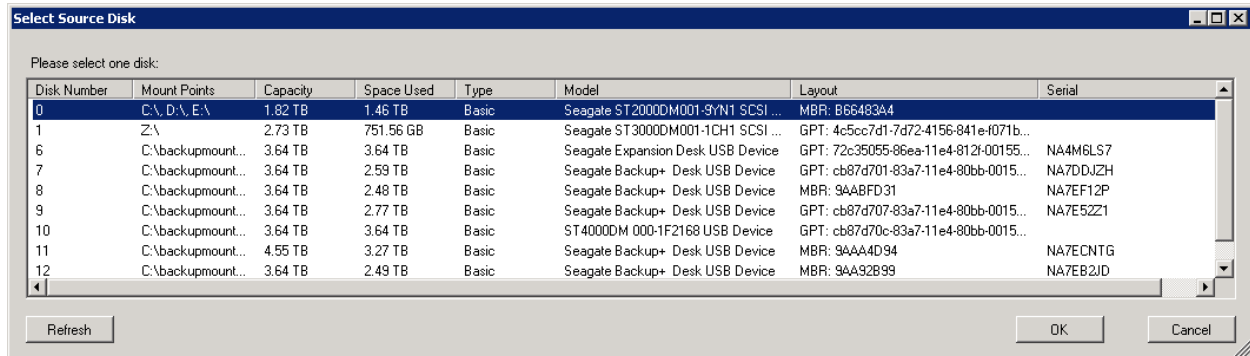
### Disk to image backup (Copy physical disk to virtual disk image)

Copying a physical disk to a virtual disk creates a backup file with the disk contents on it.

You can later

- Restore the machine by copying the virtual disk back to a physical disk.
- Mount the virtual disk to extract files and folders (VHD and VHDX via Windows Disk Management), or use BackupChain's granular restore tool (Disk Tools->Browse Disk Images and Virtual Disks) for all formats
- Immediately boot the virtual disk as a VM by creating a "dummy" VM and attaching the virtual disk to the virtual IDE controller.

Click the Select button to choose from all installed disks on your server:



BackupChain supports raw disks, basic and dynamic disks (see <https://technet.microsoft.com/en-us/library/bb726994.aspx> for definition of terms), and GPT as well as MBR partition layouts.

After you select your source disk, click OK. The selection then appears in the backup/conversion step:

**Create a New Backup Task Wizard -- BackupChain**

Select Backup Type | Help | Disk Imaging | Finished

Below select the source disk and target disk. If you want to back up several disks simultaneously, click "Add Disk" to add additional backup steps.  
For P2V, V2P, and V2V conversions, simply select the source disk type and target disk type to set up the kind of conversion you need.

Disk Step #1 [Hide Settings](#)

Disk Selection Options

Backup Type  
Selected Backup Type: Disk to Image: Copy physical disk to virtual disk image (P2V)

Source Disk  
Selected Source Physical Disk:  
Disk #1: 238.47 GB (E:\), GPT, EFI(Boot), Model: Samsung SSD 860 PRO 256GB ATA Device, Serial: 34533831474e4b413031343 Select

Target Disk Image File  
Target File: Browse

Virtual Disk Format  
☐ VHD (≤ 2TB)
 ☒ VHDX (≤ 64TB)
 ☐ VMDK (≤ 2TB)
 ☐ VDI (≤ 2TB)

Virtual Disk Type  
☐ Same as Original
 ☐ Pre-allocated, Fixed Size
 ☐ Pre-allocated, Sparse
 ☒ Dynamically Expanding

☐ Apply universal boot settings

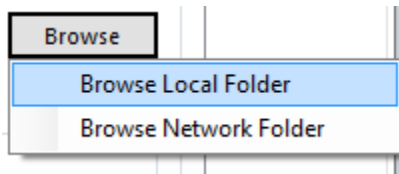
Add Disk Help Refresh Go Back Next Step

**Note:** Dynamic physical disks must be converted all combined in one step by adding additional disks to the above screen using the Add Disk button. Dynamic disks in Windows (not to be confused with expanding virtual disks, see <https://technet.microsoft.com/en-us/library/cc737048> for a definition) allow spanned, striped, and mirrored volumes that may span several disks. If you want these disks imaged you must select all of them to be converted simultaneously. You can add additional conversion steps (i.e. disks) by clicking the "Add Disk" button. Each disk will then be converted to its own virtual disk or physical disk target.

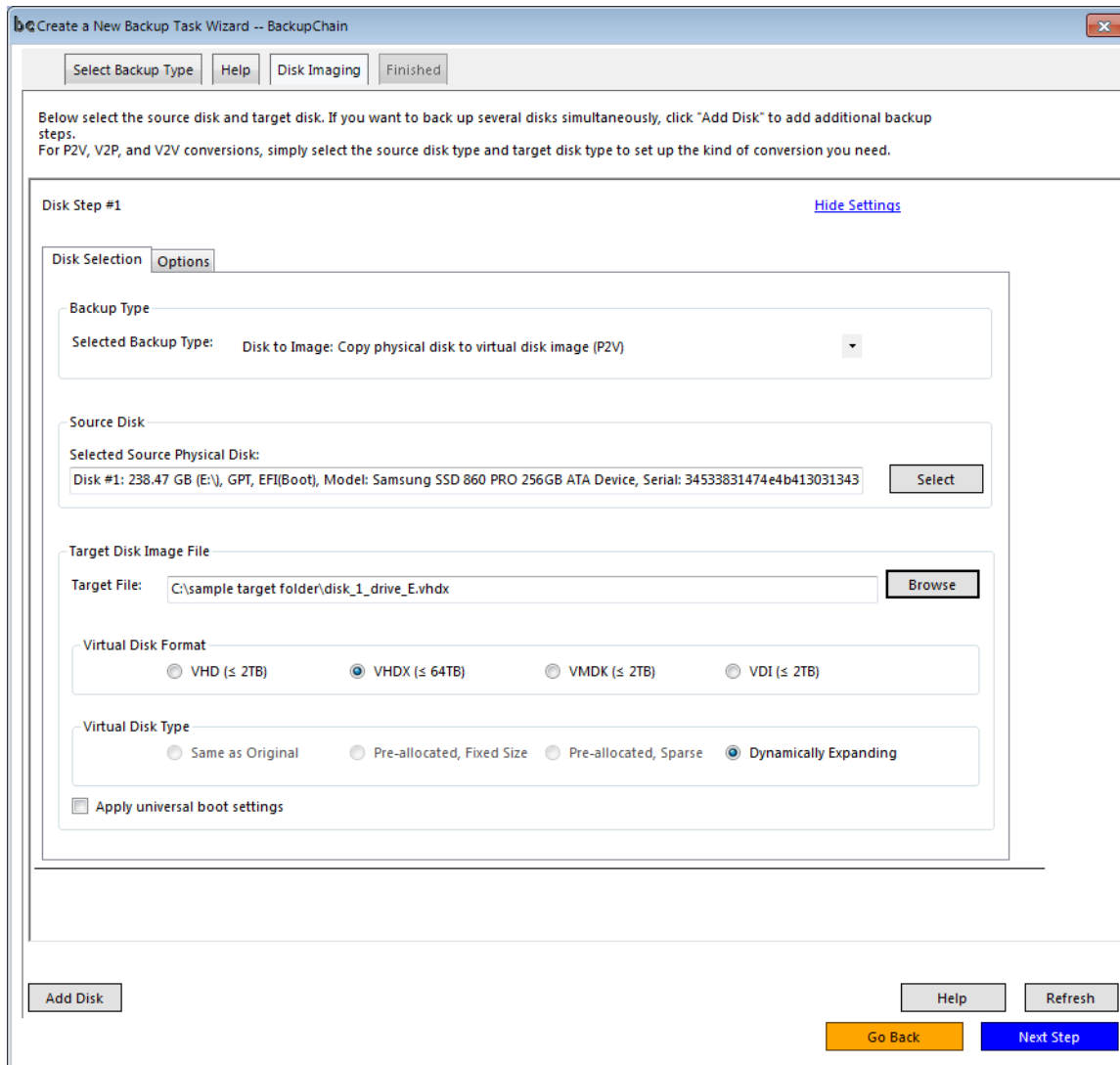
### Specifying the target file

Enter the full file path to the virtual disk you would like to create or click browse to select a target file location or network location. Our example below backs up to Z:\backup-vhds\servermaindisk.vhd:

Click “Browse” to specify the target image file, which could be stored on a local disk path or a network share.



Once you select your target folder, the ‘target file’ field shows your selection:



Below the target file you see several options. The first row is the target format (VHD, VHDX, VMDK, and VDI). The only format that supports disks larger than 2TB is VHDX. If you intend to use your backup file to boot the image as a virtual machine, note that VHD and VHDX can be used in Hyper-V, and all formats

except VHDX should work in VirtualBox. VMware Workstation and Player can handle VMDK and VHD, whereas for ESX/vSphere you need VMDK.

The above screen requires at least two choices to be made: the virtual disk format (VHD, VHDX, VMDK, and VDI) and whether you want a pre-allocated, fixed sized virtual disk or a dynamically expanding virtual disk.

A dynamically expanding virtual disk will only hold the data volume that is actually occupied in the physical disk and will hence be smaller than the original disk. For example, if your physical disk is 2 TB and only 100 GB are occupied, the virtual disk grow to be around 100 GB as well after the backup completes.

#### Choosing a virtual disk target type

If your source disk, the physical hard disk, is 2 TB or less, you can choose any virtual disk type; however, if your disk is above 2 TB you can only use VHDX.

Note that VHDs can be used in Hyper-V and some versions of VMware Workstation and VirtualBox. VHDs may be mounted to Windows 7 and Windows Server 2008 and later.

VHDX, at the time of this writing, can only be used in Hyper-V or mounted as a disk in Windows 8 or Windows Server 2012 and later.

VMDK can be used on VMware Workstation and ESX. VMware offers a tool to mount VMDK as a disk to Windows.

VDI can be used in VirtualBox.

All formats can be opened in BackupChain for a granular restore via the main menu Disk Tools->Browse Disk Images & Virtual Disks. There you can restore / extract individual files and folders without having to restore the entire disk.

### *Physical to Physical Disk Copy (Disk to Disk: Sector level copy)*

Physical disk copy allows you to have a copy of your hard drive immediately accessible.

Example usage:

- Copy RAID array disk contents to a single disk, which can be simply plugged in or brought online (via Windows Disk Management) when needed. Or the disk can be plugged into another server at any time.

- Copy the system disk or data disk to another disk. Unlike RAID you have some reaction time in case of a virus attack or accidental deletion. Also the disk can be placed offline or physically removed from the server for additional safety and security.
- Copy multiple disks to another set of disks for a complete clone of the current server.
- Physical disk to disk backup over the network: Create VHDs on another server and share them using a network share. Mount the VHDs on the other server where you plan to run the backup. The disks now appear as “real” physical disks. Create a physical disk to disk copy task in BackupChain to copy each disk to its own target disk. In case of a disaster the disks are immediately accessible on the other server or any other server over the network. The VHDs can be attached to VMs if need be (and booted) or simply attach them via Disk Management to any computer you want.

To copy one physical disk to another, select “Disk to Disk: Sector-level copy physical disk to physical disk” in the Disk Imaging tab screen as shown below:

Create a New Backup Task Wizard -- BackupChain

Select Backup Type Help Disk Imaging Finished

Below select the source disk and target disk. If you want to back up several disks simultaneously, click "Add Disk" to add additional backup steps.  
For P2V, V2P, and V2V conversions, simply select the source disk type and target disk type to set up the kind of conversion you need.

Disk Step #1 [Hide Settings](#)

Disk Selection Options

Backup Type

Selected Backup Type: Disk to Disk: Sector-level copy physical disk to physical disk

Source Disk

Selected Source Physical Disk:

Disk #1: 238.47 GB (E:\), GPT, EFI(Boot), Model: Samsung SSD 860 PRO 256GB ATA Device, Serial: 34533831474e4b413031343 Select

Physical Target Disk

Selected Target Physical Disk:

Disk #0: 3.64 TB (X:\), GPT, Model: TOSHIBA MG03ACA400 ATA Device, Serial: 4 14K276FF Select

Please check this setting carefully--this is the disk that will be deleted!

☐ Apply universal boot settings

Add Disk Help Refresh

Go Back Next Step

Then click "select" to choose the target physical disk.

**Note that the target disk will be deleted when the backup task is run.**

The target disk has to be either larger or the same exact size as the original. Virtual disks mounted in Windows (VHD or VHDX) using Windows Disk Management may also be used as targets or source disks.

**Note:** Please make sure your boot settings are configured to force booting from the "correct" disk. Once you have several bootable disks in the server, the BIOS might use the "wrong" one next time you boot and if they happen to be clones, it will be easy to confuse them as the original.

### ***Important notice regarding disk to disk live backups***

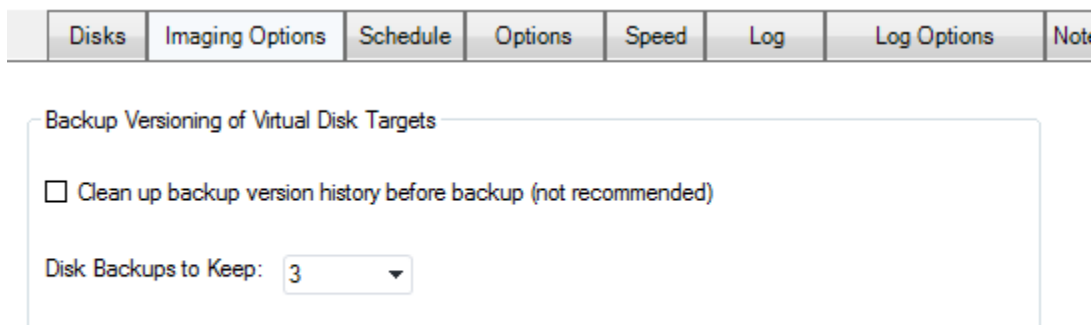
When copying one physical disk directly to another live (while Windows is running), BackupChain needs to make changes to the destination disk in order for Windows to be able to *function and boot correctly*

with both disks being mounted side-by-side. For example, BackupChain has to assign a new ID to the destination disk to avoid issues, since all operating systems expect each disk to have a unique identifier. In addition, the boot loader of the target disk needs to be modified to make the copied disk bootable just as the original. BackupChain can only take care of Windows boot loaders. If you are using a different boot loader product or operating system, you may need to edit the boot settings to work with the new disk ID.

If you intend to take the physical disk copy and boot it elsewhere, please ensure the BIOS is set to the same boot setting (EFI / UEFI or legacy) as the original server where the backup was made. It also helps to boot first into safe mode to give Windows an opportunity to switch critical boot-related drives if need be. In addition you can run the BackupChain tool “Prepare disk to boot as VM” (Disk Tools in main menu) and alter the boot settings before attempting to boot on completely new hardware. If possible try booting using an IDE / SATA port first. Once Windows is booted you can install RAID drivers if need be and attach the disk to a RAID controller.

### *Automatic Cleanup of Old Virtual Disk Backups*

Once you save the task, in the main screen you will find a new tab “Imaging Options”:



Disks	Imaging Options	Schedule	Options	Speed	Log	Log Options	Notes
-------	-----------------	----------	---------	-------	-----	-------------	-------

Backup Versioning of Virtual Disk Targets

☐ Clean up backup version history before backup (not recommended)

Disk Backups to Keep:

The above screen offers a field at the bottom “Disk Backups to Keep = 3” where you can specify how many backup files you wish to keep. The “3” above means you want to keep the last three virtual disk backup files created by BackupChain. After that, the oldest backup file will be deleted at the end of each successful backup cycle. You can change the number or enter ALL to keep all virtual disks created. Since each virtual disk created will be quite large, you will want to limit the number of virtual disks created depending on the backup storage size you have available.

Note that here BackupChain includes an additional option “Clean up backup version history before backup” which is not recommended unless you are using backup rotation or multiple backup targets. By default, BackupChain deletes the oldest backup file **after** a backup cycle completes successfully. This is to ensure there is always at least one good backup to restore from. In certain circumstances you may want to delete the oldest backup before placing the newest backup, for example when backup storage space is very limited and you have another backup on different media. However note that using this option could possibly result in having no backup to restore from in case the backup is stopped or fails.

### Backing up Several Disks Simultaneously

Use the “Add Disk” button to add additional “Backup / Conversion” steps as needed. Whenever you have a server with multiple hard drives where one service is accessing more than one, you may have to back up all disks simultaneously. For example, SQL Server may use be using the system disk as well as disk #2 to store the bulk of its database records. In that case you would select disk #0 (assuming that’s the system disk), then click ‘add disk’ and in the new section, select “disk #2” as the source.

When you back up several disks simultaneously, the backup is consistent in time and the resulting virtual disk backup files are consistent to each other as the backup was taken at the same point in time for all disks.

## Virtual Disk Conversion

A unique feature in BackupChain is its ability to convert virtual machines live from one format to another without interrupting or otherwise affecting the original VM.

For example you could convert Hyper-V VMs to VMDKs and power them up using VMware Workstation in case of a disaster. Alternatively you could convert VMs live in order to migrate them from one platform to another, such as from VMware Workstation to Hyper-V.

Similar to the instructions of the preceding section, create a new task of “V2V” type. The example below converts a Hyper-V VHD to a VMDK to be used in VMware Workstation:

I want to convert physical and virtual machines / disks...

☐ P2V

(Physical disk to virtual disk conversion)

☐ V2P

(Virtual disk to physical disk conversion)

☒ V2V

(Virtual disk format conversion)

Then in the next screen we select the source VHD and the target VMDK file we want:

bc Create a New Backup Task Wizard -- BackupChain

Select Backup Type Help Disk Imaging Finished

Below select the source disk and target disk. If you want to back up several disks simultaneously, click "Add Disk" to add additional backup steps.  
For P2V, V2P, and V2V conversions, simply select the source disk type and target disk type to set up the kind of conversion you need.

Disk Step #1 [Hide Settings](#)

Disk Selection Options

Backup Type  
Selected Backup Type: Image Format Conversion: Convert virtual disk image to another format (V2V)

Source Disk Image File  
Original file: d:\virtual\Ubuntu Server.vhd Browse  
Supported virtual disk formats: VHDX, VHD, VDI, and VMDK. ☒ Perform Live VM Conversion

Target Disk Image File  
Target File: z:\Converted VMs\Ubuntu.vmdk Browse

Virtual Disk Format  
☐ VHD (<= 2TB) ☐ VHDX (<= 64TB) ☒ VMDK (<= 2TB) ☐ VDI (<= 2TB)

Virtual Disk Type  
☒ Same as Original ☐ Pre-allocated, Fixed Size ☐ Pre-allocated, Sparse ☐ Dynamically Expanding

☒ Apply universal boot settings

Add Disk Help Refresh  
Go Back Next Step

Note the option “Perform Live VM Conversion” has to be checked if you want to back up or convert this VM **while it’s running**. In the case of Hyper-V, this conversion will be made application consistent and you will notice in the Hyper-V Manager the VM switching to a live backup state (no interruptions will occur unless Hyper-V pulls the VM into a Saved State at its own discretion. Contact our tech support for details).

The file Z:\Converted VMs\Ubuntu.vmdk will be produced from the Hyper-V VM while the VM is running. The VMDK can be directly attached to a new VMware Workstation or ESX VM and booted in most cases. An intermediary step may be necessary for some VMs, see sections below. The intermediate step can be included in the screen above by selecting ‘apply universal boot settings’, which alters the VM’s boot settings to be more compatible with VMware in this case.

### *Automatic cleanup*

If your target disk above is a virtual disk and you intend to run this backup repeatedly, BackupChain offers an automatic cleanup mechanism. See page 38 for details.

### *Image to Disk: Copy virtual disk image to physical disk*

Instead of copying a VHD to another virtual disk you can also copy the virtual disk contents to a physical disk. This way you can convert the VM to boot as a physical machine. Note that some modifications may be necessary on some systems.

The screen below shows how to configure a physical disk target. Select 'Image to Disk' as the backup type, then the virtual disk source file, and finally the physical target disk.

**Note that the target disk will be deleted when the backup task is run.**

**Create a New Backup Task Wizard -- BackupChain**

Select Backup Type   Help   Disk Imaging   Finished

Below select the source disk and target disk. If you want to back up several disks simultaneously, click "Add Disk" to add additional backup steps.  
For P2V, V2P, and V2V conversions, simply select the source disk type and target disk type to set up the kind of conversion you need.

**Disk Step #1** [Hide Settings](#)

**Disk Selection** Options

**Backup Type**

Selected Backup Type: Image to Disk: Copy virtual disk image to physical disk (V2P) ▼

**Source Disk Image File**

Original file: d:\virtual\Ubuntu Server.vhd Browse

Supported virtual disk formats: VHDX, VHD, VDI, and VMDK. ☒ Perform Live VM Conversion

**Physical Target Disk**

Selected Target Physical Disk:

Disk #0: 3.64 TB (X:\), GPT, Model: TOSHIBA MG03ACA400 ATA Device, Serial: 4 14K276FF Select

Please check this setting carefully--this is the disk that will be deleted!

☐ Apply universal boot settings

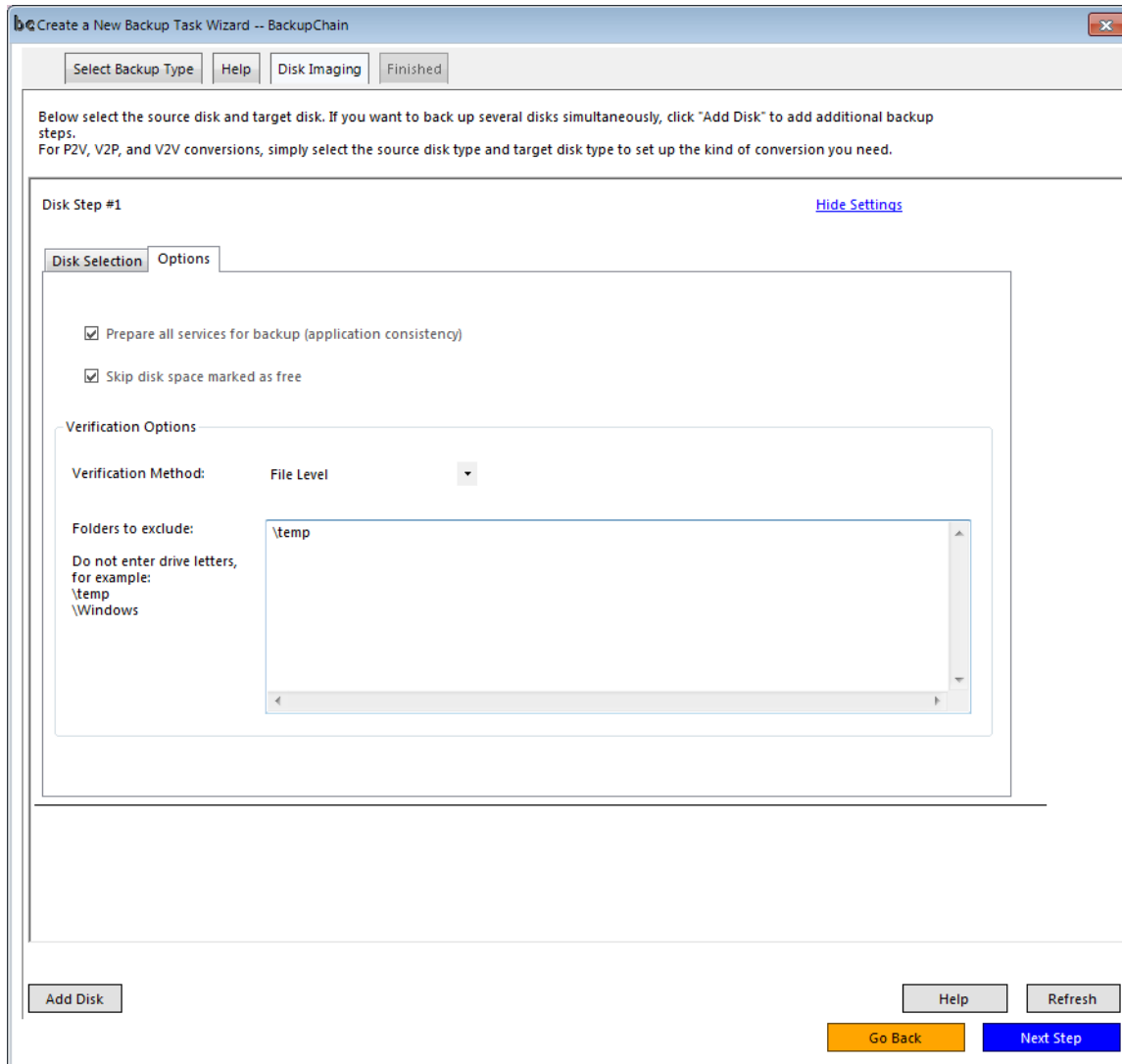
Add Disk Help Refresh

Go Back Next Step

**Note:** Make sure your boot settings are configured to force booting from the “correct” disk. Once you have several bootable disks in the server, the BIOS might use the “wrong” one next time you boot.

## Disk Backup Verification

All disk backup processes (P2P, P2V, V2P, V2V) can be verified on either block or file level or both as shown below:



The option shown above “Prepare all services for backup (application consistency)” causes BackupChain to send a signal to all VSS aware services to prepare for backup. Use this option if the server runs a VSS aware service, such as SQL Server, modern versions of Oracle, Microsoft Exchange Server, etc.

The option “skip disk space marked as free” allows BackupChain to skip disk storage blocks if they are explicitly marked by the file system as free, such as free space on the volume “C:”.

Verification can exclude certain paths. Enter each path in a separate line and do not enter drive letters. The above example excludes the path “\temp” from verification. Since verification prolongs the time needed to complete a backup, it makes sense to reduce the verification volume when possible. The above example excludes the \temp folder as it holds uncritical files that do not have to be verified.

## Creating a New Task

This section outlines file backup tasks. Disk backup tasks are discussed in the previous section.

When you first start BackupChain it automatically opens the following screen which assists you in creating your first backup task:

**Create a New Backup Task Wizard -- BackupChain**

Select Backup Type | Help | Select Folders | Default Settings | Options | Target | Finished

**Welcome to BackupChain's Backup Task Wizard!**

This wizard guides you through the main functions of BackupChain and assists you in setting up a backup task. Backup tasks store all your settings for future use. Tasks may be scheduled or may be run manually whenever you need to run a backup. Once saved, you may fine-tune your backup task later in the Main Screen, where all features of BackupChain are available.

Create Task on Server: backupchain-PC

Enter a Task Name: File Server Backup

Please select the purpose of this backup task:

**I want to back up documents and file server data...**

☒ **File-Level Backup**  
(File Server and Version Backup.  
Use for file server data, documents, etc.  
Files are placed individually in backup folder.  
Do not use for VMs)

**I want to back up virtual machines...**

☐ **Hyper-V Backup (Server)** ☐ **Hyper-V Backup (Client)** ☐ **VMware Backup** ☐ **VirtualBox Backup**  
(Automatic or Granular Backup) (File-based, recommended only for Windows 8-10 + Pro Edition) (VMware Workstation, Player, VMware Server backup)

**I want to back up the Windows boot disk or sector-level backup...**

☐ **Disk to Image Backup (Sector-Level)** ☐ **Disk Cloning (Sector-Level)** ☐ **Restore Disk Image Backup (Sector-Level)**  
(Sector-based backup of a physical disk into a disk image file. This is usually only done to back up operating system disks) (Sector-based copy of a physical disk to another physical disk. This can be used for Windows operating system boot disks as well as data disks) (Restore a disk image file to a physical disk)

**I want to convert physical and virtual machines / disks...**

☐ **P2V** ☐ **V2P** ☐ **V2V**  
(Physical disk to virtual disk conversion) (Virtual disk to physical disk conversion) (Virtual disk format conversion)

**Other backup task types:**

☐ **SQL Server Backup** ☐ **Universal Backup**  
(Backup SQL Server and MSDE Databases) (Backup all VSS aware services. Use only if no other backup type suits)

Go Back Next Step

Name the backup task at the top and describe it in a meaningful way, which can be useful if you plan to run several backup tasks.

It is important to select the correct type of backup at the beginning to match your needs. If no other type matches your needs, please select “Universal Backup”. Documents and file server data should be backed up using the “File-Level Backup” type selected in the above example.

File-Level Backup should be used if you don't want to back up databases, virtual machines, or other VSS aware applications.

Use Hyper-V Backup (Server) only to back up Hyper-V VMs or for Hyper-V Granular Backup using the Server Editions or Platinum Edition. You can use this type of backup also on Windows 10 with the Server Edition of BackupChain.

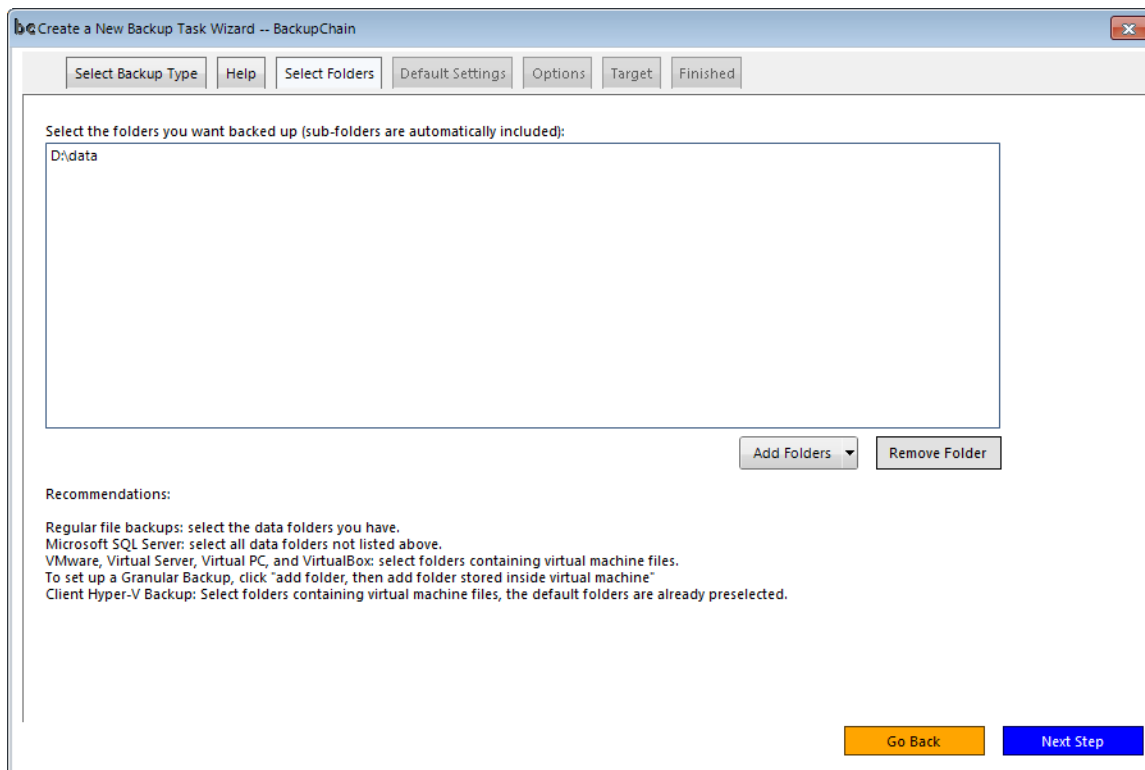
Use Hyper-V Backup (Client) on Windows 8 or Windows 10 with Hyper-V installed, with the Professional Edition of BackupChain. This type of backup uses the file-based Hyper-V backup method discussed in later sections of the user guide. Advanced users can use this option also on Windows Servers with the Server Editions of BackupChain for very specific scenarios only.

Use the SQL Server Backup type only when backing up Microsoft SQL Server and regular data files.

If you have a server with several virtual machines and databases, unless they depend on one another, it makes sense to back them up individually. Backing up many services simultaneously increases the load on the machine and may severely impact system performance. VM backups are discussed in detail in the tutorial section of this manual.

## Selecting folders

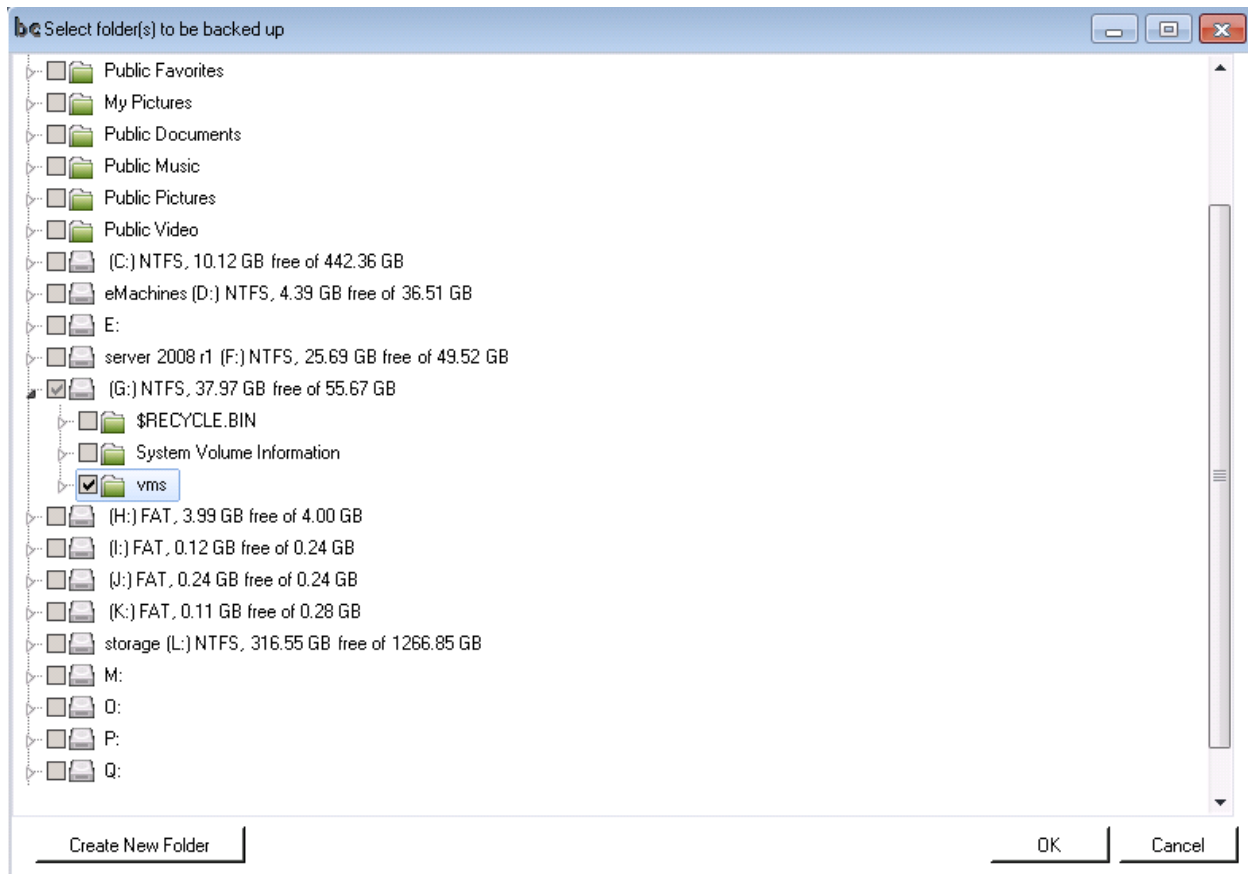
After clicking Next, you may select folders for backup in the following screen:



Note that when you select a folder to be backed up, subfolders are automatically backed up as well. You may leave this screen empty and select folders and files later on. If you don't need the folders automatically listed, you can remove them.

## Backing up Local Folders

Click Add Folders and select Add Local Folder, which opens the folder selection screen:



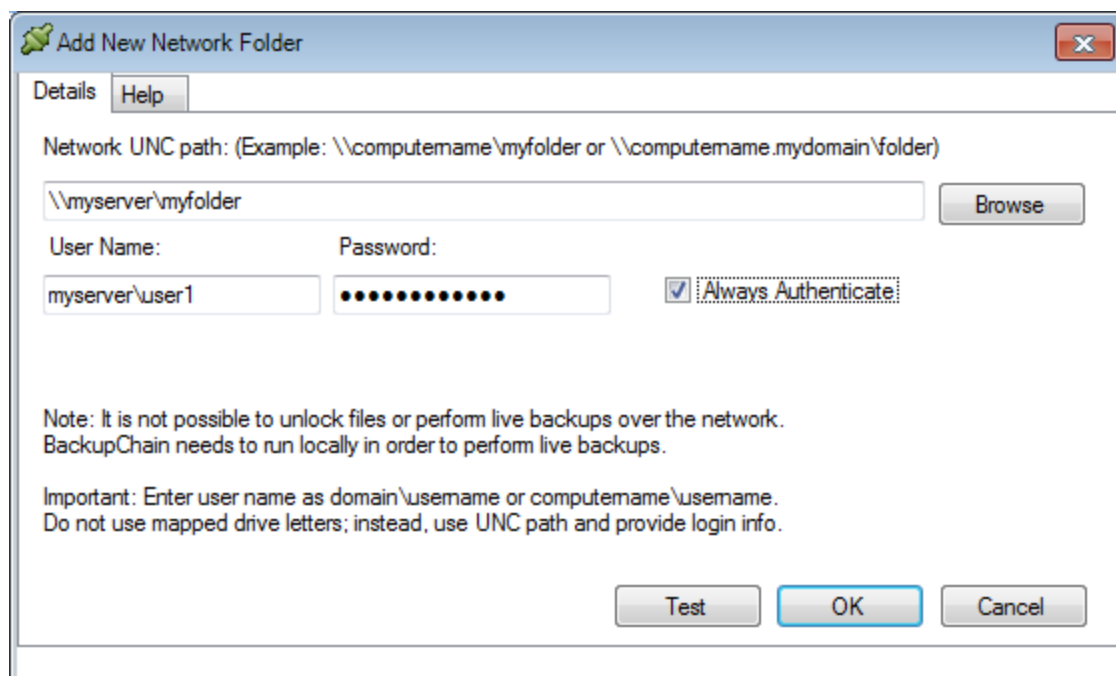
You may select one or more folders and create new folders as needed.

## Backing up a Network Folder

Backing up **from** a network folder is called a 'pull strategy'. Here files are "pulled" from the other computer.

**Note:** Files in use (opened exclusively) **cannot be backed** up using this method. You need to run BackupChain on that machine locally in order to unlock files. Examples of files in use: Hyper-V or other virtual machines, databases, Microsoft Outlook files, and Microsoft Exchange.

The example below shows the screen that appears after clicking Add Folder -> "Add Network Folder". In our example we connect to another computer in a workgroup (not a domain):



**Add New Network Folder**

Details Help

Network UNC path: (Example: \\computename\\myfolder or \\computename.mydomain\\folder)

\\myserver\\myfolder Browse

User Name: Password:

myserver\\user1 ..... ☒ Always Authenticate

Note: It is not possible to unlock files or perform live backups over the network. BackupChain needs to run locally in order to perform live backups.

Important: Enter user name as domain\\username or computename\\username. Do not use mapped drive letters; instead, use UNC path and provide login info.

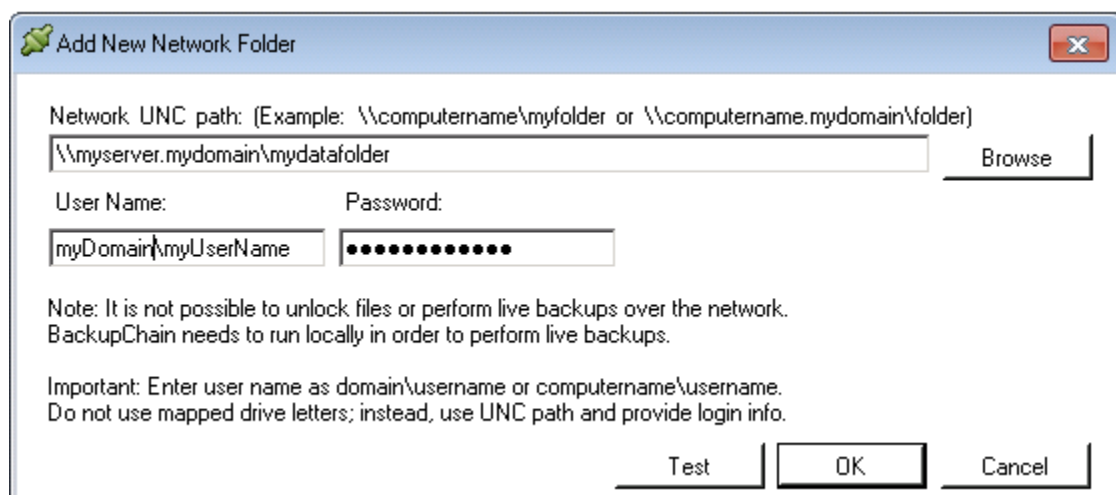
Test OK Cancel

The previous chapter elaborates on network connections in more detail. Please refer to the previous section for more information on how to connect to network shares.

The feature “Always Authenticate” allows BackupChain to skip authentication if it isn’t necessary. This may also help prevent re-authentication attempts leading to connection errors.

**Note:** Mapped drives cannot be used. Instead you will need to enter UNC paths with credential information. See previous chapter for more information.

The following example demonstrates how to connect in domain environments when the target server is member of a domain:



**Add New Network Folder**

Network UNC path: (Example: \\computename\\myfolder or \\computename.mydomain\\folder)

\\myserver.mydomain\\mydatafolder Browse

User Name: Password:

myDomain\\myUserName .....

Note: It is not possible to unlock files or perform live backups over the network. BackupChain needs to run locally in order to perform live backups.

Important: Enter user name as domain\\username or computename\\username. Do not use mapped drive letters; instead, use UNC path and provide login info.

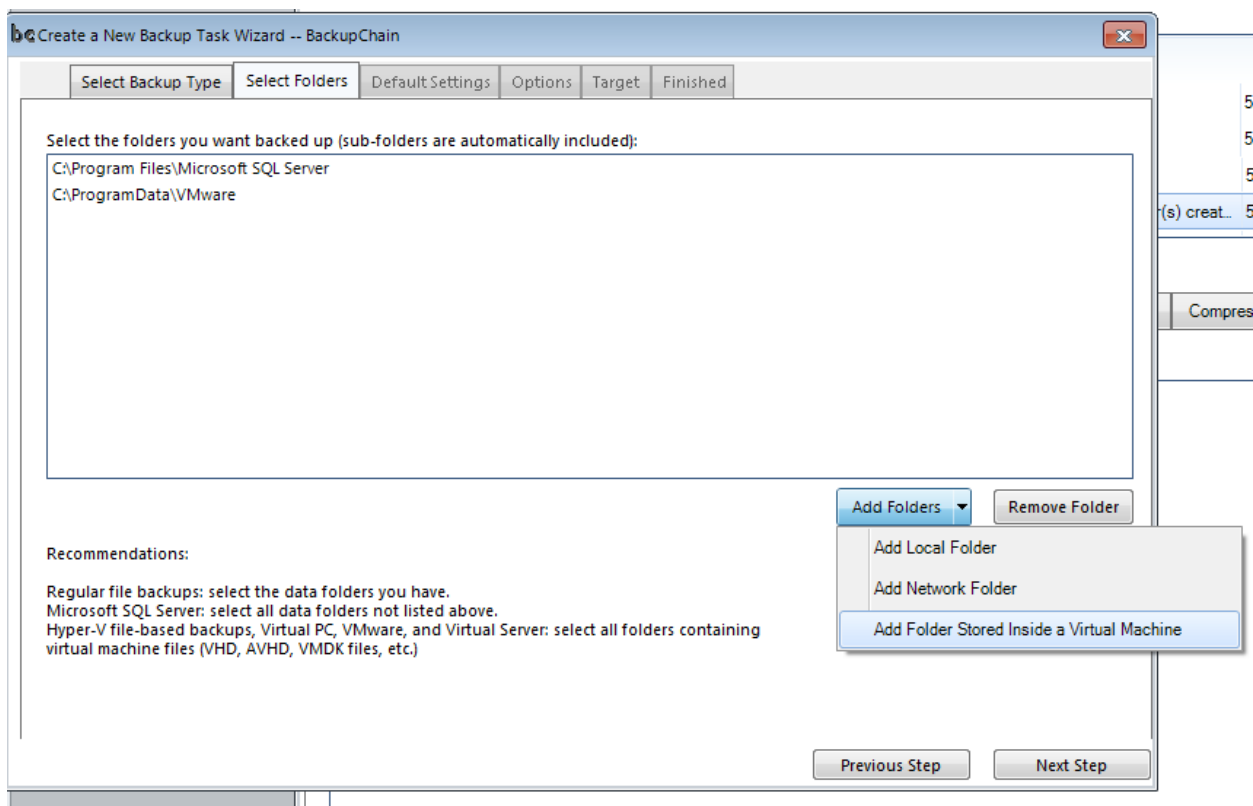
Test OK Cancel

## Backing Up Folders Stored Inside a Virtual Machine (Granular Backup)

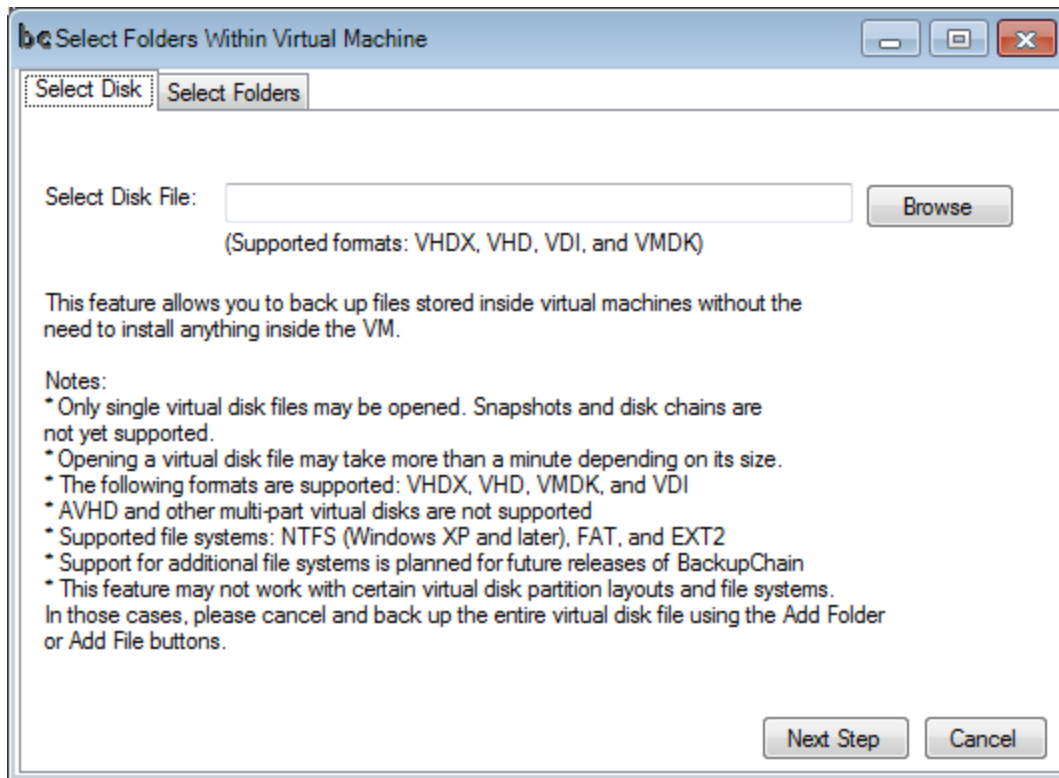
**BackupChain Server Enterprise Edition** and the Platinum Edition include Granular Backup. It allows users to back up files and folders that are stored inside a virtual disk of a virtual machine, such as a VHD, VHDX, VMDK, or VDI. Note that limitations apply as shown on BackupChain's user interface.

*This feature is available only in Server Enterprise and Platinum Editions.*

To back up folders inside a virtual machine, select Add Folders and then "Add Folder Store inside a Virtual Machine":

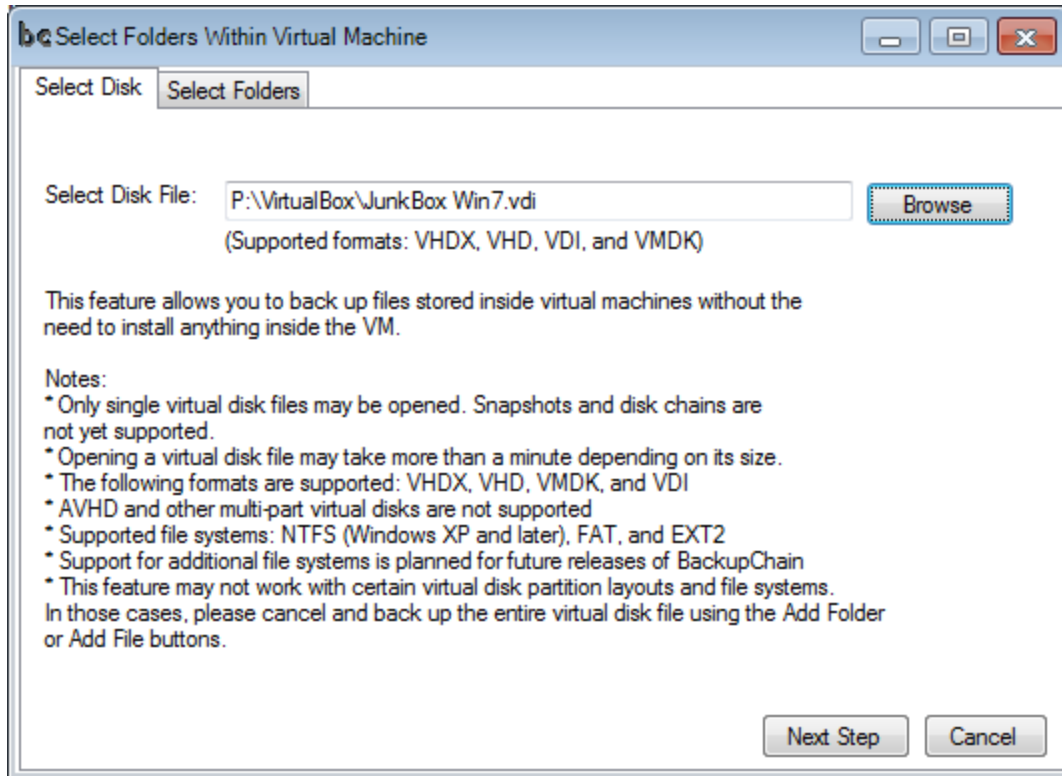


Now a new screen opens: "Select Folders Within Virtual Machine" as shown below:



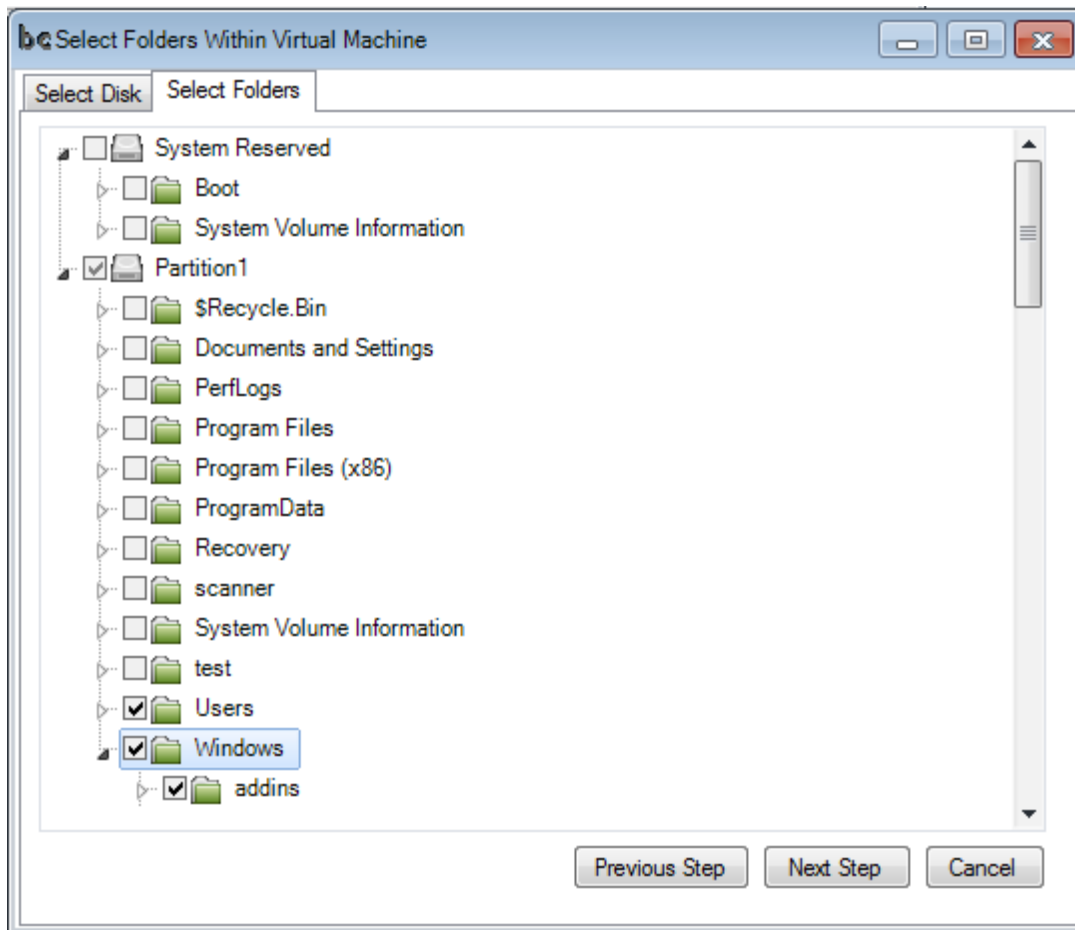
Note that not all types of file systems are supported. The Granular Backup feature does not yet support snapshots or multi-file virtual disks. Virtual disk files have to be single files. Hyper-V (AVHD or AVHDX files) or VMware snapshots are not supported.

Proceed and select a virtual disk file. In our example we open a VirtualBox VDI file; however, you could also open Hyper-V (VHD / VHDX), Virtual PC, Virtual Server, and VMware VMDK files:

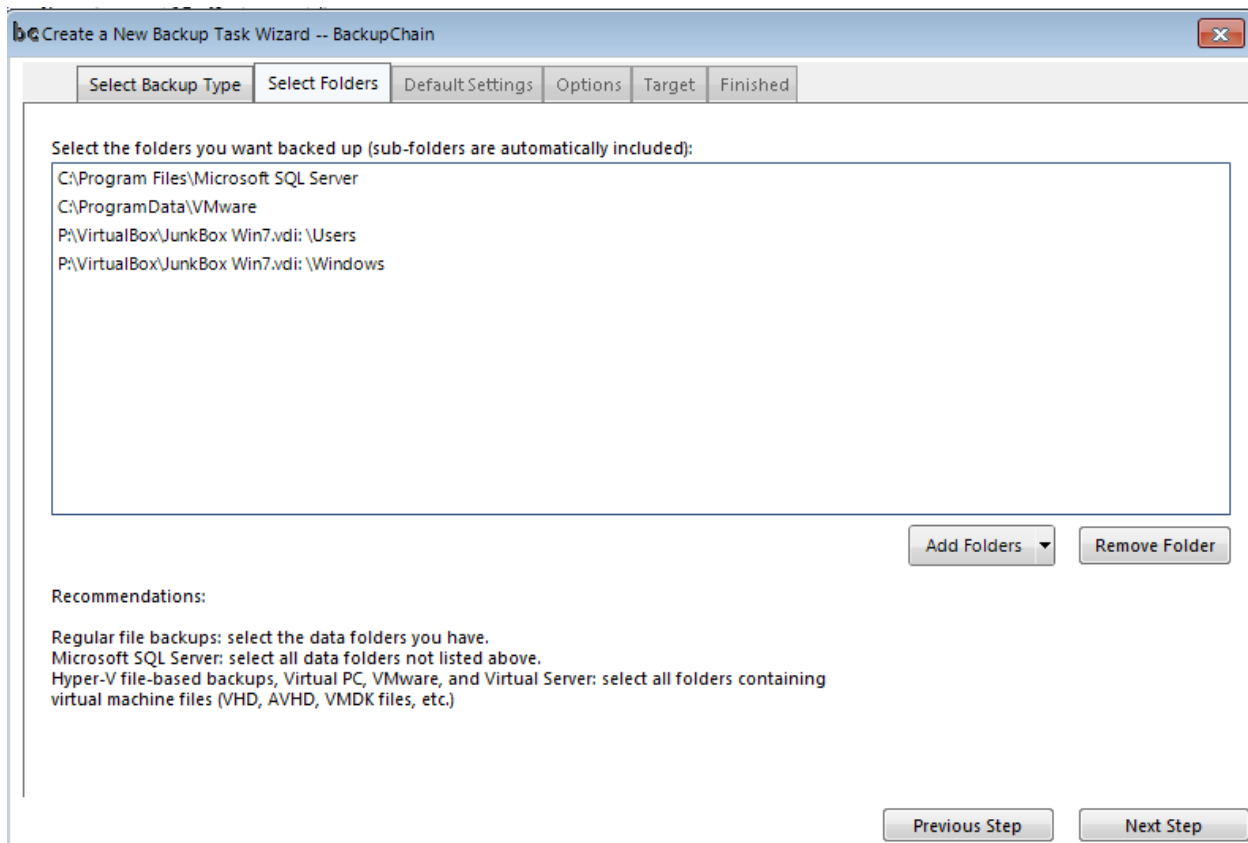


Click “Next Step” to open the virtual machine. It is not necessary to stop or pause the virtual machine to make a folder selection. **The virtual machine will not be affected or interrupted.**

In our example we select the folders Users and Windows from the virtual machine's major partition:



The folders are now select and we may move on to the next step:



## Backup Defaults

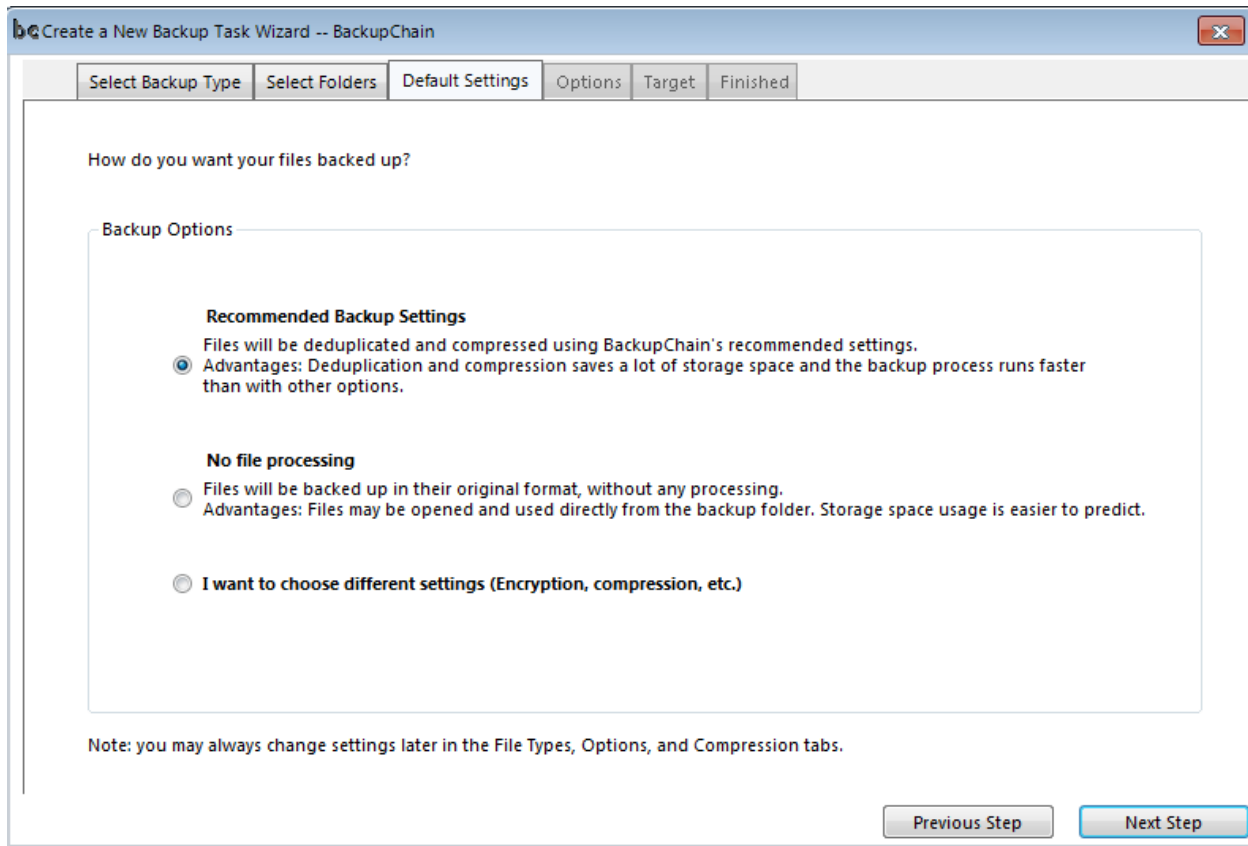
The next step in the Backup Wizard shows a selection of “Default Settings” that impact how the backup is to be taken. You are shown three different options:

- Recommended Settings
- No File Processing
- I want to choose different settings

### Recommended Settings

“Recommended Settings” is the option that suits most users and it preconfigures the task with fastest compression, deduplication, and regular version retention of 10 backups per file. This means that for each file up to ten backups will be held in the backup target. Thereafter, BackupChain deletes the oldest backup copy of a file to make room for the next one.

Note that no matter what backup default options you choose, you may always amend your settings later using BackupChain's Main Screen.



The advantage of using compression and deduplication is that backups finish faster and use less space. A disadvantage of compression in general is that it is difficult or impossible to predict actual runtime and storage space needed. If your environment requires exact timing and storage usage you need to use the next option: No File Processing.

### *No File Processing*

No File Processing means that BackupChain will not compress, encrypt, or deduplicate any files. BackupChain will be configured to make a backup copy of each file; however, file versioning will nevertheless be available. BackupChain keeps up to ten backup copies of each file (default setting, can be changed) and thereafter deletes the oldest file version to make room for the newest backup. This process is done at the file level; each file is processed separately.

## Custom Backup Settings

If you select “I want to choose different settings” the following screen is shown:

The screenshot shows the 'Options' tab of the 'Create a New Backup Task Wizard -- BackupChain' window. The window has a title bar with a close button. Below the title bar is a tabbed interface with tabs: 'Select Backup Type', 'Help', 'Select Folders', 'Default Settings', 'Options' (selected), 'Target', and 'Finished'. The main content area contains the following settings:

- A message: "Please choose among the following options. These are minimum settings to get you started. More advanced settings can be specified later if necessary."
- A checkbox labeled "Permit deduplication in task" which is checked. Below it is a "Deduplication" section with two radio buttons: "On" (selected) and "Off".
- A "Compression Settings" section with four radio buttons: "No Compression (Usually slower)", "Fastest Compression" (selected), "Standard Compression", and "High Compression (Slower)".
- A "Resource Usage" section with three radio buttons: "Maximum Speed (Uses more resources and RAM)", "Minimal System Impact (Slower)" (selected), and "Reduce Hard Drive Stress (Slowest)".
- A dropdown menu labeled "Keep this many versions of each file in the backup store:" with the value "10" selected. To its right is a text box explaining: "These are Automatic Cleanup / File Version Backup Limits. Enter a number or ALL to keep all file changes. A setting of 10 will keep the last 10 versions of each file. A new file version is only created when a file change occurs."
- A checkbox labeled "Encrypt files with military strength encryption (AES 256, HIPAA compliant)" which is unchecked. Below it are two input fields: "Password:" and "Confirm password:".

At the bottom right of the window are two buttons: "Go Back" (orange) and "Next Step" (blue).

Compression may be switched off, set to fastest, standard, or high level. Disabling compression is useful if you know beforehand that the data is not compressible. Music, video, media, and previously encrypted files are examples for files that do not compress well. To save time you may want to switch off compression completely as it does not add any benefit in the case of encrypted or media files.

Regular files generally compress well and take up less space in the backup store; hence, backups run faster because less information needs to be written or transmitted. The high compression setting, on the other hand, leads to longer backup times because the CPU will take more time trying to compress the data to a smaller size.

The switch “Deduplication” controls the use of deduplication on your files. Deduplication is compression based on a previous backup of a file. The contents of a file are compared to its last backup and only the difference (the delta) is backed up. This process saves storage space and backup time, especially when dealing with large files, such as databases and virtual machines.

The “Resource Usage” setting controls BackupChain’s background process priority. Maximum Speed lets backups run with normal priority and without CPU limitations. Note that BackupChain’s Main Screen (Speed tab) offers many more settings to fine tune the speed of each backup task.

“Minimal System Impact” reduces the process priority to minimal and limits the process to just one CPU core for the backup. This is useful when you want to limit the impact of the backup process on your server.

The setting “Reduce Hard Drive Stress” limits the backup process even more and applies a 10MB/sec read and write speed limitation.

The setting “Automatic Cleanup” is preset to 10 and controls how many copies you wish to keep in the backup store. Entering ALL will keep every single file change forever, while entering “1” will keep only one backup copy of each file. Every time a file is changed and subsequently backed up, a new file version is created in the backup store. This allows you to restore older file versions but uses more space in the backup store. If you are backing up large files that change often you may need to reduce this setting or you can utilize BackupChain’s deduplication feature.

Note that you may fine tune the “Min. Number of File Versions” setting on a per-file-type basis in BackupChain’s Main Screen, along with several other data retention features.

Finally, you may want to encrypt your files using AES256, which is today’s military-strength encryption standard. If you lose your password, however, you will not be able to restore any of your files. If you plan to change your password regularly, it’s recommended to change backup folders when you change passwords since encryption passwords would otherwise vary within the same folder and lead to restore problems.

Note that all of the above settings may be fine-tuned later if necessary in the Main Screen of BackupChain.

## Selecting a Backup Target

Proceed to the next screen and configure your backup target:

Create a New Backup Task Wizard -- BackupChain

Select Backup Type | Select Folders | Default Settings | Options | **Target** | Finished

Target Folder Settings: Where do you want to store your data?

☒ Local folder    
 Use this option to send your files to a local hard drive, external USB/Firewire drive, flash drive, etc.

☐ Network UNC folder    
 Use this option to send your files to a network drive on your LAN or VPN. Example: \\myserver\myfolder

☐ FTP site    
 Use this option to transmit files via FTP to a remote server. Example: ftp://ftp.myserver.com

Note: Every task should have its own separate backup folder.

Use the above screen to send your backups to either a local drive, network share, or FTP/FTPS site.

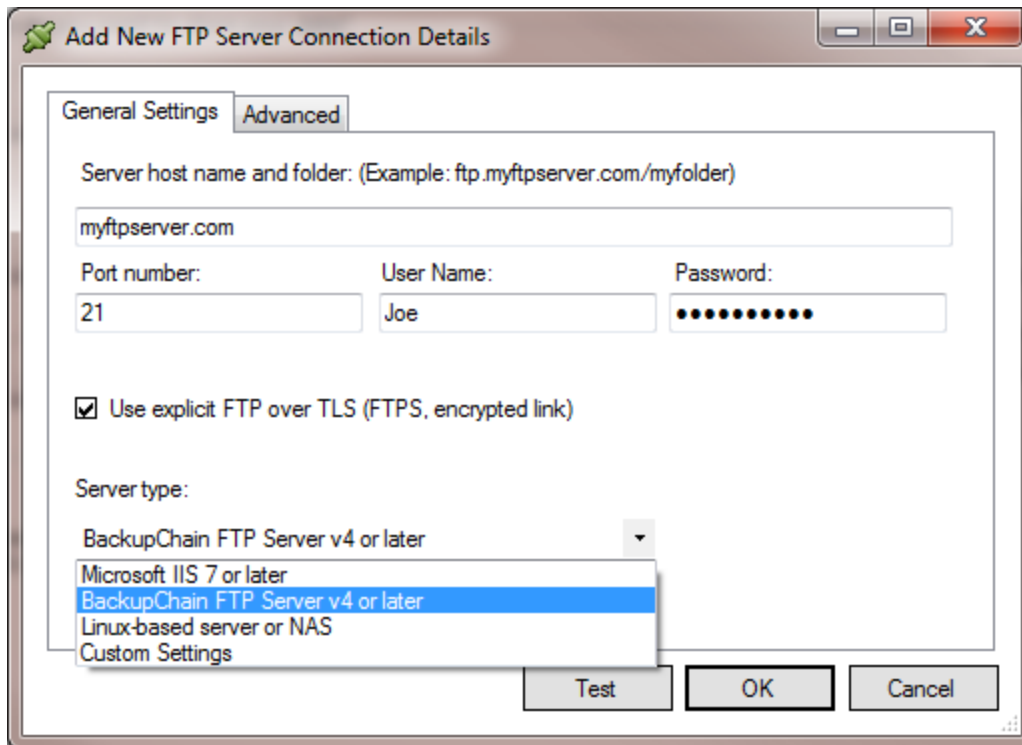
Local folders may be external drives (USB 1/2/3, FireWire, eSATA, etc.) or local hard drives.

Network folders are shared folders on a LAN or VPN, see previous chapter for details.

FTP Site allows you to specify an FTP server as a target, which may be a BackupChain FTP Server or a standard FTP server on the Internet. FTPS is also supported.

### Specifying an FTP Backup Target

In this example we want our backup to be sent to an FTP server:



Enter the server's name or IP address, port number, user name, and password and run a quick test to check your settings.

Some servers (especially some Linux-based variants) that are not following the full FTP standard do not support the SIZE command or Passive Mode and some have other limitations as well. In those cases you may want to switch the server type to "Linux-based server" and see if this resolves the connection problems.

In case of a connection failure an error will be displayed with more information. To investigate the cause of the problem you may also want to check your outbound firewall restrictions and all the settings above. Also you may want to look at the *FTP server logs* in case of a connection error.

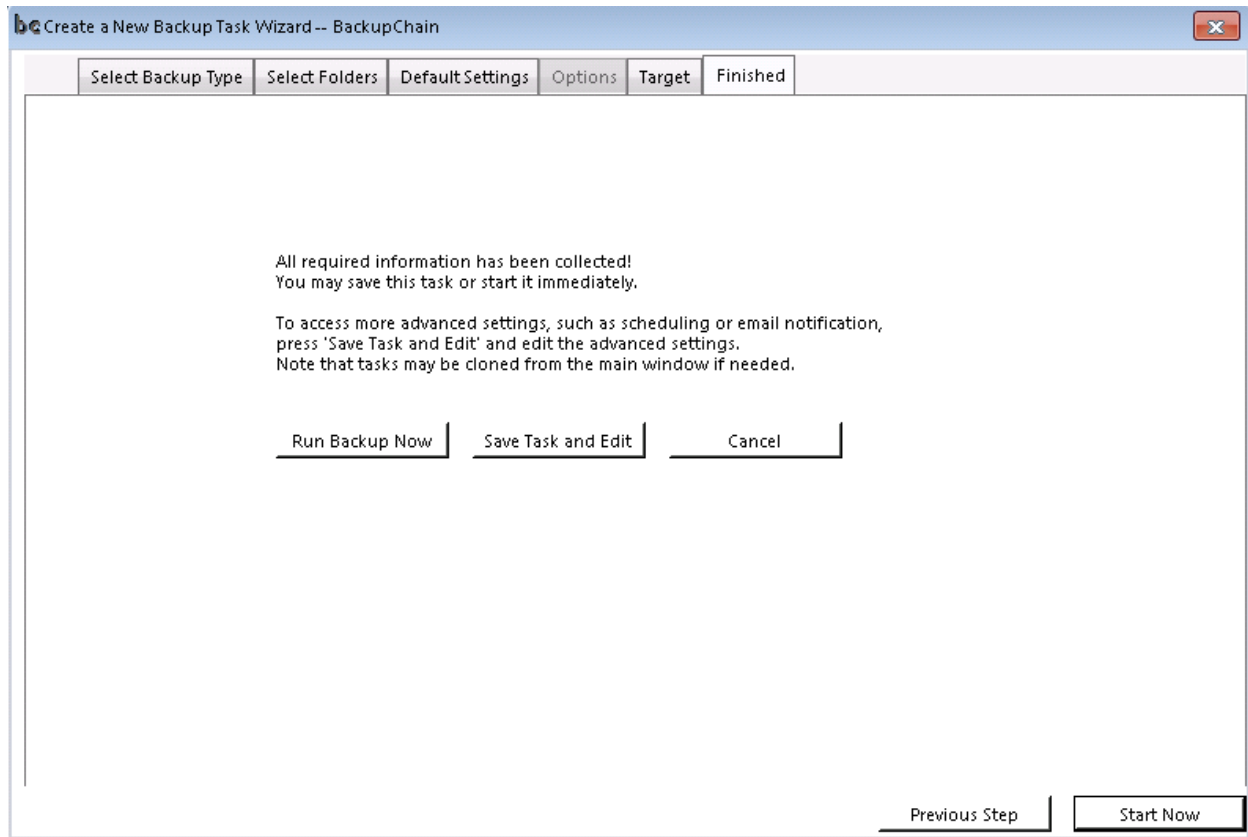
"Use explicit FTP over TLS" is secure FTP. The initial handshake is done clear text but then the connection is explicitly turned into a secure, encrypted link before user name and password travel over the wire. Data is also encrypted.

Please do not change the server type once you have run a successful backup, as it changes internal structures in the backup folder. If you must change the setting, you should also wipe the target folder or start a new target folder.

The folder entered in the address must already exist; it will not be created by BackupChain if it doesn't.

## Running your Backup

After specifying your target, you may want to start the task immediately or save it to run it later:



## Where Do I Set Up a Schedule?

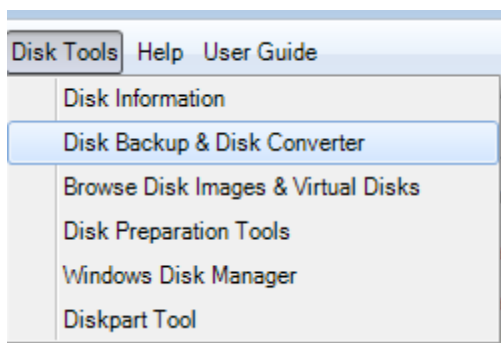
Backup task schedules may be entered in the main screen's Schedule tab. You can schedule several jobs using separate schedules and backups may overlap; however, overlapping schedules should be avoided because they put a high load on your computer.

## Disk Backup and Disk Converter

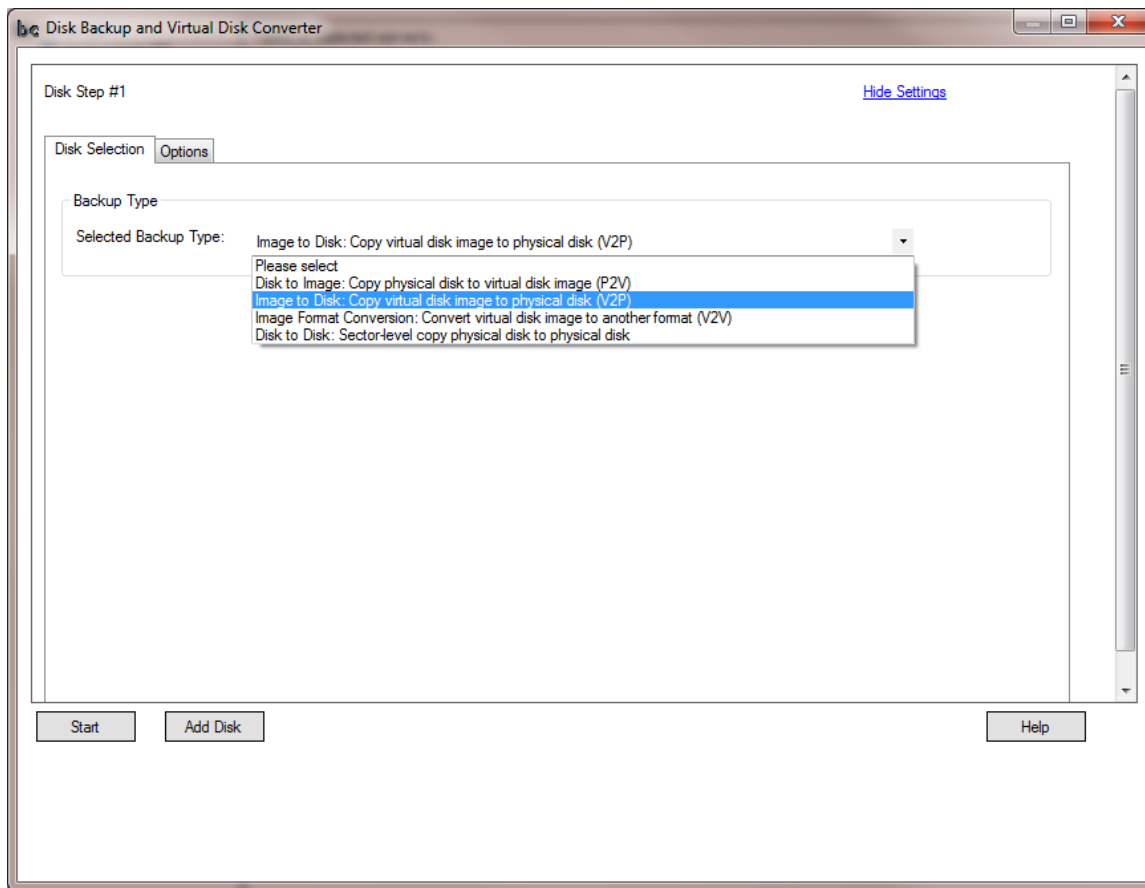
If you want to copy disks, convert VMs from one format to another, or take a backup of a physical disk, you can use the “Disk Backup & Disk Converter” tool.

The “Disk Backup & Disk Converter” tool offers the exact same functions as discussed in the previous chapter (Disk Backup Tasks) but it’s a once-off operation and the settings won’t be saved. Unlike creating a task that is meant to be repeated at some point, either manually or via the task scheduler, the “Disk Backup & Disk Converter” tool offers disk backup functionality for manual, once-off operations.

Select Disk Tools->Disk Backup & Disk Converter from the BackupChain Monitor main menu:



A new screen will open with essentially the same layout as when you create a new disk backup task via the “New Task Wizard”:



You can also add additional disks to the operation via the “Add Disk” button, for example, when you need to back up two drives at the same time due to applications that use multiple drives for data storage simultaneously. When you add more disks, some settings will be copied over for your convenience.

See page 29 for in-depth details of each function provided in this tool.

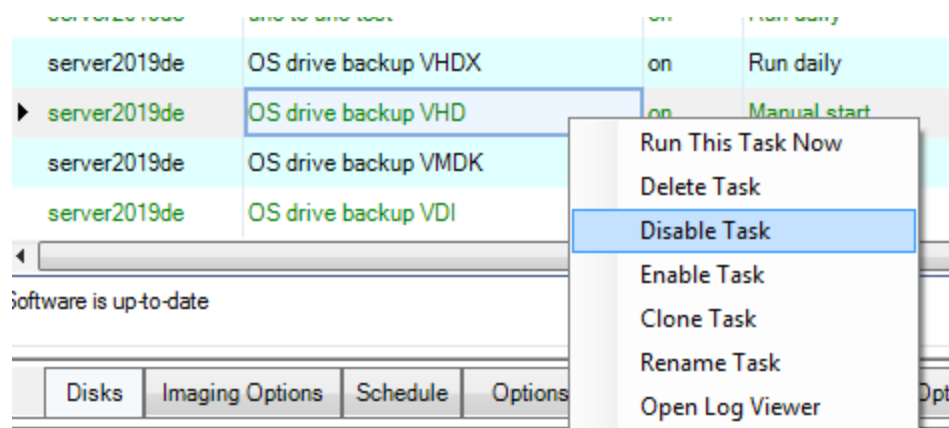


Server Enterprise edition, you can remotely control other instances of BackupChain (all editions except the Server Edition), and the servers can be added to the server tree on the left. By clicking the “Server List” node at the top of the tree, BackupChain will show all tasks of all servers simultaneously so you can have an overview of all connected servers.

It is recommended to use the Save button to save your settings.

## Context Menu

By right-clicking on a task you can open a menu of shortcuts:



Note that if you click ‘disable task’ it will ask you to confirm whether you want to stop the task, if it is currently running.

## Open Log Viewer

The Open Log Viewer option opens a new window for the task’s log, so you can inspect several logs simultaneously.

## Deleting Tasks

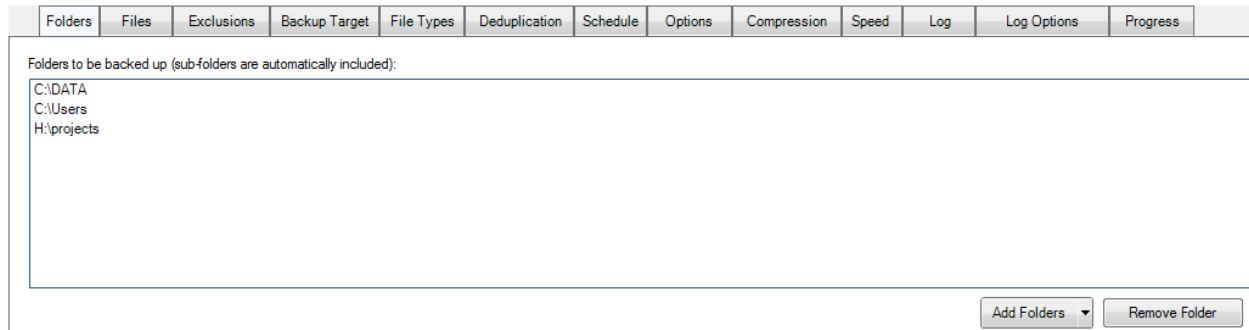
You can delete tasks from the context menu by right-clicking on the task’s line in the Backup Task List.

### *Cloning Tasks*

A useful productivity tool is the clone function: right-click on the task's line in the Backup Task List and select Clone. This will copy all task settings into a new task.

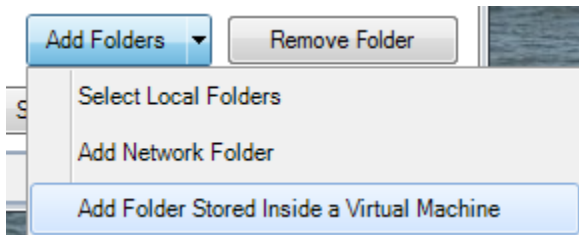
## Selecting Folders

Use the Folders tab to select the folders you want to back up:



Note that subfolders are always included during backup automatically. If you do not want to include all the content below a folder, you can either include subfolders instead, or use the Exclusions Tab to select individual files or subfolders to omit.

When you click Add Folders, a sub-menu opens:

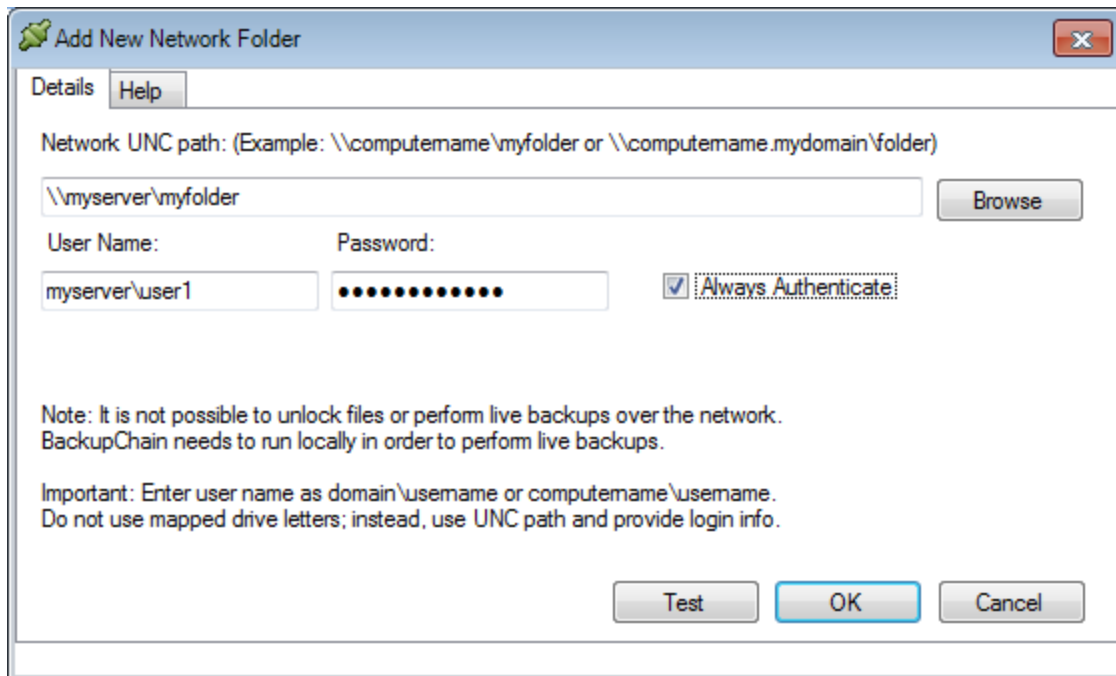


### Select Local Folders to Be Backed Up

Click on “Add Folders” and then “Select Local Folders” to back up specific **local** folders on your machine. Subfolders are scanned automatically during backup. **Note:** Mapped drives cannot be added, use the “Add Folders” -> “Add Network Folder” option instead.

### Select Network Folders to Be Backed Up

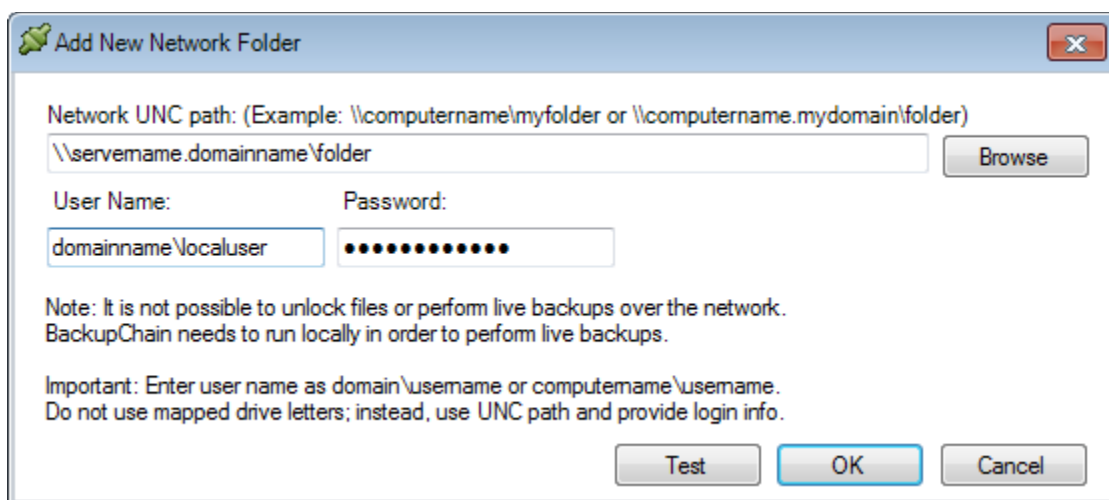
Click on “Add Folders” -> “Add Network Folder” to open the following screen:



The example above shows a connection to a workgroup computer. Note that it is recommended to prefix the user name with the computer's name to avoid ambiguities.

The "Always Authenticate" option will permit BackupChain to skip network authentication if possible. This may prevent re-authentication issues that could lead to errors and is also faster if a connection has previously been established.

Use the following example as a guide when connecting to domain controlled servers:



You can use the Browse button after entering network path, user name and password. User name and password are optional in case the target path is allowed to everyone.

Note that the service “BackupChain Service” is a background service (listed in Service Manager of Microsoft Windows) and the test button and backups run using that service. By default the service is running as LocalSystem user. You may need to change the Log On settings of BackupChain Service to run it as a local/domain administrator instead in case you encounter connection or authentication problems.

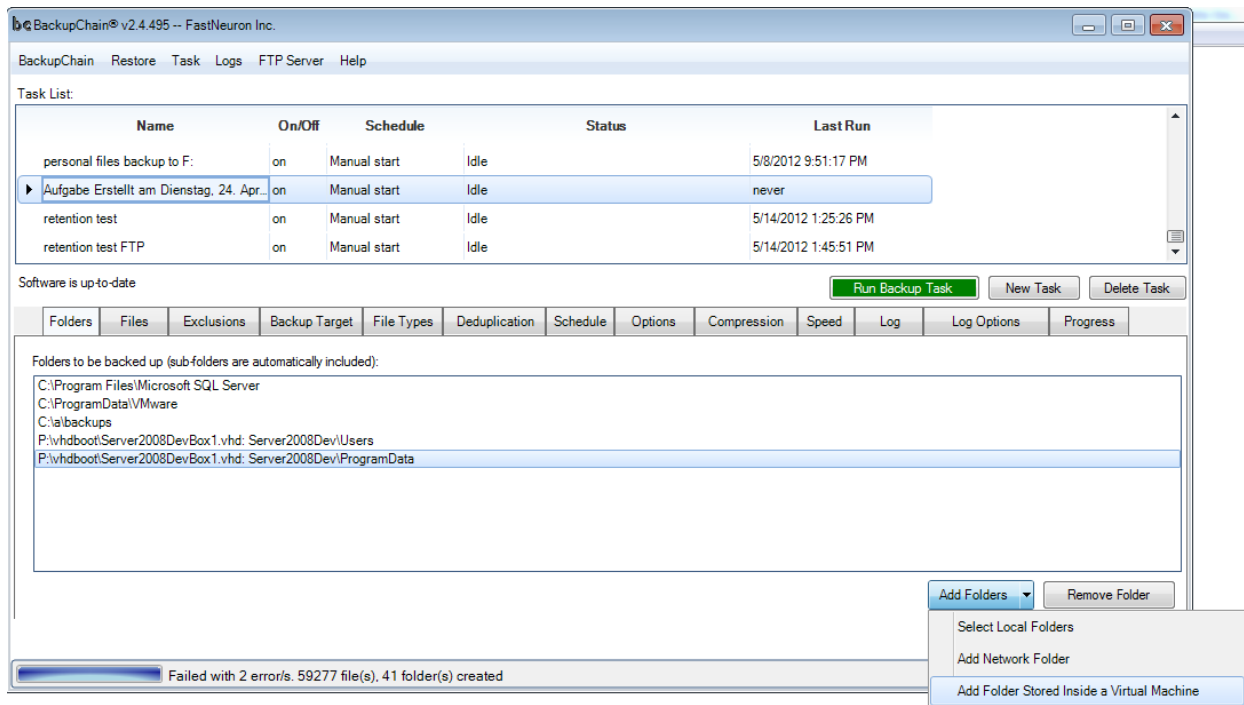
However most of the connection problems have to do with Windows not knowing how to authenticate a user. Use the “always authenticate” option and prefix the user name with the domain name (mydomain\joe) or in a workgroup setting the name of the server where the user was created (filesrv1\joe). Note you can also use the IP in the user name: 10.0.0.2\joe (no backslashes at the beginning as this is a user name, not a UNC path)

### Select Folders Stored Inside a Virtual Machine or Virtual Disk (Granular Backup) to Be Backed Up

A great feature in *BackupChain Server Enterprise Edition* is Granular Backup which is just as useful as Granular Restore but operating at the backup level rather than the restore process. Granular Backup allows you to take **live backups of folders stored inside a virtual machine, without backing up the entire virtual machine and without interfering with the virtual machine processes.**

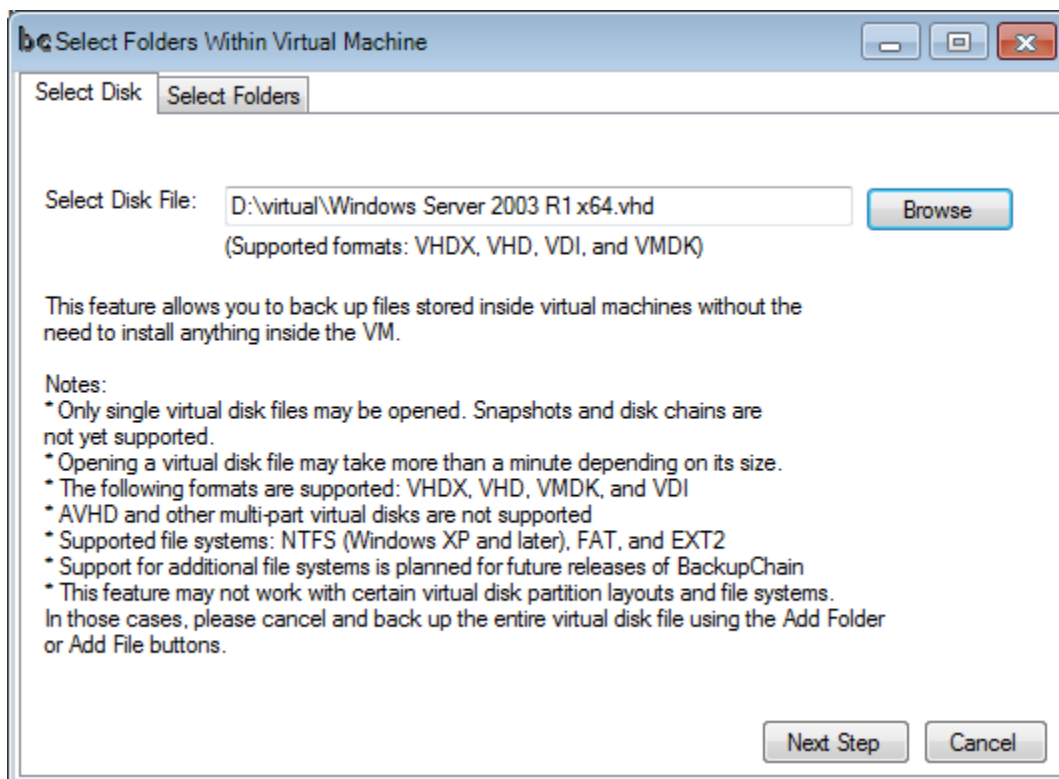
**In addition, no software needs to be installed inside the virtual machine. Note: *This feature is only available in BackupChain Server Enterprise Edition and Platinum Edition.***

Hence, in addition to backing up physical files, you may also select a folder that is stored inside a virtual disk or virtual machine and back it up from the host. *This Granular Backup functionality is available from the host and does not require an agent inside the virtual machine. It does not interfere with the virtual machine either.* As shown below, local and VM files may be backed up simultaneously:



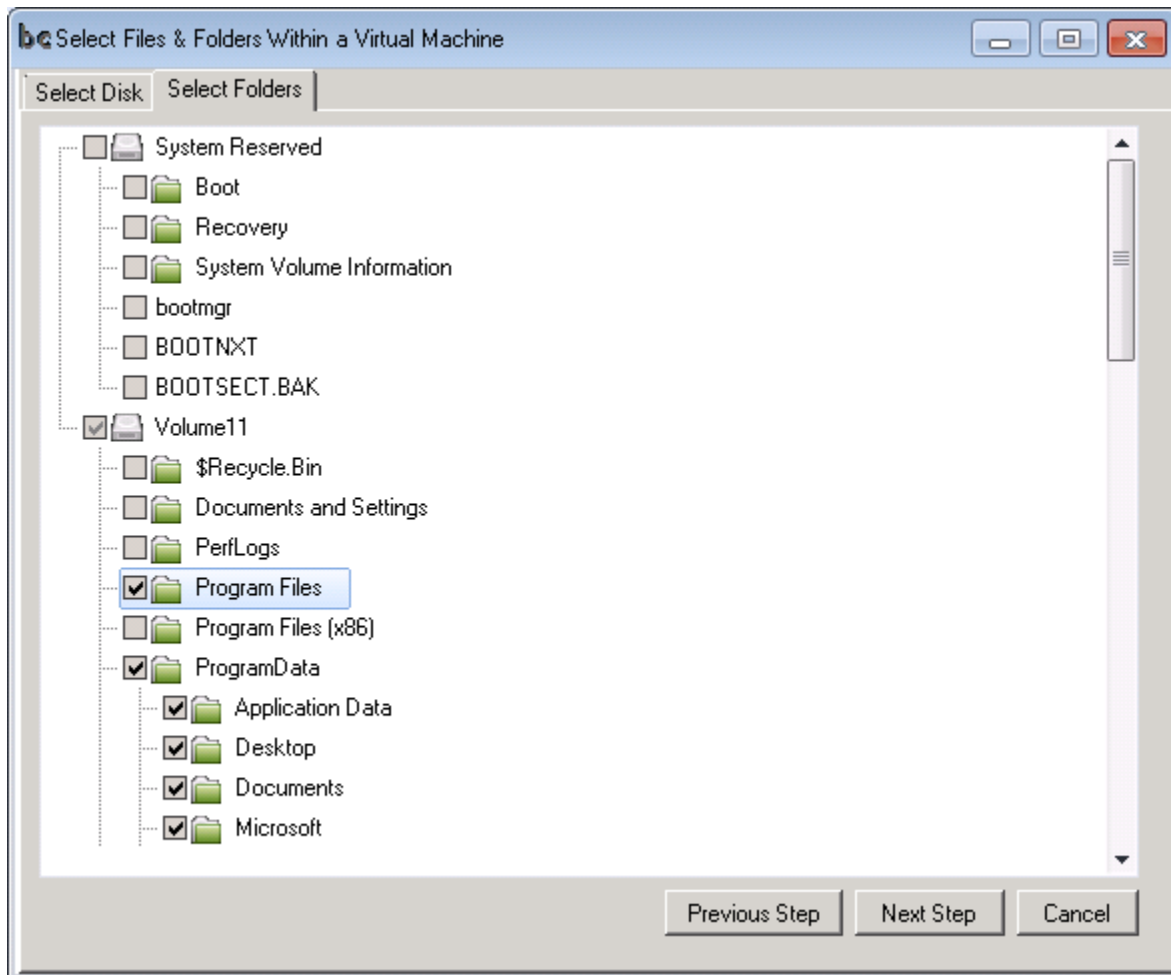
Click “Add Folders” and then “Add Folder Stored Inside a Virtual Machine”.

In the screen “Select Files & Folders within a Virtual Machine”, click browse and navigate to the virtual machine’s virtual disk file. In our example it’s a VHD of a Hyper-V virtual machine:



As you can see above, several limitations apply. Note that this feature is being extended in future releases of BackupChain. Note that VMs with snapshots are not supported (AVHD or AVHDX files or multi-file VMDK in the case of VMware Workstation or VMware Server).

Click “Next Step” and the virtual machine will be opened. You can then select the folders you want backed up:



By continuing with “Next Step” the selection is accepted and BackupChain is configured to back up the virtual machine’s folders.

**Note:** The virtual machine will not be taken offline or during this process or during VM file backup. There will be no interference with the virtual machine processes during backup.

**Note:** If you change the partition layout inside the VM you may need to update the backup folder settings in BackupChain.

## Adding Individual Files to Backup Task

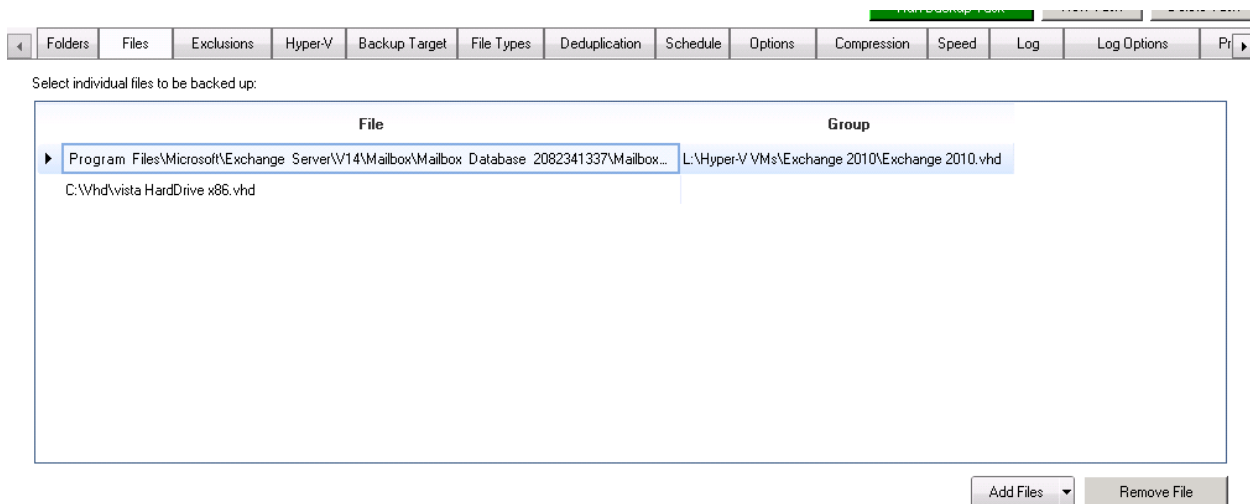
If you don't need to back up entire folders, you can instruct BackupChain to back up just single files.

As with folders, you have the choice to back up:

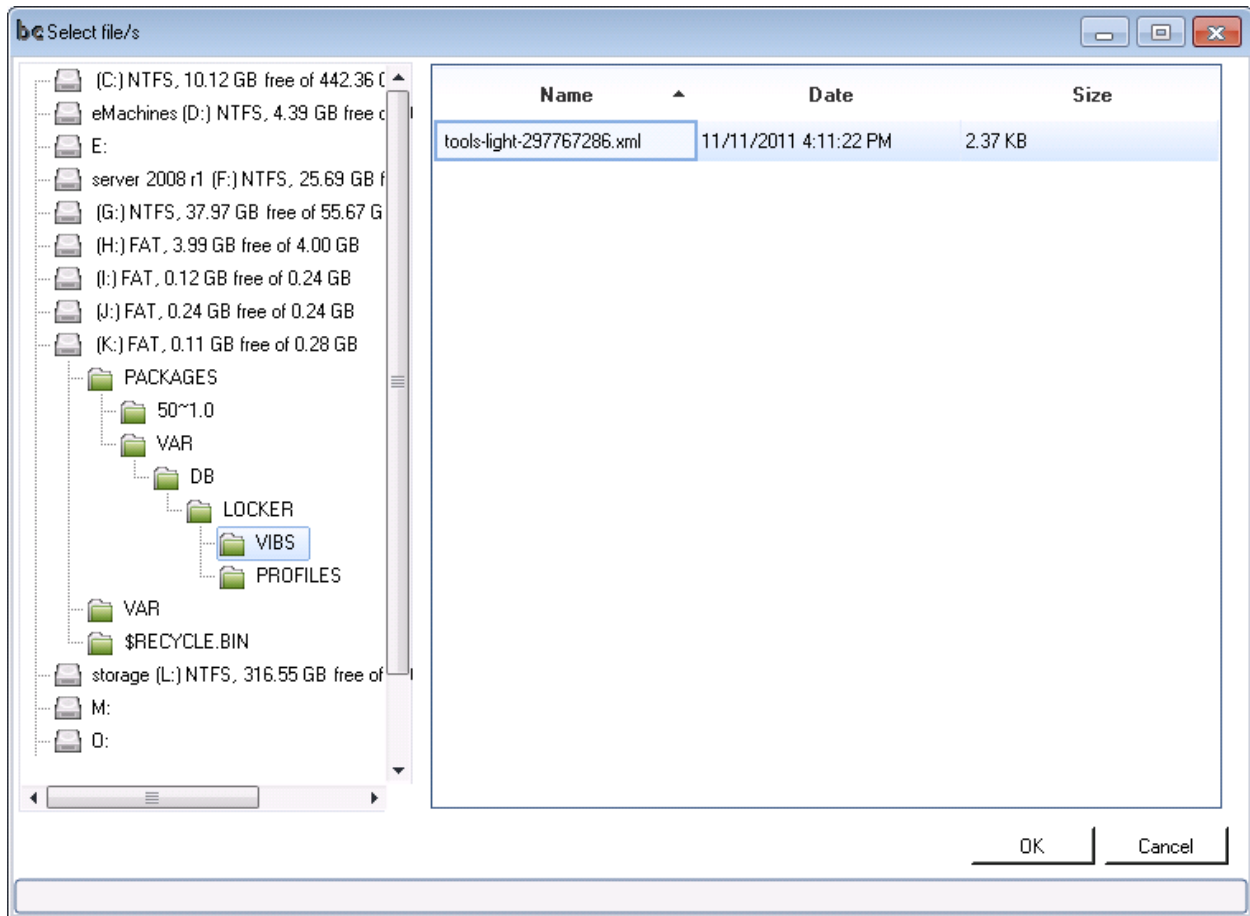
- Local files.
- Files located on a network share.
- Files stored inside a virtual machine disk file.

## Adding Local Files

Navigate to the Files tab to select individual files to be backed up:

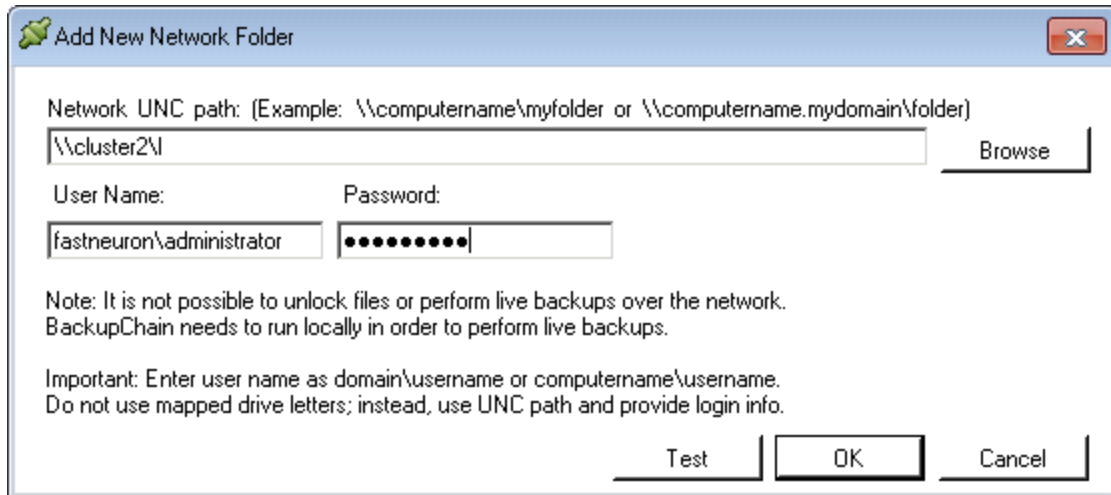


Click the button “Add Files” and then “Add Local Files” to select a single local file to be backed up:



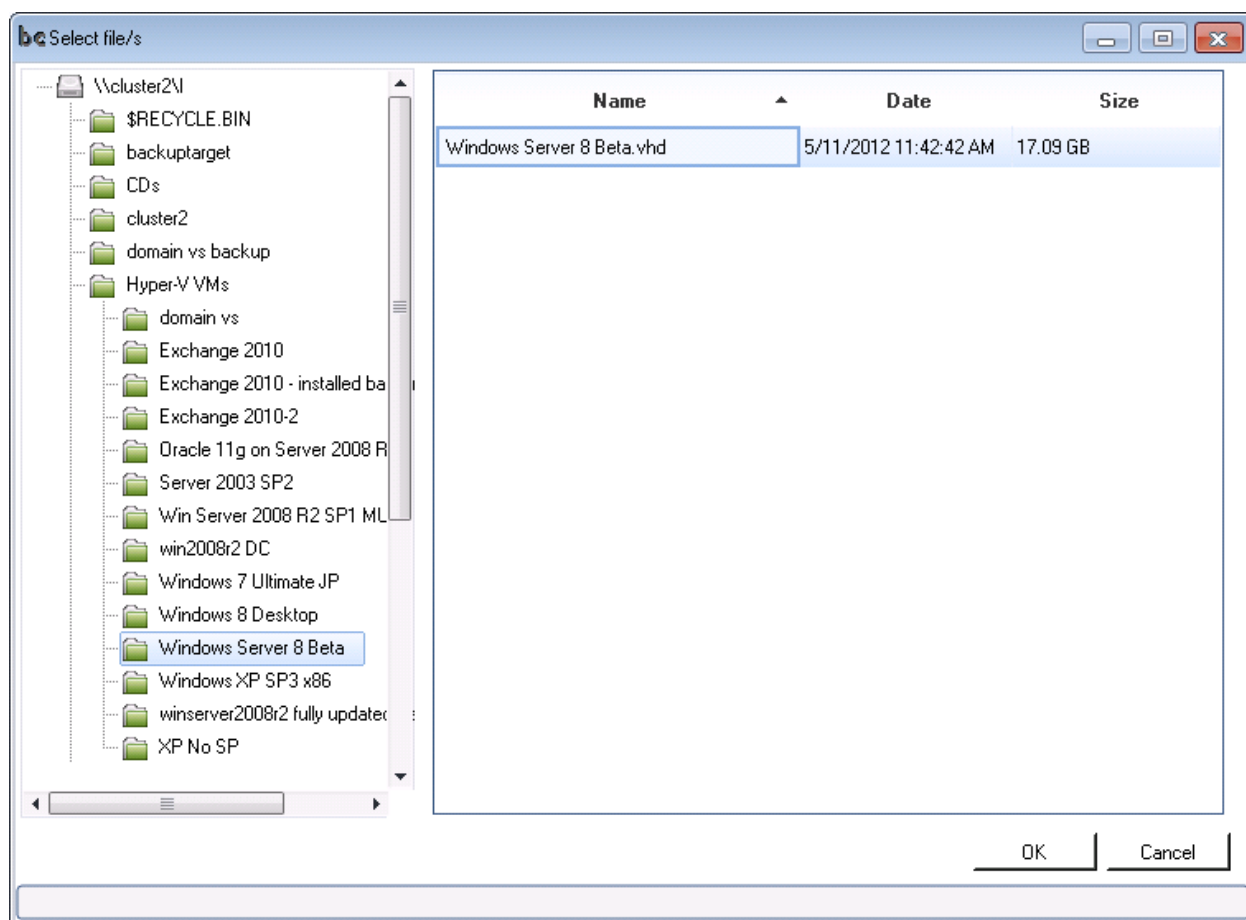
### Adding Individual Network Files to Backup Task

Individual files on a network share may be selected as well. After clicking “Add File” and “Add Network File” BackupChain will display the standard network connection screen discussed in the previous section, followed by a file selection screen:



You can use the Browse button after entering the UNC **path** and user name and password. Note in the above example the domain name is prefixed to the user name. You could also use the following format to address the server in a domain: cluster2.fastneuron (fastneuron being the domain name and cluster2 the server name). Alternatively you can enter the IP address of the server, provided it's static.

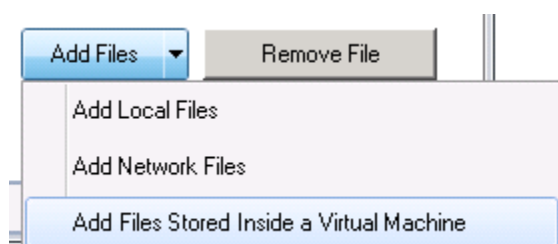
After clicking OK, the file selection screen opens, where you can select the network file and complete the selection process:



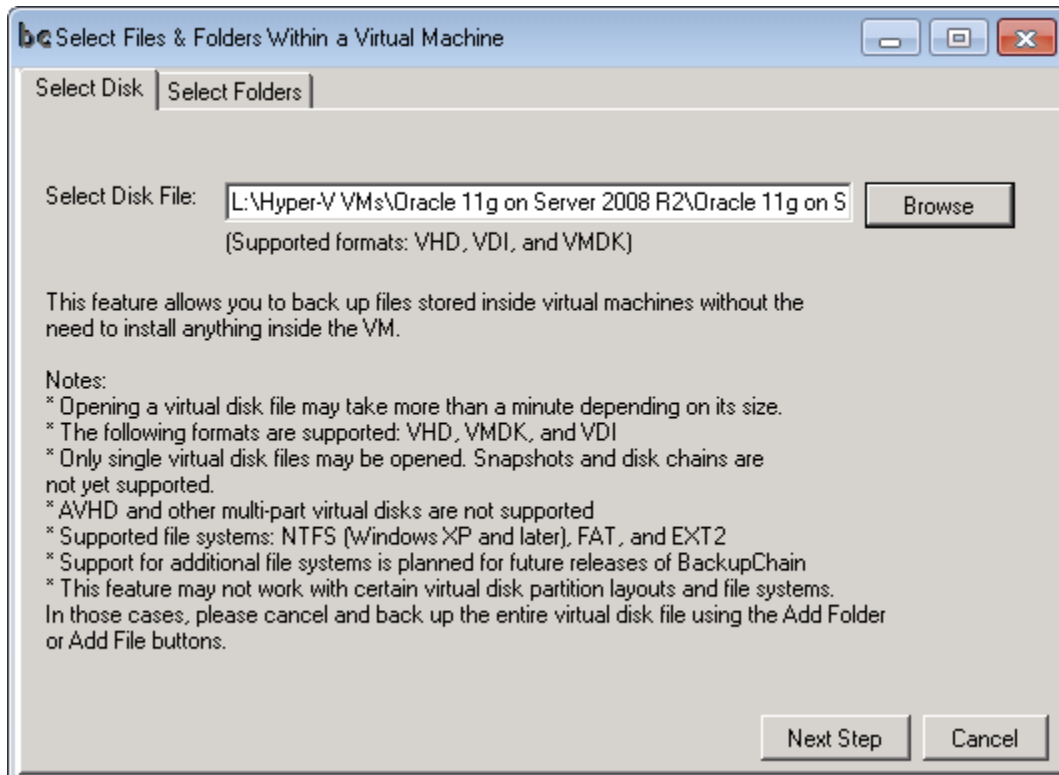
### Adding Files Stored Inside a Virtual Machine to Backup Task (Granular Backup)

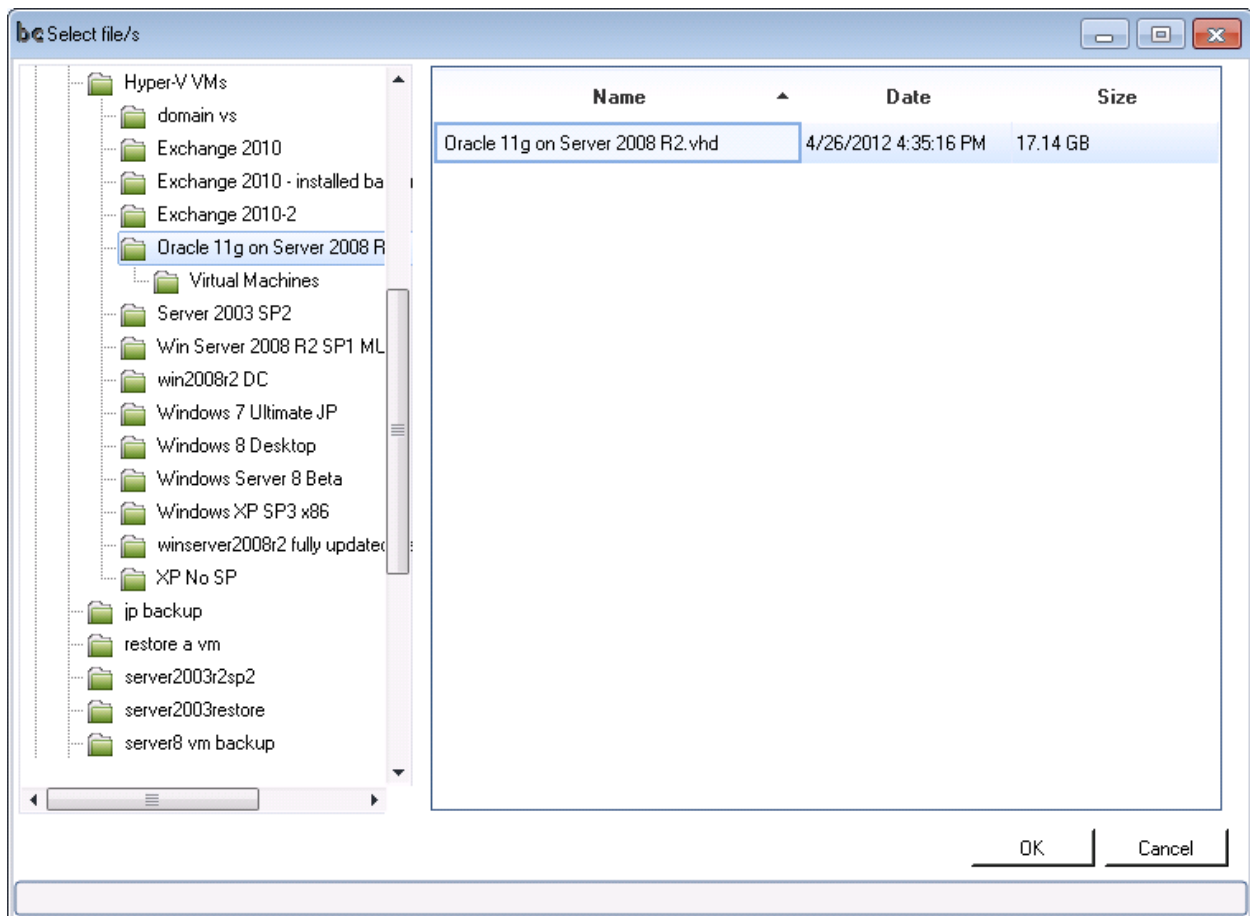
A great feature in BackupChain is Granular Backup which is just as useful as Granular Restore but operating at the backup level rather than the restore process. Granular Backup allows you to take **live backups of files stored inside a virtual machine, without backing up the entire virtual machine and without interfering with the process. In addition, no software needs to be installed inside the virtual machine. Note: This feature is only available in BackupChain Server Enterprise Edition and Platinum Edition.**

Select “Add Files” and then click “Add Files Stored Inside a Virtual Machine”:

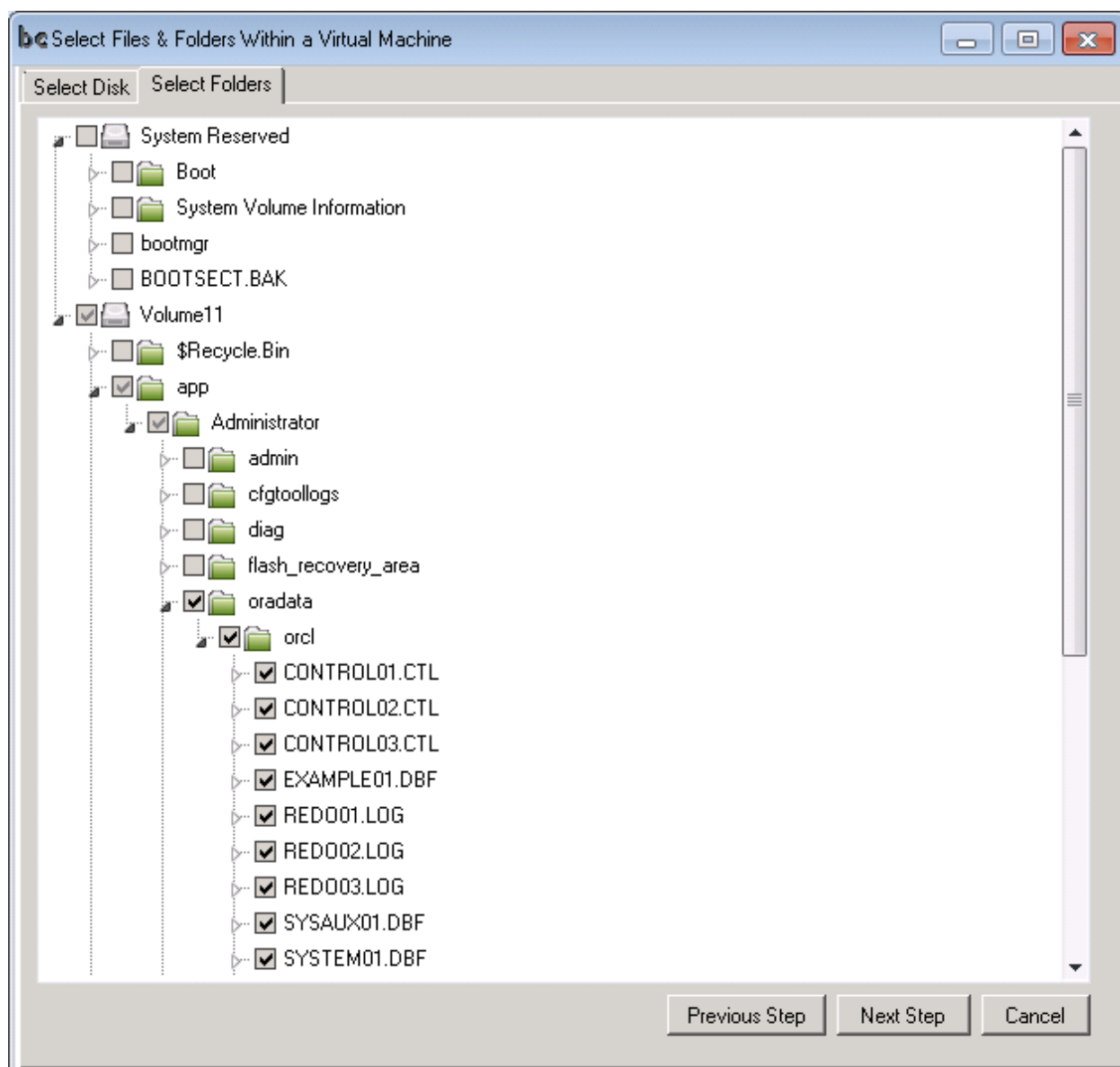


Enter or click Browse to select a virtual machine file:





Click “Next Step” to open the virtual machine file browser and select the files you would like backed up:



## Excluding Folders and Files

If you do not want certain folders or files backed up you can configure BackupChain to omit them:

The screenshot shows the 'Exclusions' tab in the BackupChain configuration window. The window has a tabbed interface at the top with tabs for Folders, Files, Exclusions, Hyper-V, Backup Target, File Types, Deduplication, Schedule, Options, Compression, Speed, Log, Log Options, and Progress. The 'Exclusions' tab is active.

Under the 'Folders to exclude: (Folders you do not want backed up):' section, there is a text area containing the following paths:

- C:\Users\administrator.FASTNEURON\AppData\Local\Microsoft\Windows\Temporary Internet Files
- C:\Windows\TEMP
- C:\Users\administrator.FASTNEURON\AppData\Local\Temp\2
- C:\Windows\Temp
- C:\Users\Default\AppData\Local\Microsoft\Windows\Temporary Internet Files

Below this text area are two buttons: 'Select Folders' and 'Remove Folder'.

Under the 'Files to exclude (Files you do not want backed up):' section, there is an empty text area.

Under the 'Exclude files and folders containing this text in their name (type one or more lines):' section, there is a text area containing the following text:

- pagefile.sys
- hiberfil.sys

Under the 'Advanced: Enter one or more regular expressions to define which files/folders to exclude:' section, there is an empty text area.

At the bottom right of the window are two buttons: 'Save' and 'Enable Schedule'.

Temporary file folders are excluded by default from backups. Add files and folders as needed to exclude more folders when necessary.

The Exclusion tab offers four different ways to exclude files:

- Exclude folders by name.
- Exclude files by name.
- Exclude files if certain text is contained. Use this with caution. Example: if you enter *.tmp* then all files and folders will be excluded if the text *.tmp* appears anywhere in the entire file path.
- For advanced users: You can enter several Regular Expression filters to custom filter your files. The .NET flavor of RegEx is used internally. Ensure your regular expressions are syntactically correct; otherwise, backups will report errors.

Note: If you want to exclude a certain file type, it's simpler to do this in the File Versioning / Cleanup tab. There you should enter a new line for the extension and set the "Min. Number of File Versions" to No Backup. See File Types discussion in next chapters.

## Adding Hyper-V Virtual Machines to Backup Tasks

On a Windows Server 2008 – Windows Server 2019 with Hyper-V role installed, or on a Hyper-V Server 2008 R2 / 2012 / 2016 / 2019 or Windows Core installation, you may back up Hyper-V virtual machines using BackupChain's Hyper-V tab.

**The Hyper-V tab is not available in the BackupChain Professional Edition.**

Inside the Hyper-V tab are two major sections, which differ in the selection mode that is being offered. You can either 'select VMs from a list' by hand or use the "Automatic VM Selection" feature.

**The Automatic VM Selection feature is only available in Server Enterprise and Platinum editions.**

### Manual VM Selection

The manual selection feature allows you to select the VM from a list:

Backup Mode

☒ Sequential VM Backup ☐ Multiple-VM consistent backup

Virtual Machine Selection Mode

☒ I want to select VMs from a list ☐ Automatic VM selection

Manual VM Selection

Select in the table below all Hyper-V Virtual Machines you want backed up:

Select	Name	Size	Files	Path	Checkpoints
<input checked="" type="checkbox"/>	<a href="#">win10 EN</a>	<a href="#">2.1 GB</a>	4	C:\ProgramData\Microsoft\Windows\Hyper-V\Vi...	0
<input type="checkbox"/>	<a href="#">HV2019</a>	<a href="#">2.2 GB</a>	5	F:\server2019\VMs\HV2019\Virtual Machines\8...	0

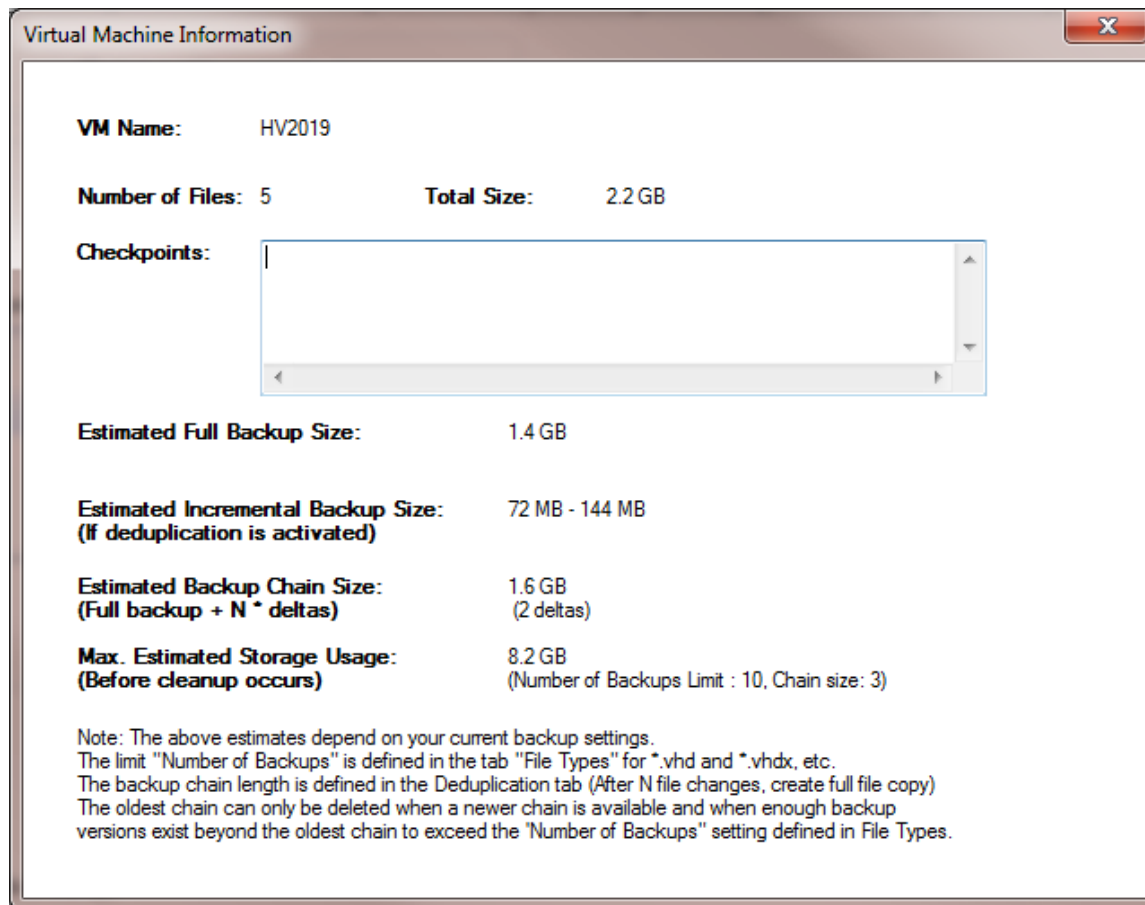
Double click on VM to see storage usage estimates

Refresh

If the VM you selected is not present at the time of backup, the VM will be skipped and an error will be logged. In environments where VMs are moved, either automatically or manually, it's best to use the automatic VM selection feature presented in the next section.

### VM Backup Size Estimation

By double-clicking on the blue links above (the VM name or size field), a new screen will open with detailed size information that is based on your current backup settings. The screen will help you figure out how much space you need to back this VM up, depending on current backup settings and the VM's actual current size:



As you can see above, the VM's size is reported as full backup size, which is the current size in uncompressed form. If your backup task has deduplication and compression switched on, the screen shows **estimated sizes** for increments and full backups. The estimates use 5-10% of compressed size (60% estimate) as rule of thumb. If you switch deduplication and/or compression off, the estimates will update accordingly to reflect the new backup configuration. Note that the traditional backup scheme consists of a full, compressed backup followed by a number of increments or differentials. This forms one backup chain. After completion of one backup chain, a new one is created for easier management and faster restore operations. Once a new backup chain is created, and only then, BackupChain can try to delete the oldest backup chain, if your cleanup settings require it (see tab "File Versioning / Cleanup").

### Automatic VM Selection Feature

The automatic VM selection feature allows you to configure a 'set it and forget it' type of backup configuration and handles the case where certain VMs may move in and out of hosts and certain VMs might be for testing only and do not require backup.

The screen is shown below:

Folders	Files	Exclusions	Hyper-V	Backup Target	File Versioning / Cleanup	Deduplication	Sch
---------	-------	------------	---------	---------------	---------------------------	---------------	-----

**Backup Mode**

☒ Sequential VM Backup
 ☐ Multiple-VM consistent backup

**Virtual Machine Selection Mode**

☐ I want to select VMs from a list
 ☒ Automatic VM selection

**Automatic VM Selection Settings**

This function will automatically back up all VMs on this host without further configuration. All VMs will be backed up. Filter options below are optional.

☒ Include only VMs with this text in their name:  
 (Do not use \* char.; use one line for each filter)

Example to include VM names containing \_Imp and \_Prod, enter:  
\_Imp  
\_Prod

☐ Exclude VMs with this text in their name:  
 (Do not use \* char.; use one line for each filter)

Example to exclude VMs containing "Test" or "Temp" in their names, enter:  
test  
temp

☐ Do NOT back up VMs that are replicated  
☐ Do NOT back up VMs that are shut down

☒ Wait for VM if it is being backed up by another task (avoid backing up the VM twice at the same time)

☒ Log a warning if no VMs are selected for backup

The above screen uses a text to match the VMs that we want backed up: "Production". This means that we have configured our VMs in Hyper-V Management to use the word "Production" somewhere in the VM's name. When BackupChain starts the task and sees VMs with the word Production in their name, they will be automatically included to the backup task.

If you don't provide an inclusion filter, all VMs are included.

In addition, you can exclude VMs based on their name as well. In above exclusion box, you could enter 'test' without the quotes to let BackupChain omit those VMs that contain the word test in their name.

Furthermore, you can omit backups for VMs that are being replicated or that are shut down.

**Note:** If you decide to not back up VMs that are shut down, this will lead to potential data loss. If the VM was backed up live and subsequently turned off, the last backup will be from the time it was running and will not include the changes that have occurred since the last backup. A VM that just happens to be always switched off when the backup task runs, will never be backed up because it will never be seen running at the time when the backup starts. Please keep such potential side-effects in mind when using these filters.

If no VMs are selected for backup, by default, a warning is logged, which you can turn off. There are cases where all VMs are moved intentionally to another host. In such cases you probably do not want the warning to occur and hence you would uncheck that option.

The wait option above is for situations where a VM cannot be backed up simultaneously; hence, BackupChain would need to wait for the other backup (or conflicting operation on the VM) to finish first. It's highly recommended to leave this option on, unless you know for sure the VM can handle simultaneous backups. Some services internal to a VM might use exclusive locks in internal databases and hence backups will fail if run simultaneously. Potentially this can occur with certain SQL Server and Exchange Server databases, which are set up in a way that does not allow for simultaneous backups.

**Note:** You need to select "Hyper-V Backup (Server)" when creating a new task in order to use these screen. In addition, if the task was created using the "Universal Backup" option, the option "Backup all VMs simultaneously" will remain checked and cannot be switched off.

**Note:** On Windows Server 2012, Server 2016, and Server 2019 do not use Universal Backup to backup Hyper-V; use Hyper-V Backup task types instead to back up Hyper-V virtual machines.

To back up a Hyper-V virtual machine, including its snapshots and configuration, simply select it from the list or use the automatic VM selection mode. If you select several virtual machines and want them backed up simultaneously, select the option "Backup all VMs simultaneously". On a very busy system you may want to back up your VMs one after another instead.

**Note:** Sequential virtual machine backup is supported for tasks that were created using the "Hyper-V Backup" option only.

**Note:** Do not use the simultaneous backup option in an attempt to cut down backup time. It may actually shorten the backup time a little but at the expense of much greater resource consumption. In a typical Hyper-V host environment most users prefer to keep their backup process in the background without much interference with the rest of the system. If you uncheck the option "Backup all VMs selected above simultaneously" BackupChain will back up the selected VMs sequentially. Sequential

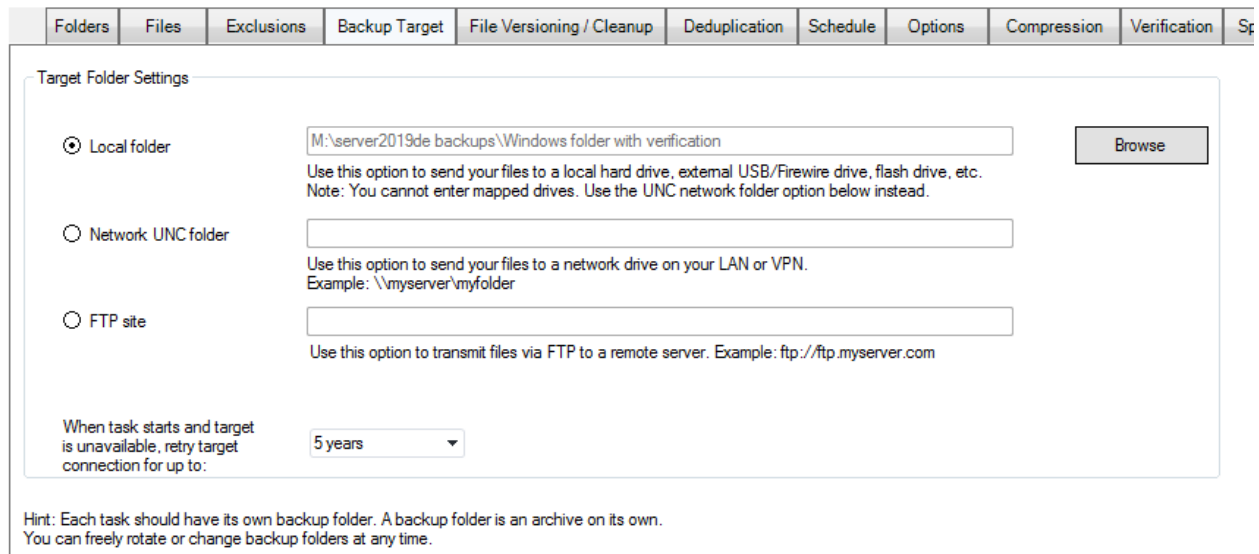
backup is almost as fast as the simultaneous option but much more efficient because it involves only one virtual machine at a time in the backup process.

You may need to click “Refresh” if you added a new VM after BackupChain was started.

**Note:** If you use the Granular Backup option you do not need to check the VM here again, unless you also want a full backup of your VM in addition to selective VM folder backups.

## Selecting a Backup Target

Navigate to the Backup Target tab to specify a backup target:



Target Folder Settings

☒ Local folder

Use this option to send your files to a local hard drive, external USB/Firewire drive, flash drive, etc.  
Note: You cannot enter mapped drives. Use the UNC network folder option below instead.

☐ Network UNC folder

Use this option to send your files to a network drive on your LAN or VPN.  
Example: \\myserver\myfolder

☐ FTP site

Use this option to transmit files via FTP to a remote server. Example: ftp://ftp.myserver.com

When task starts and target is unavailable, retry target connection for up to:

Hint: Each task should have its own backup folder. A backup folder is an archive on its own.  
You can freely rotate or change backup folders at any time.

As shown above, you have the option to choose between local folders, network shares, and FTP / FTPS sites.

The option at the bottom is the retry option. In the example above, the task will retry to reach the target folder for 5 years if it can't be reached at the beginning of the backup. If a target is not found, an error is logged and an email alert is sent once, if configured. The task will then retry every minute until the configured period limit is hit.

### Local Drive Backup Targets

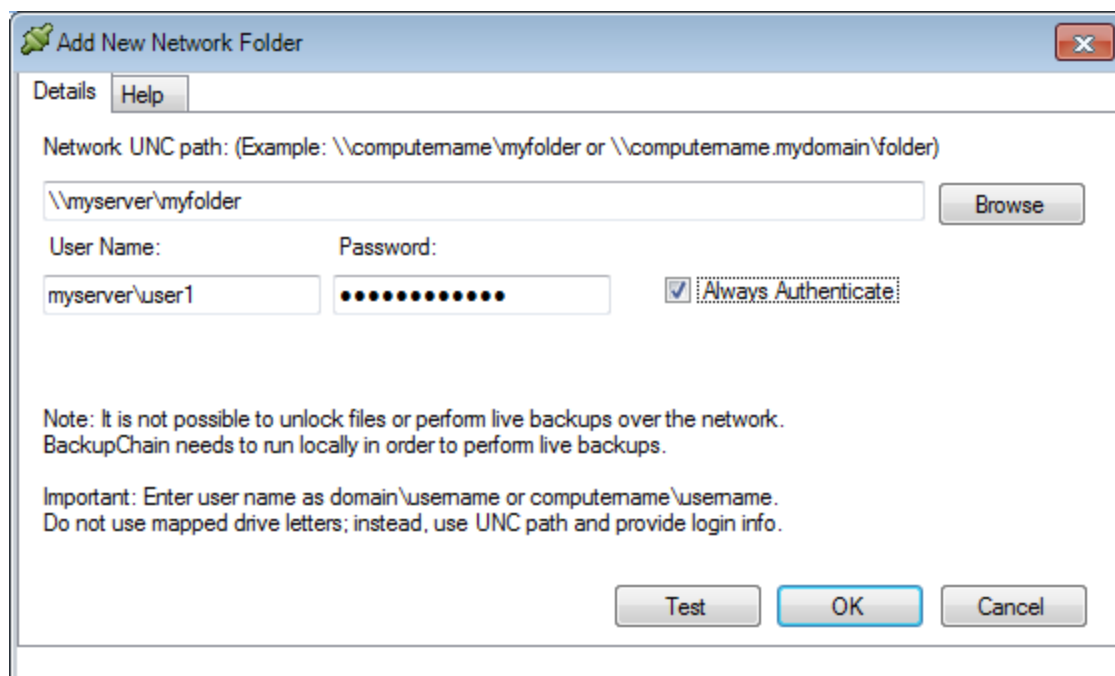
All types of local drives are supported, such as physical internal drives, external drives, USB (all versions), eSATA, FireWire, etc.

**Hints:** For best performance, use NTFS formatted targets. NTFS is also necessary if you use the ACL backup option in the Options tab.

If you format the target drive (or even the source drive) with large clusters (64KB) you could increase backup speed even further.

### Network Folder Targets

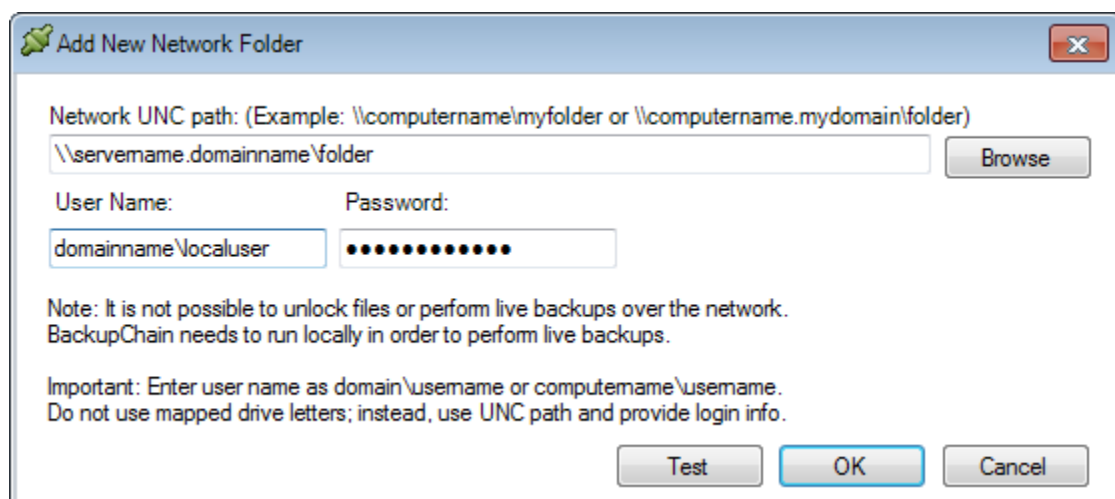
Follow the examples below to specify a network folder (see previous chapters for more details) :



The example above shows a connection to a workgroup computer. Note that it is recommended to prefix the user name with the computer's name to avoid ambiguities.

The option "Always Authenticate" may be turned off in order to re-use existing connections rather than to force re-authentication. This may help avoid some connection issues.

Use the following example as a guide when connecting to domain controlled servers:

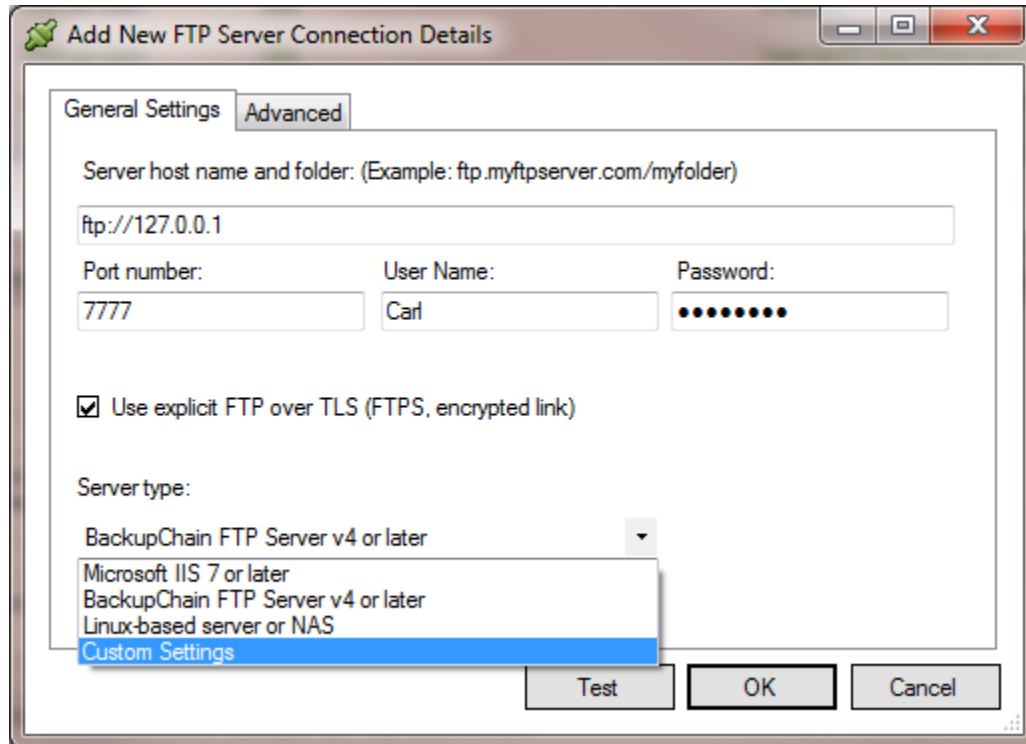


You can use the Browse button after entering a network path, user name and password. User name and password are optional in case the target path is allowed to everyone.

Note that the service “BackupChain Service” is a background service (listed in Service Manager of Microsoft Windows) and the test button and backups run using that service. By default the service is running as SYSTEM user. You may need to change the Log On settings of BackupChain Service to run it as a local/domain administrator instead in case you encounter connection or authentication problems.

### FTP / FTPS Backup Targets

The following is a sample configuration for an FTP backup:



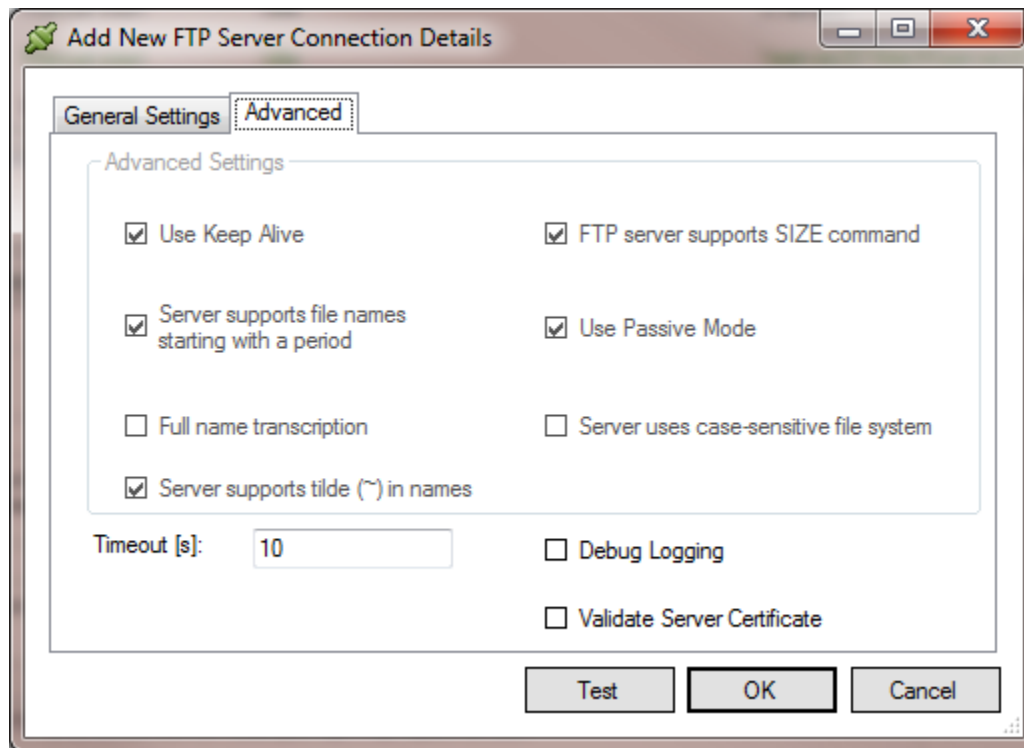
Enter the server’s name or IP address, port number, user name, and password and run a quick test to check your settings.

Some servers (especially some Linux-based variants) that are not following the full FTP standard do not support the SIZE command or Passive Mode, or other certain features. In those cases you may want to try switching those features off to resolve the connection problem by using “Linux-based server or NAS” or custom settings.

In case of a test connection failure an error will be displayed with more information. To investigate the cause of the problem you may also want to check your outbound firewall restrictions and all the settings above.

### Advanced FTP Settings

Advanced FTP settings include server certificate validation, timeout and various features that can be turned on or off. Depending on some FTP servers you may have to switch to custom settings to get backups to work properly.



For example, some Linux systems do not support file names starting with a dot, which can lead to backup errors. Also, if the target uses a case-sensitive file system, as almost all Linux/Unix systems, the option above should be checked because Windows uses a case-insensitive name comparison. Some software systems may produce file names with varying case, which is permitted in Windows but not on case-sensitive file systems. To cover that potential source of errors, check the option “Server uses case-sensitive file system” above.

Certain versions of Microsoft IIS servers do not allow files with ~ in their file names. The IIS preset takes care of that possibility. If you are using a version of IIS that does allow tilde characters, use the custom option and set this option to true again.

## Backup Configuration Depending on File Type (File Versioning / Cleanup Tab)

BackupChain contains a great configuration feature located in the **File Versioning / Cleanup** tab.

You can fine-tune your backups and configure different settings **depending on the file type** of each file.

For example, you may want to treat your heavyweight \*.DB files differently than your Microsoft Word documents \*.DOCX.



Note that files are only backed up if a change occurred; hence, even if the backup runs 100 times but the file hasn't changed, you will see only one file version in the backup folder.

**Alternatively you can enter No Backup to exclude a file type.**

**Or, you may enter ALL to keep all file revisions.**

You will see those two entries in the drop down box when you attempt to edit the File Versioning / Cleanup table:

Folders	Files	Exclusions	Backup Target	File Versioning / Cleanup	Deduplication	Schedule	Options	Compression	Verification	Speed	Log	Log Options	Notes	Progn
---------	-------	------------	---------------	---------------------------	---------------	----------	---------	-------------	--------------	-------	-----	-------------	-------	-------

Define below how you would like files to be backed up, depending on their file type:

Extension	Min. Number of File Versions	Compression	Min. File Age	Deduplication	Delayed Deletion Period	Archive Period
▶ *.*	10	<input checked="" type="checkbox"/>	0 secs	<input type="checkbox"/>	Never delete	Forever
*.pst	No Backup	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever
*.msg	2	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever
*.sc2	3	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever
*.org	4	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever
*.accdb	5	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever
*.adp	6	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever
*.apr	7	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever
	8	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever
	9	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever
	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever
	11	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever
	12	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever

## Enabling / Disabling Data Compression

Data compression is useful for most types of files, especially text files, Word documents, Excel sheets, databases, and program files; however, there are certain file types that do not compress well by their nature: media files, music files, videos, encrypted files, and other digitally recorded data.

Extension	Min. Number of File Versions	Compression	Min. File Age	Delayed Deletion Period	Archive Period
*.db	10	<input checked="" type="checkbox"/>	0 secs	15 days	3 months
▶ *.*	2	<input checked="" type="checkbox"/>	0 secs	Never delete	Forever

In the above example, \*.db type of files are compressed and kept for up to 3 months (after 3 months the backup file will be deleted, **even if the original still exists**) and deleted after 15 days if the original is deleted, whereas all other files (\*.\*) will be compressed and kept forever, even after the original is deleted.

## Minimum File Age

When BackupChain comes across a new file, that is a file that doesn't exist in the backup store, it backs it up immediately.

If, however, the file exists already, BackupChain checks the time difference between the backed up file and the current file. This is how it determines if changes have occurred.

The Minimum File Age setting defines the minimum time period that needs to pass before another backup is taken.

For example, your backup could be scheduled to run continuously (indefinitely) every 30 minutes and your folder contains a very large database file which changes every minute. You may want to back up the database immediately when it appears in the folder but not every 30 minutes thereafter. You may want to restrict database backups (example: \*.DB) to 8 hours instead. By choosing these settings, the backup may run every 30 minutes but the backup of \*.DB files is taken after at least 8 hours passed since the last backup.

A setting of "0 secs" basically turns off this functionality and backs up files immediately when a change is detected; hence, the default is 0 Sec.

Note: you may enter any value you want, such as 45 sec, "1 hour, 9 minutes" as fractions of an hour, "1 year, 3 months".

## Enabling Deduplication Depending on File Type

Extension	Number of Backups	Compression	Min. File Age	Deduplication	Delayed Deletion Period	Retention Period
**	10	<input checked="" type="checkbox"/>	0 secs	<input type="checkbox"/>	30 days	3 months
*.pst	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	30 days	1 year

The example above turns off deduplication as default (\*.\*) but enables it for \*.pst files (Outlook).

You can fine-tune your backup this way and allow deduplication for all files or just particular file types of your choice. You can add new lines to the above File Types table, as shown in the next sections.

Note: v4 renamed "retention period" to "archive period".

## Delayed Deletion Periods Depending on File Type

Extension	Number of Backups	Compression	Min. File Age	Deduplication	Delayed Deletion Period	Retention Period
**	10	<input checked="" type="checkbox"/>	0 secs	<input type="checkbox"/>	30 days	3 months
*.pst	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	30 days	1 year

Note: v4 renamed “retention period” to “archive period”.

Delayed deletion is a feature that prevents the backup store from overfilling. It basically permits BackupChain to delete files once BackupChain detects that a file has been deleted at the original source.

For example, if C:\temp\testfile.txt is deleted today and BackupChain runs tomorrow, the “timer” will start tomorrow. According to the above table (assuming there is no entry for \*.txt), the delayed deletion period is 30 days; hence, BackupChain will delete the file 31 days from now or later, depending on when BackupChain runs after 30 days. The 30 day limit is hence the minimum time to keep a file in the backup folder *after its deletion has been detected*. If your backups runs daily then today’s deleted files will be detected at the next backup run (tonight or tomorrow) and the deletion in the backup folder will take place another 30 days after that.

### File Backup Archive Period Depending on File Type

	Extension	Min. Number of File Versions	Compression	Min. File Age	Deduplication	Delayed Deletion Period	Archive Period
▶	*.*	10	<input checked="" type="checkbox"/>	0 secs	<input type="checkbox"/>	Never delete	3 months
	*.pst	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	1 year
	*.msg	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever
	*.sc2	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever
	*.nm	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever

Note: In v4 the column “retention period” was renamed to “archive period” and “number of backups” to “min. number of file versions”.

The above example shows that the default (\*.\*) is to keep files and file versions for 3 months. For \*.pst files (Outlook), however, we want a archive period of 1 year.

What does this mean exactly? Assuming that your backup runs daily, and assuming you are backing up an active Outlook database, chances are you will hit the 10 ‘Min. Number of File Versions’ limit above (second column).

If you set ‘Min. Number of File Versions’ to ALL, this means there will be no limit in terms of number of changes retained in the backup. However, the archive period of 1 year still applies.

Assuming that your Outlook database is changed and backed up daily, you’ll end up with 365 backups a year. After 365 backups, the retention limit will be hit and the oldest backup version will be deleted. This will ensure your backup history doesn’t go back forever and space is released after a given time limit.

### Example Interpretation of File Versioning / Cleanup table

This is an example of how the following table is interpreted:

Folders	Files	Exclusions	Backup Target	File Versioning / Cleanup	Deduplication	Schedule	Options	Compression	Verification	Speed	Log	Log Options	Notes	Progress
Define below how you would like files to be backed up, depending on their file type:														
Extension	Min. Number of File Versions	Compression	Min. File Age	Deduplication	Delayed Deletion Period	Archive Period								
***	10	<input checked="" type="checkbox"/>	0 secs	<input type="checkbox"/>	Never delete	Forever								
*.pst	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever								
*.msg	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever								
*.sc2	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever								
*.org	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever								
*.accdb	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever								
*.adl	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever								
*.apr	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever								
							Add	Remove						

Note: If \*\*\* is defined, it will be used if there is no exact file extension match.  
 Min. Number of File Versions defines the number of file versions you want to keep for each file, before automatic cleanup occurs.

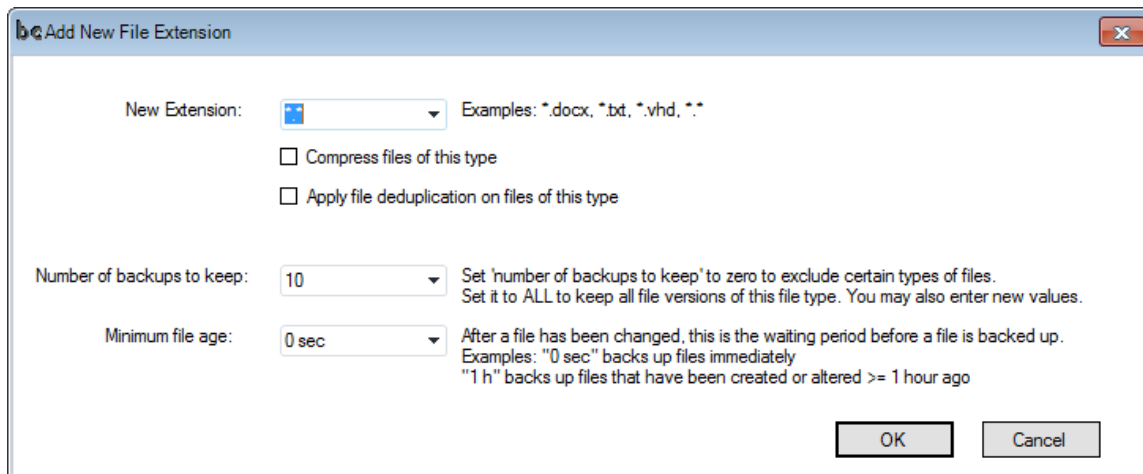
Note: v4 renamed “retention period” to “archive period”. “Number of Backups” was renamed to “Min. Number of File Versions”.

The second line (\*.pst) configures BackupChain to keep the last 10 copies of each file ending with a PST extension. File deduplication is switched on, causing BackupChain to create delta files (incremental or differential). Data compression is also switched on; hence, BackupChain will compress the deltas created. If file deduplication is switched off and data compression is on, BackupChain will create ZIP files instead (or another format as configured in the Options tab). Note that deduplication and compression may also be turned on and off *globally* in their respective tabs “Deduplication” tab and “Compression” tab.

The “Minimum File Age” determines how much time has to pass since the last backup before BackupChain processes a given file type. For example, a setting of 20 minutes means the PST file will not be backed up until at least 20 minutes have passed since its last time the PST file was backed up. If the backups run every minute, BackupChain will hence skip 20 cycles before backing up the same PST file.

The “Minimum File Age” is useful to fine-tune your backups, especially when large files are involved. For example, if your VHD files are over 100 GB and you have small TXT files included in your backup as well, you may want to run the backup every 10 minutes (to back up your TXT files) but you would want the VHDs processed every 60 minutes or less. Instead of backing up everything in 10 minute intervals, you set the \*.VHD minimum file age setting to 60 minutes. Now VHD files must be at least one hour older than the copy in the backup store before they are backed up again. This saves time and resources when files are changed often and backup cycles are kept short. Note that new files will always be backed up immediately, regardless of the minimum file age setting.

To add a new file type definition, click Add:



**Note:** Versions to Keep may be set to “No Backup” to omit a file type from the backup.

You may also set Versions to Keep to ALL, to have BackupChain hold on to all changes made to a particular file type.

Deduplication is recommended for large files that change often and in cases where you want to hold on to an entire history of file changes. These conditions generally apply to database files, virtual machine files, and other large documents.

## How to Exclude a File Type from your Backup

Change the setting “Min. Number of File Versions” to No Backup. In the example below, \*.PST files are excluded from the backup and \*.MSG files are kept with all file revisions but for no longer than 1 year (Archive Period):

Folders	Files	Exclusions	Backup Target	File Versioning / Cleanup	Deduplication	Schedule	Options	Compression	Verification	Speed	Log
Define below how you would like files to be backed up, depending on their file type:											
	Extension	Min. Number of File Versions		Min. File Age		Delayed Deletion Period		Archive Period			
▶	*.msg	all		0 secs		Never delete		1 year			
	*.pst	No Backup		0 secs		Never delete		Forever			
	*.vhd	12		10 seconds		Never delete		Forever			
	*.*	14		0 secs		Never delete		7 days			

The \*.msg example will cause BackupChain to hold each backup file version for up to 1 year and there can be an unlimited number of file versions for \*.msg files during that year. \*.VHD above is configured so that BackupChain will keep up to 12 versions of each VHD file without an archive period defined = store forever.

## How do I Backup Specific File Types Only?

**Remove** the line \*.\*. This will cause BackupChain to only process the file types listed in the table.

The line \*.\* is a “catch-all” and is there to define the default backup setting for all file types not listed elsewhere. The example below shows the line \*.\* removed; hence, only \*.msg, \*.pst, and \*.vhd files will be backed up:

Folders	Files	Exclusions	Backup Target	File Versioning / Cleanup	Deduplication	Schedule	Options	Compression	Verification	Speed	Log
Define below how you would like files to be backed up, depending on their file type:											
	Extension	Min. Number of File Versions		Min. File Age	Delayed Deletion Period		Archive Period				
	*.msg	all		0 secs	Never delete		1 year				
	*.pst	No Backup		0 secs	Never delete		Forever				
	*.vhd	12		10 seconds	Never delete		Forever				

## Deduplication (Delta Compression) Settings

Deduplication, also known as delta compression, is a process that reduces redundancy when backing up a large file on a regular basis. Delta compression algorithms cut down storage usage and backup time by detecting the change that occurred between backup cycles.

Folders	Files	Exclusions	Backup Target	File Types	Deduplication	Schedule	Options	Compression	Speed	Log
<div> <input checked="" type="checkbox"/> Activate Deduplication (Delta Compression) </div> <div> Delta type: <span>Incremental</span> </div> <div> Every <span>5</span> cycles, create a full file copy </div> <div> Delta Block Size: <span>4 MB</span> </div> <div> Max. Deduplication Workers <span>2</span> </div> <div> <p>Note:</p> <ol style="list-style-type: none"> <li>1. Delta compression detects file content changes between backup cycles and is ideal for backing up large files, such as virtual machines, databases, and Microsoft Outlook databases.</li> <li>2. Use larger block sizes for larger files. It is recommended to use &gt;1MB block sizes for files greater than 1 GB.</li> <li>3. Restore operations are more efficient when full copies are recreated more frequently. The ideal number of versions before creating a full copy depends on the file size of the data file. For quick restores, recreate full copies more frequently.</li> <li>4. Incremental deltas store the changes from file version to file version and are more economical with storage but take more time to restore.</li> <li>5. Differential deltas store the changes compared to the first file version and restore faster; however, they are not as efficient and use more storage space.</li> <li>6. Increasing the number of deduplication workers may help running backups faster at the cost of an increase in RAM and CPU usage. It is not recommended to use more workers than available CPU cores. Before increasing this number, it is recommended to check whether the CPU is indeed the bottleneck.</li> </ol> </div>										

In order to turn off deduplication globally, uncheck “Activate Deduplication (Delta Compression)” in the Deduplication tab.

The “delta type” setting switches between incremental and differential backup deduplication.

Delta block size is the granularity by which deduplication works, basically the smallest detectable change. If a large size is used, it speeds up the process and reduces overhead but wastes more storage space. A small block size is more space efficient but involves more overhead and hence takes more time to complete.

The number of deduplication workers controls parallel execution of the deduplication process. You can get significant speed gains by allowing more than one CPU core to deduplicate a single file. However, RAM and CPU consumption will rise significantly as more workers are deployed.

### What is Incremental Deduplication?

Incremental deduplication is a fundamental backup term and refers to a backup chain that starts with a full copy, followed by increments. The increments are based on a file content comparison between the current file copy and the copy from the previous backup cycle. Hence, each successive increment depends on the previous one.

Advantages: Fast and efficient backups, increments are as small as possible.

Disadvantages: Each increment requires its own step when restoring; hence, restore takes longer than with differential deduplication. In addition, access to all increments as well as the last full copy is needed when restoring.

### What is Differential Deduplication?

Similar to incremental deduplication, differential deduplication starts off with a full copy of the file. Then, increments are generated with each backup cycle but all refer to the last available full copy of the file. The difference to incremental deduplication is that the current file version is compared to the last full copy of the file. While incremental deduplication creates a backup chain (full copy, followed by interdependent increments), differential deduplication creates a star relationship: each differential depends on the last full copy, not the last differential.

Advantages: Faster restore time, since only the last full copy and the last differential delta are needed. The restore process is hence a one or max. two step process.

Disadvantages: Differentials tend to get bigger after each backup because the percentage of change between the last full copy and the current backup cycle (usually) grows larger.

### Why and How to Create Intermittent Full Copies

There is no right or wrong answer and no strategy suits all situations.

The setting 'Every X cycles, create a full copy' is a useful remedy to balance the advantages and disadvantages of the incremental and differential backup strategies discussed above.

A setting of "5" creates a full copy every five backup cycles. For example, if your backup runs daily, every 5<sup>th</sup> day a full copy will be generated rather than an incremental or differential delta file.

The advantage of this strategy is that it cuts down restore time for incremental backup schemes because there won't be more than five incremental steps to restore.

The advantage for differential backup schemes is that the differential delta files will be much smaller.

The disadvantage of recreating full copies at regular intervals is that they use more space in the backup store.

It is the responsibility of the administrator / user to balance the above pros and cons and match them to his/her goals and preferences. All strategies have advantages and disadvantages and each setting may be different from another.

For most large files, such as databases and virtual machine images we recommend a setting of "5" to "10", to keep restore time and backup store usage as short as possible, while providing efficiently small delta files.

### **Delta Block Size and its Meaning**

When comparing files for the purpose of deduplication, the file is processed in chunks for easier processing. Smaller delta blocks lead to a more economic change detection and reduce waste; however, smaller delta blocks require more overhead and management resources; hence, the backup runs slower.

Larger delta blocks significantly reduce the overhead when deduplicating a file and therefore the backups run faster. On the other hand, larger chunks waste more space in the backup store and require more RAM during processing.

To sum up, use smaller deltas to create economic deltas with less RAM but at a slower rate, and use large deltas to speed up your backups, but be informed that large delta blocks require more RAM and create larger delta files. We found a delta block size between 4MB and 16MB suits most applications.

### **How to Turn off Deduplication for all Files**

For each backup task you can completely switch off deduplication by unchecking "Activate Deduplication (Delta Compression)" , see above.

## How to Turn on Deduplication for Specific File Types

See above section.

First, ensure the setting “Activate Deduplication (Delta Compression)” (see screenshot above) is checked. Then navigate to the File Versioning / Cleanup tab and check “deduplication” in the table for the file type:

Folders	Files	Exclusions	Hyper-V	Backup Target	File Versioning / Cleanup	Deduplication	Schedule	Options	Compression	Verification	Speed	Log	Log Options
---------	-------	------------	---------	---------------	---------------------------	---------------	----------	---------	-------------	--------------	-------	-----	-------------

Define below how you would like files to be backed up, depending on their file type:

	Extension	Min. Number of File Versions	Compression	Min. File Age	Deduplication	Delayed Deletion Period
▶	*	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete
	*.vhd	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete
	*.avhd	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete
	*.vhdx	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete
	*.avhdx	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete
	*.vud	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete
	*.hdd	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete
	*.sav	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete

The example above has deduplication switched ON for VHD, AVHD, and VHDX files.

It is recommended to compress files as well when using deduplication, unless you know beforehand that the original file is encrypted or does not compress well, for example if you are dealing with encrypted virtual disk images or encrypted database files.

## Schedule Settings

BackupChain a powerful scheduler which offers the following features:

1. It runs backups automatically even when you are not logged into Windows.
2. Continuous backups (repeat backup at given intervals indefinitely).
3. One time execution: Start backup task in the future, once.
4. Daily execution: Start backup task every day or every N<sup>th</sup> day at a certain time.
5. Weekly: Start backup tasks every week or every N<sup>th</sup> week at a certain time.
6. Monthly: Select individual months, weeks, and days to run your backup, including special features: first, second, third, and last weekday of a month, such as “last Wednesday of January and February at 3 AM”.
7. The ability to run missed tasks immediately as soon as the system boots up.
8. The ability to terminate long-running tasks automatically using a timeout.
9. The ability to repeat tasks in-between their scheduled intervals, such as “run task daily at 6 AM and repeat every hour for four hours).
10. The ability to expire tasks at a certain date.
11. The ability to stipulate fractions of time, see example below (2 hours + 2 minutes).

Hint: Remember to click Enable Autopilot when you're done.

**Settings**

Run this task: Start this task on: 8/ 4/2020 4:36 PM

☐ Manually  
☒ Continuously  
☐ One time  
☐ Daily  
☐ Weekly  
☐ Monthly

Repeat continuously every: 2 hours + 2 minutes

Note: Custom values may also be entered. Example: 8 hours, 30 minutes

**Advanced settings**

☒ Enable schedule

☒ Repeat task in-between scheduled intervals every: 1 day + 1 hour for a duration of: 1 day + 10 hours

☐ Run task once if missed

Save

Note, in order to temporarily prevent a task from being started automatically until you are done editing, you could disable the task in the Options tab or by right clicking on the task in main task list above.

“Repeat task in-between scheduled intervals every” X days/hours/minutes for a duration of Y days/hours/minutes. This setting allows you to repeat the task between intervals. For example, you may want to run a task once a day (daily schedule) and then repeat the task every 45 minutes for four hours.

“Run task ASAP if missed” should be switched on if you want BackupChain to start tasks immediately at boot time in case the server was down during the task’s scheduled startup time.

“Expire this task on” sets an expiration date for this task schedule. The scheduler will stop running this task at the specified date if you enable this option.

## Continuous Backups

Continuous here means indefinite repetition at given intervals.

You may want to set up a continuous backup task to back up your data at regular intervals. The example above uses 2 hours and 2 minutes, or 122 minutes. BackupChain will immediately start this task when the system boots and then wait 2:02:00 hours before repeating this task.

## One-Time Backups

One-time backups are scheduled to run a single time in the future. To use this option, select one-time backups and select a start date (“Start this task on:”)

## Daily Backups

In the example below, the backup task starts every day at 1:27 PM. If you want to run the task every 3<sup>rd</sup> day, enter “3” for “Repeat task every X days”.

Folders	Files	Exclusions	Backup Target	File Types	Deduplication	Schedule	Options	Compression	Speed	Log
<div>Settings</div> <div> Run this task: Start this task on: 6/23/2012 1:27 PM </div> <div> <input type="radio"/> Manually <input type="radio"/> Continuously Repeat task every: 1 day(s) <input type="radio"/> One time <input checked="" type="radio"/> Daily <input type="radio"/> Weekly <input type="radio"/> Monthly </div>										

## Weekly Backups

The example below runs the backup task every 3<sup>rd</sup> Monday and Friday at 1:27 PM:

Folders	Files	Exclusions	Backup Target	File Types	Deduplication	Schedule	Options	Compression	Speed	Log	Log Options	Progress
---------	-------	------------	---------------	------------	---------------	----------	---------	-------------	-------	-----	-------------	----------

Settings

Run this task: Start this task on: 6/23/2012 1:27 PM

☐ Manually  
☐ Continuously  
☐ One time  
☐ Daily  
☒ Weekly  
☐ Monthly

Repeat task every: 3 week(s) on:

☐ Sunday ☒ Monday ☐ Tuesday ☐ Wednesday  
☐ Thursday ☒ Friday ☐ Saturday

If you wanted to run the task every Sunday, select Sunday and enter “1” for “Repeat task every 1 week”.

## Monthly Backups

The most complicated schedule settings can be handled using the monthly backup scheduler setting. The example below runs the backup only on the first day of January and February at 1:27PM:

Folders	Files	Exclusions	Backup Target	File Types	Deduplication	Schedule	Options	Compression	Speed	Log
---------	-------	------------	---------------	------------	---------------	----------	---------	-------------	-------	-----

Settings

Run this task: Start this task on: 6/23/2012 1:27 PM

☐ Manually  
☐ Continuously  
☐ One time  
☐ Daily  
☐ Weekly  
☒ Monthly

Months:

☒ January  
☒ February  
☐ March  
☐ April  
☐ May  
☐ June  
☐ July

Days:

☒ Days: 1 2 3  
☐ On: First Second Third

☐ Sunday  
☐ Monday  
☐ Tuesday

Using the “On” switch, you can stipulate weekdays instead, such as “Second Thursday”. In that case the backup would run only on every second Thursday of January and February.

## The Options Tab

A plethora of options are available in the Options tab:

Folders	Files	Exclusions	Backup Target	File Types	Deduplication	Schedule	Options	Compression	Speed	Log	Log Options	Progress
<div>Task Settings</div> <div> <input checked="" type="checkbox"/> Allow this backup task to run         </div> <div>           Backup task name: <input type="text" value="single type backup"/> </div> <div>           Folder for temporary files: <input type="text"/> <input type="button" value="Browse"/> </div> <div> <small>Note: create new folder for temp files because all contents will be deleted!</small> </div> <div> <input type="checkbox"/> Move old file versions to recycle bin instead of deleting them         </div> <div> <input type="checkbox"/> Stop task if it runs longer than: <input type="text" value="8 hours"/> </div>												
<div>Locked File Handling</div> <div> <input checked="" type="checkbox"/> Copy open and locked files           <input checked="" type="checkbox"/> Always back up locked files (ignore their timestamp)           <input checked="" type="checkbox"/> Strict VSS Handling         </div> <div>           Exclude these VSS writers: (separate with semicolon ";") <input type="text"/> </div>												
<div>Access Control Lists</div> <div> <input type="checkbox"/> Back up Directory ACLs           <input type="checkbox"/> Back up File ACLs         </div> <div> <small>Note: In order to back up ACLs, the backup target needs to be formatted using NTFS.</small> </div>												
<div>Sound Alert Settings</div> <div> <input type="checkbox"/> Play this sound when an error occurs: <input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Speaker"/> </div> <div> <input type="checkbox"/> Play this sound when the task has completed successfully: <input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Speaker"/> </div>												

And if you scroll further down you'll find additional options:

External Utilities

☐ Run Program when this backup task starts:

☐ Wait for program to finish
 ☐ Check exit code:

☐ Run Program when this backup task ends:

☐ Wait for program to finish
 ☐ Check exit code:

Task Chaining

Task chaining allows you to run a task after this task ends. Circular references should be avoided.

Task to run:

☒ Do not run above task if this task fails

☒ Wait for task to finish

## Task Settings

“Run this backup task” enables or disables the task completely. Uncheck a task here if you don’t want it to start automatically.

“Backup Task Name” holds the name of the task. You can rename a task by changing the text in the Options tab.

“Folder for temporary files” specifies a folder for ZIP and other temporary file handling. Usually temporary files are necessary when using FTP or other remote backups where no direct file access is available. The default folder is C:\ProgramData\BackupChainService\temp when no folder is provided.

The option “Move old file versions to recycle bin instead of deleting them” does not delete files but moves them off to the bin; however, the recycle bin in Windows has its own retention setting and may delete files if it runs full.

The option “Stop task if it runs longer than” stipulates a time limit after which the task cycle will be canceled. If the task is scheduled to run again, such as daily, it will be started again at the next scheduled intervals.

## Locked File Handling

**Note:** this feature works only on local NTFS drives (at least one drive must be NTFS). You cannot unlock files from a distance / remote computer. BackupChain needs to run locally in order to unlock files.

Locked file handling allows BackupChain to access exclusively opened files, such as system files, application files, database files, and virtual machine files and provide a live backup. Live backups are only guaranteed to work if the application that locks the file is VSS compliant. (Volume Shadow Copy Service).

In order to provide a live backup, the hard drive is brought to a consistent state. BackupChain can create valid and application-consistent live backups when the application you wish to back up ships with its own VSS writer, such as Hyper-V, Microsoft SQL Server, etc. The NTFS file system is also brought to a consistent state and hence the file system and operating system are brought to a valid state as well before the backup begins.

**Note:** it is important to use the correct Backup Type when creating a new backup task. Use Universal Backup if you are not sure, or if you want to back up several services or applications simultaneously.

For example, do not create a SQL Server task and then add folders for Hyper-V. If you want to back up SQL Server, use a SQL Server backup type when creating the task and then only add the files and folders related to SQL Server. Other data files may be added as well but do not add files that are controlled by another application, such as Hyper-V.

“Exclude these VSS writers” is a semicolon separated list of VSS writers that you wish to exclude from the backup. Use this option at your own risk. It is provided to resolve problems with specific applications during backup.

**Note:** You can switch off locked file handling and BackupChain will simply skip locked files.

“Strict VSS Handling” is recommended to be used unless there is a VSS problem.

## Sound Alert Settings

Use the sound alert options to play a sound (MP3, WAV, etc.) file when the task finishes successfully or fails. Select a sound file for each box found in the “Sound Alerts Settings” box of the Options tab.

## External Utilities

You can run external utilities when a backup starts and finishes. You can use this feature to control external resources or run external notification tools.

One application of external utilities is to bring a database offline before the backup and then start it again once the backup has finished.

If you use the “Check exit code” option, BackupChain will terminate the backup and report an error if the utility returns a different exit code than expected.

You can run batch files or PowerShell commands as well by using %SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe and its switches to run a stored script.

Hints: Use quotes around path names. Use the > operator to send console output to a log file.

Example:

```
C:\app\Myapplication.exe someparameter >c:\temp\mydir.txt
```

The above command may produce errors but because the backup runs unattended you won't see them. The above “>” operator routes all console output to mydir.txt so it can be inspected later on if an error occurs.

## Access Control List

You can switch on Access Control List backup for directories and files in the Access Control Lists box.

Note that ACLs are only available on NTFS, so your source and destination folders need to be formatted using NTFS in order for this feature to work.

## Task Chaining

Task chaining allows you to run a task after another task has finished. Hence, you can ensure that the second task never overlaps with the first task by simply chaining it. In addition, you can omit the second task if the first one failed or was stopped. A wait option is also available which can be used to prevent the first task from running again until the second task is finished. Furthermore, if you wait for the second task, the first task's final status will depend on the success of the secondary task (and tasks further down the chain if more than one task is chained in sequence).

**Task Chaining**

Task chaining allows you to run a task after this task ends. Circular references should be avoided.

Task to run: vmware

☒ Do not run above task if this task fails

☒ Wait for task to finish

## The Compression Tab

The compression tab offers compression options and encryption options. Note that if you want to encrypt a file it also needs to be compressed. This has two reasons / advantages.

Files are being compressed first and then encrypted which improves randomization and makes the encrypted file more secure. Second, the encrypted file needs a file container, also known as a file format. Standard ZIP and other formats are available containers for encrypted files.

Encryption occurs using AES 256, today's military-strength encryption algorithm.

In order to turn on encryption, turn on compression first and select a mode. You could even select the compression mode "no compression" which puts ZIP in plain archiving mode if you know ahead of time that your files don't compress well anyways, as in the case of music and other media files.

Archive mode (no compression mode) is engaged automatically for the file types listed in the box below:

Folders	Files	Exclusions	Backup Target	File Types	Deduplication	Schedule	Options	Compression	Speed	Log	Log Options	Progress																																																
<div> <input checked="" type="checkbox"/> Turn on data compression to save space           <input type="checkbox"/> Encrypt and protect my files with a password         </div> <div>           Compression format: <span>Standard ZIP (.zip)</span>           Password: <input type="text"/> </div> <div>           Compression mode: <span>Fastest compression</span>           Confirm password: <input type="text"/> </div> <div>           Do not compression for these file types (Note: An uncompressed archive will still be created if compression is turned on above):           <table border="1"> <tbody> <tr><td>.7z</td><td>.mpg</td></tr> <tr><td>.ace</td><td>.png</td></tr> <tr><td>.arc</td><td>.rar</td></tr> <tr><td>.arj</td><td>.swf</td></tr> <tr><td>.avi</td><td>.tgz</td></tr> <tr><td>.bz2</td><td>.tib</td></tr> <tr><td>.bzip</td><td>.tib</td></tr> <tr><td>.bzip2</td><td>.tif</td></tr> <tr><td>.cab</td><td>.tiff</td></tr> <tr><td>.bz2</td><td>.wav</td></tr> <tr><td>.cdx</td><td>.wma</td></tr> <tr><td>.gho</td><td>.wmv</td></tr> <tr><td>.gif</td><td>.wvl</td></tr> <tr><td>.gz</td><td>.z</td></tr> <tr><td>.gzip</td><td>.zip</td></tr> <tr><td>.jar</td><td>.zoo</td></tr> <tr><td>.jpg</td><td></td></tr> <tr><td>.jpeg</td><td></td></tr> <tr><td>.lzh</td><td></td></tr> <tr><td>.mov</td><td></td></tr> <tr><td>.mp1</td><td></td></tr> <tr><td>.mp2</td><td></td></tr> <tr><td>.mp3</td><td></td></tr> <tr><td>.mpeg</td><td></td></tr> </tbody> </table> </div> <div>           Note: Choose 7-zip format for best compression and performance. Choose ZIP for best compatibility with other systems. It is recommended to switch on compression when using file deduplication (Delta Compression). Encryption is based on AES-256.           <div> <input type="button" value="Add File Type"/> <input type="button" value="Remove File Type"/> </div> </div>													.7z	.mpg	.ace	.png	.arc	.rar	.arj	.swf	.avi	.tgz	.bz2	.tib	.bzip	.tib	.bzip2	.tif	.cab	.tiff	.bz2	.wav	.cdx	.wma	.gho	.wmv	.gif	.wvl	.gz	.z	.gzip	.zip	.jar	.zoo	.jpg		.jpeg		.lzh		.mov		.mp1		.mp2		.mp3		.mpeg	
.7z	.mpg																																																											
.ace	.png																																																											
.arc	.rar																																																											
.arj	.swf																																																											
.avi	.tgz																																																											
.bz2	.tib																																																											
.bzip	.tib																																																											
.bzip2	.tif																																																											
.cab	.tiff																																																											
.bz2	.wav																																																											
.cdx	.wma																																																											
.gho	.wmv																																																											
.gif	.wvl																																																											
.gz	.z																																																											
.gzip	.zip																																																											
.jar	.zoo																																																											
.jpg																																																												
.jpeg																																																												
.lzh																																																												
.mov																																																												
.mp1																																																												
.mp2																																																												
.mp3																																																												
.mpeg																																																												

## The Verification Tab

The verification tab offers various features to protect your backups:

Folders	Files	Exclusions	Backup Target	File Versioning / Cleanup	Deduplication	Schedule	Options	Compression	Verification	Speed
<div> <input type="checkbox"/> Verify files after backup           </div> <div>             Remote targets only: Do not verify files above this size: <input type="text" value="50"/> [MB]           </div> <div>             Remote targets only: Percentage of files to verify: <input type="text" value="1.0"/> [0.1 - 100%]           </div> <div> <input type="checkbox"/> Turn on bit rot and manipulation protection           </div> <div>             Percentage of unchanged files to be re-verified at each backup cycle: <input type="text" value="5.0"/> [0.1 - 100%]           </div> <div>             Percentage of RAM blocks allocated by BackupChain to be verified: <input type="text" value="5.0"/> [0.1 - 100%]           </div> <div> <input checked="" type="checkbox"/> Log files verified successfully           </div>										

Note that backup verification will slow down your backups considerably because the data has to be read back from the target media. In addition, the access reading back will be slower than usual because the Windows disk cache will be turned off for those files and by doing that, several optimizations in Windows that speed up file access will not be available, *when accessing those particular files (this slower access affects only the file being verified and is not system-wide)*.

However, backup verification is crucial when handling critical data. When a file is backed up, its backup file, which may be in a different format than the original file, such as a ZIP archive, is read back and checked. For remote targets, the above option offers a max size limit to prevent downloading very large files for the purpose of verification, as well as a percentage limit. Using the percentage limit, you can limit, for example, verification to just 5% of all new files to keep backups finishing faster.

This percentage limitation makes a lot of sense, especially for very large file server backups and in combination with the second feature “turn on bit rot and manipulation protection”.

### Reverification of backup files

Files at the target may become damaged without your knowledge. Even on RAID controllers utilizing mirror configurations, files and sectors may become corrupt without the controller noticing. RAID controllers usually do not compare sectors while reading between several drives. A hardware fault can hence go undetected for quite some time. In addition, RAM chips can corrupt data. RAM contained in hard drives as well as server RAM, despite ECC technology, can be damaged and the damage can go undetected for quite some time without producing any noticeable symptoms. For example, ECC RAM can be damaged in a way that causes bytes to be written correctly but to the wrong address due to damage in the chip’s internal address bus. The nature of ECC does not offer protection against such and other types of defects. Furthermore, malicious software may encrypt, and sometimes disgruntled employees, may vandalize backup files.

To catch such possibilities within reasonable time and use minimal resources in doing so, BackupChain

offers a percentage based resource coverage option. You can specify to test a *fraction* of RAM used for I/O against RAM defects and a *fraction* of files to be **re-verified**. In case of remote targets, the size options of the upper half of the screen are also taken into consideration when re-verifying.

Re-verifying backup files involves (downloading and) reading back the entire backup file and checking for internal consistency, for example using checksums. This can also be done with previous backup versions of a file that has changed since.

### Coverage of Re-verification

By processing only a fraction of files to be re-verified, *on a per backup cycle basis*, you spread the work over many backup cycles, to keep the amount of additional time required at a minimum. This idea assumes that all files are roughly average size and that the backup task in fact runs periodically. In addition, another assumption is that excessive re-verification of files will not help beyond a certain point but that choice is yours. You can set up tasks to re-verify 100% of all files each time, if you the impact it doesn't prolong the backup cycle too much. The advantage of a 100% reverification is that you will be notified immediately if the quality of your backup media is affected.

If you choose to re-verify, say 5% of files, it will take on average about 20 backup cycles to cover all files once. If the backup task is scheduled to run daily, that would be a 20 day cycle where each and every backup file has been checked again, on average. Whether that's feasible depends on many factors, such as overall backup time available, the total number of files and their size, and access and I/O speeds involved.

### Re-reading files actualizes sectors

A great feature of modern and enterprise grade hard drives, whether used in a RAID or not, is that reading sectors involves many internal checks to occur within the hard drive. In addition to BackupChain checking the consistency of backup files, the hard drive itself re-evaluates the quality of a given sector and may decide to relocate the data on that sector on a spare internal sector if need be.

### Benefits of Verification and Reverification

A lot of users intuitively prefer to keep backup time short as possible, but their underlying notion is often that digital storage is somehow perfect and can't have defects, not even partial defects. In the case of backup verification, prolonging the backup process is unavoidable; however, when data has a very high value for an organization one should consider the benefits and the risks that are being covered.

Let's examine a few potentialities. Hard drives can fail completely or just partially. There is a very wide spectrum of data loss between the time when a hard drive internally detects hardware issues and when it actually reports it to the controller, and then to the OS. Losses can occur before there is a chance for the hard drive to report them.

When files are processed on a server, the data travels through various memory chips. Apart from the main server RAM, some RAM is encapsulated in controllers and hard drives and other equipment. When

a file is loaded and saved, it travels through various RAM cells and chips. If just one of them has a defect, it will corrupt the chunk of data that was carried within it. RAM damage is not as uncommon as widely believed, partly because RAM damage and other forms of bit rot can go undetected for years, unless it is specifically investigated, for example by using RAM checker software. In some “lucky” circumstances, the server might blue screen and spontaneously reboot. Even then, the warning signs of a RAM defect are often overlooked and mistaken for something else, such as a software defect or driver problem. RAM defects are extremely difficult to notice and pinpoint without taking the server offline and specifically investigate for them.

ECC RAM offers some protection against single bit failures, but not all types of RAM damages. As mentioned above, multiple bit failures or damage to the RAM chip’s handling of memory addresses (address bus) can cause damage that is difficult to spot even for many RAM checker software. In data files, these types of RAM damage effects may show up as random characters in random areas of the file, or as missing or overwritten characters. Address bus damage in particular can bypass a range of checks because a valid data word is written to RAM but to the wrong address. There have been numerous reports of such hardware damage from our customers. The common denominator was that many files got corrupted without notice for many months before the issue was even noticed. A RAM defect affecting a centralized file server is especially dramatic since the server handles all files for wide range of users on a daily basis. Every time a file is read or saved and travels through defect RAM, it might get corrupted on the way in or out.

Bit rot occurring inside hard drives can also slip through various checks that are in place in the hardware and software components of a server. But even if a sector is reported as bad by a hard drive, the user will be unaware of the problem until the file is actually being read. I.e. a sector that belongs to a file might go bad but if the file is never read back in full, this will never be noticed. In mirror RAID devices, a corrupted sector will also go unnoticed unless the sector is in fact reported bad by the drive to the controller. If bit rot has occurred inside main server RAM, the file will be corrupted on the way to the drive, unnoticed, unless it is read back and verified.

Reverification, hence, alerts you to the possibility of a hardware fault that would otherwise go undetected. By reverifying, BackupChain causes the file to be read back and this gives hard drives the opportunity to reevaluate the health of each sector the file is stored on. In addition, some of the RAM that is being used in the process is indirectly being checked as well. In some cases, some modern enterprise-grade hard drives are capable to recognizing a frail sector and internally move the sector to a set of spare internal sectors. But this process only occurs if the entire drive is scanned specifically for that purpose or if the file is read back in full.

Ransomware is known to also encrypt backup files. If backups are stored on a vulnerable device or have been somehow affected by an infected device, the fact that the backup files are damaged can potentially go unnoticed for quite some time. For more intensive protection against the special case of ransomware, please contact our support team for additional recommendations.

## The Speed Tab

Many of our customers spent well over \$100,000 on server hardware and hence it is no surprise we have received numerous customer requests to provide more options to allow them to fine-tune backup speed. The speed tab is where most of the speed related options are available.

There is often a need to either limit speed or the inverse, to make full use of all available resources in order to keep the backup cycle as short as possible.

Folders	Files	Exclusions	Backup Target	File Versioning / Cleanup	Deduplication	Schedule	Options	Compression	Verification	Speed
Performance Options / System Stress Prevention										
Backup process priority: <span>Below Normal</span>										
Max. number of CPU cores to use: <span>2</span>										
<input type="checkbox"/> Enable speed limits         Max read speed [kB/sec]: <span>100,000</span> Max write speed [kB/sec]: <span>100,000</span>										
Number of simultaneous file backups: <span>1</span>										
<input checked="" type="checkbox"/> Enable folder cache <input checked="" type="checkbox"/> Enable write cache <input checked="" type="checkbox"/> Enable read-ahead optimization <input type="checkbox"/> Use minimal buffering										
<b>Note:</b> It's not recommended to back up too many files simultaneously; it can actually slow down the entire process if the hardware is not fast enough to perform many tasks in parallel. The usual limitations are number of CPU cores and hard drive speeds. Exception: FTP backups without compression should run in parallel because it tends to be faster for most sites.										

## Specifying Resource Allocation Limits / System Stress Prevention

There are several ways to reduce the usage of system resources, such as RAM and CPU. A lower resource usage usually results in a slower backup process but keeps the system responsive to other services and programs.

The backup process priority controls the priority of the background BackupChain process relative to all other processes on the system, including Windows itself. We recommend using a low setting unless you are running BackupChain at a time where no other service needs to remain responsive.

“Max number of CPU cores to use” limits BackupChain’s CPU usage and also helps saving RAM since only a certain number of workers will be active at a time. Entering all available CPUs leads to full CPU utilization; however, this depends on additional factors, such as the number of simultaneous file backups and the number of deduplication workers used (in Deduplication tab). The limit is automatically lifted if you have parallel file backups or if you use more than one deduplication worker.

“Enable Speed Limits” activates the read and write input/output speed limits. Use these options to limit the transfer speeds to hard drives, FTP, or network shares. This is useful to prevent “clogging” or network and Internet lines, but it also helps reducing the stress on your hard drive.

It is in your best interest to avoid straining your system to prevent system overload and hard drive stress. To keep your system responsive it is recommended to use only a percentage of the actual throughput rates. Most of today’s hard drives can deliver a constant read / write speed of 20 to 50MB/sec with much higher burst rates; however, running a hard drive consistently at fast rates for a long time increases its temperature and decreases its life expectancy.

## Simultaneous File Backups

“Simultaneous file backups” implies that BackupChain can parallelize file backups within a task.

Note, however, it’s strongly recommended not to use this feature unless you know your hardware well and you have selected a specific backup set where it makes sense to use parallelization.

**Note: If you configure a large number of files to be backed up simultaneously the entire process may actually take longer than with sequential backups if it is not configured correctly.** If handling files one by one is in fact using all resources to their maximum throughput, adding additional files in parallel will only make the entire process slower. Parallel backups make sense, for example, if considerable time is spent compressing a file. A second file could run a separate CPU core (in the case of the ZIP format where only one core can be used per file). Or, for example, a second file could be uploaded while the other is still being prepared. Trying to push many files through the same network connection is generally not recommended; an exception is the case where you upload files to a remote WAN server, where each link may be throttled due to external networks and it’s beneficial to use multiple upload streams for better overall throughput.

## Background info on hard drives

Mechanical hard drives are built using rotating disks and heads that move back and forth to read and write data. A modern mechanical hard drive is optimized to give you good average read and write data throughput in terms of streaming, and good burst speeds when small files are read or written.

If the heads need to move a lot, also called ‘seek time’, you will end up with an enormous degradation of performance. Moving a hard drive head is very wasteful and takes a relatively long time of several milliseconds. Note that solid state disks do not use mechanics and hence do not have this disadvantage.

If you back up a lot of files from the same hard drive, chances are the heads will need to move back and forth. If the CPU in the system is the bottleneck and you are using ZIP compression, or if you use a slow

FTP upload link, it may actually make sense to multitask and back up several files at a time. But if the backup target is fast and CPU speed is sufficient as well, the backup will run slower when more than one file is backed up at a time.

All hard drives also have cache space. If you read and/or write many files in parallel the cache is shared and hence its usefulness is minimized. The best hard drive speed is achieved when large files are read and written in long streams with almost no head movement. In that case the cache is also used efficiently as read ahead cache.

### *Ethernet Background Info*

Ethernet networking is actually one of the most inferior designs in networking; yet, it is the most widespread and lowest cost technology.

The key thing to know about Ethernet is that its performance is reduced exponentially when more than one node on the bus starts transmitting. Packets collide and lead to long delays each time an additional node wants to 'speak into the wire'.

If your backups are taken from a network server or they are being sent to a network device you need to understand that the backup traffic will most likely max out all available network bandwidth. For that reason we offer a Speed Limit for Read Speed and Write Speed. You may have to limit the backup speeds to match a fraction of your network speed, in order to ensure the network remains operational to other computers on the network.

The above may also become extremely critical in a cluster shared volumes environment or failover cluster setting.

In a network setting you probably would not want simultaneous backups at all.

### *When to use Simultaneous Backups*

The short answer is: if the hard drive or network is NOT the bottleneck.

If your CPU is relatively slow but the hard drives are very fast, as the case with many servers that are optimized for data transfer rather than computations, it makes sense to use more than one backup in parallel.

Note that BackupChain's deduplication algorithm parallelizes on its own (you can specify more than one deduplication worker in the Deduplication tab). So usually there is no need to run several deduplications simultaneously.

Obviously simultaneous backups make sense when many CPU cores are available and idle. In case of virtual machine backups, chances are you are using deduplication. Then it would most likely be better to do sequential file backups and increase the number of deduplication workers.

Another typical example is FTP. If your FTP target uses load balancing and severely limits upload bandwidth per link, you could bypass that by uploading several files at a time.

Another typical parallelization example is ZIP. ZIP, by its nature, cannot be parallelized. So if your hard drives are really fast but one single CPU core is relatively slow (this is the case with almost all multi core server CPU systems) it also makes sense to back up several files at a time.

### *Folder Caches, Read-ahead, and Buffering Options*

The speed tab also offers options to enable folder cache, write cache, read-head optimizations, and the option to keep buffer to minimal size.

As with all algorithms, there are pros and cons and it happens as a consequence of the nature of an algorithm that in certain environments it does not perform well. A cache works miracles with cache hits occur often and a cache miss is rare, but these events greatly depend on the data being backed up and the server environment and hardware.

Most users will not need to alter these settings; however, there are certain scenarios where performance can be improved by changing the configuration.

#### *Enable Folder Cache*

This option minimizes the lookup of files through internal caches. If you use remote backups (FTP) that do not use a BackupChain FTP Server with remote scan capability, you will want to switch this option off.

BackupChain FTP Servers with remote scan capability use a database of all server-side files that is sent down to the client. This one time operation eliminates all file lookups thereafter and significantly reduces backup time when large file servers are being backed up. As other FTP server products do not offer such a feature, you will want to turn it off if you do not use a BackupChain FTP server.

#### *Write cache & read-ahead optimization*

Microsoft Windows includes some clever algorithms to cache file access and I/O in general, and most of the time these algorithms produce good results. There are some specific use-cases that result in bad performance and even make the system unstable, such as when Windows runs out of memory due to a bug in the caching algorithm. To our knowledge these bugs in Windows persisted at least until Windows

Server 2016. To address these rare issues in Windows you can turn off write cache and read-ahead optimization. Note that in general you will want to keep these switched on for better performance.

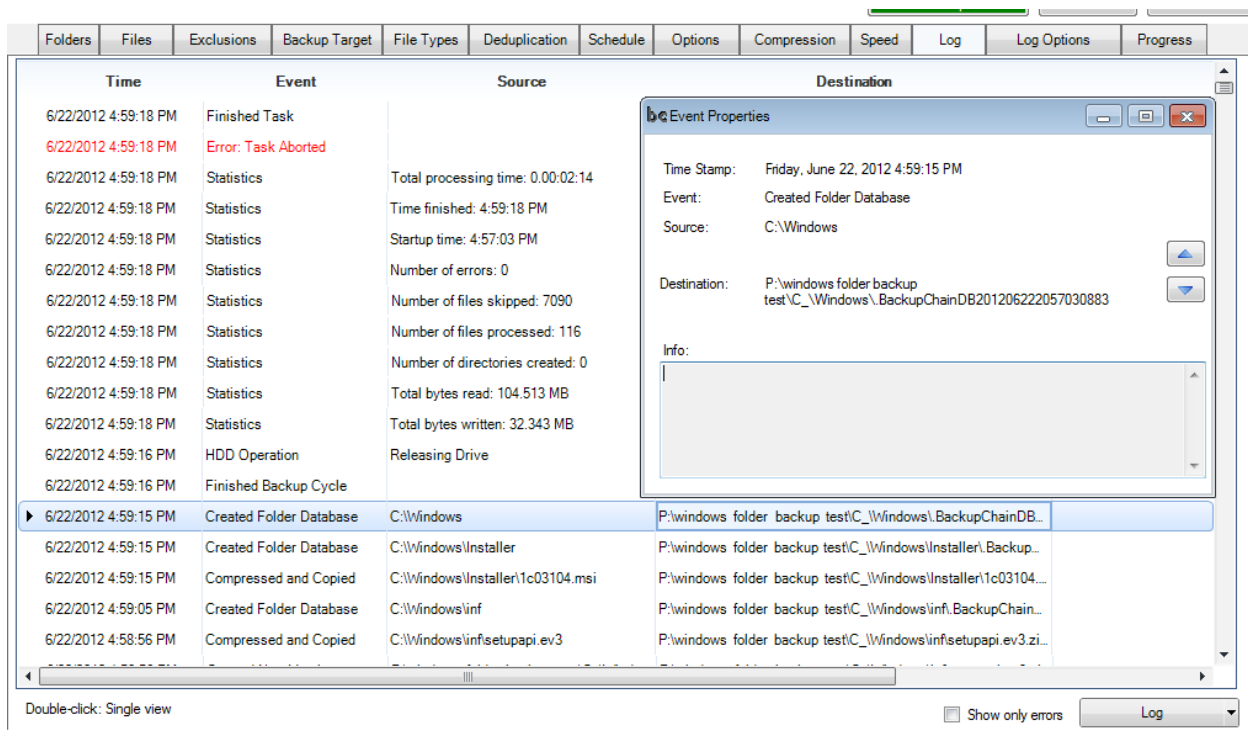
### *Minimal buffering*

Faster I/O benefits from larger buffers; however, some servers are to run with limited RAM resources. In those scenarios you will want to enable minimal buffering to reduce RAM consumption and peaks, at the potential cost of some performance degradation.

## The BackupChain Log

BackupChain's log keeps a record of all files processed and displays several statistics and summaries at the end of each backup task cycle.

The default log settings (see Log Options tab) prevent an unnecessary accumulation of log entries; however, if you want all files to be recorded (included skipped files) you can change the log settings in the Log Options screen.



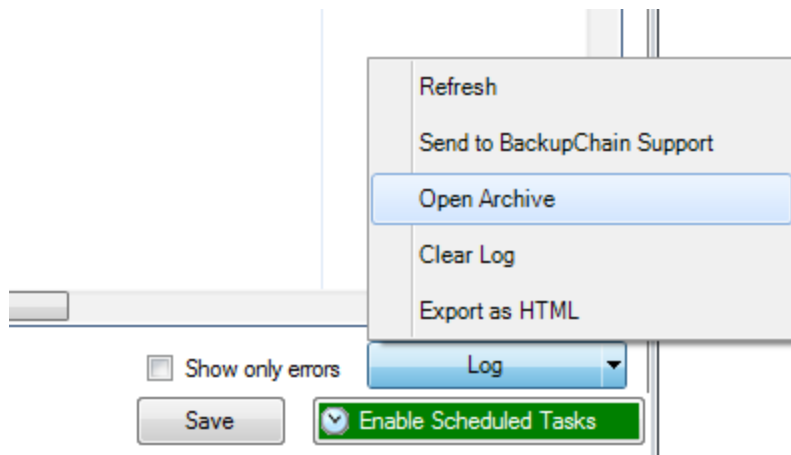
The log view is color coded. Errors appear in red.

Double clicking on a line opens the Event Properties as shown in the smaller popup window above.

At the bottom right you can click 'show only errors' to filter out all regular entries and show only failed operations.

The time column shows the time local to the viewing machine. If you are using a master console that connects to a remote server, which is in different time zone, the time column will show the time in your local time, not that of the remote server.

The Log button offers several additional functions:



Export as HTML, Clear Log, Open Archive, Send to BackupChain Support, and Refresh.

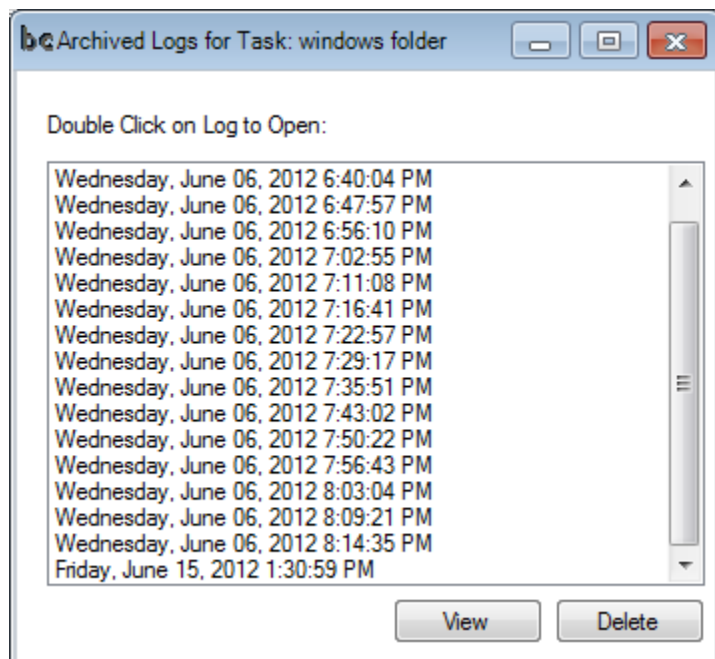
### Export Log as HTML

Logs may be exported as HTML files. HTML logs are color coded as well and open in a new Internet browser window.

### Log Archive

The size of the log archive is configurable in the Log Options tab.

Every time a log gets too large, it's archived and compressed. By using the Open Archive function, you can open older logs and browse through them:



After clicking View, a new Log Viewer will be opened with the same functionality as the Log tab (color coding, HTML export, etc).

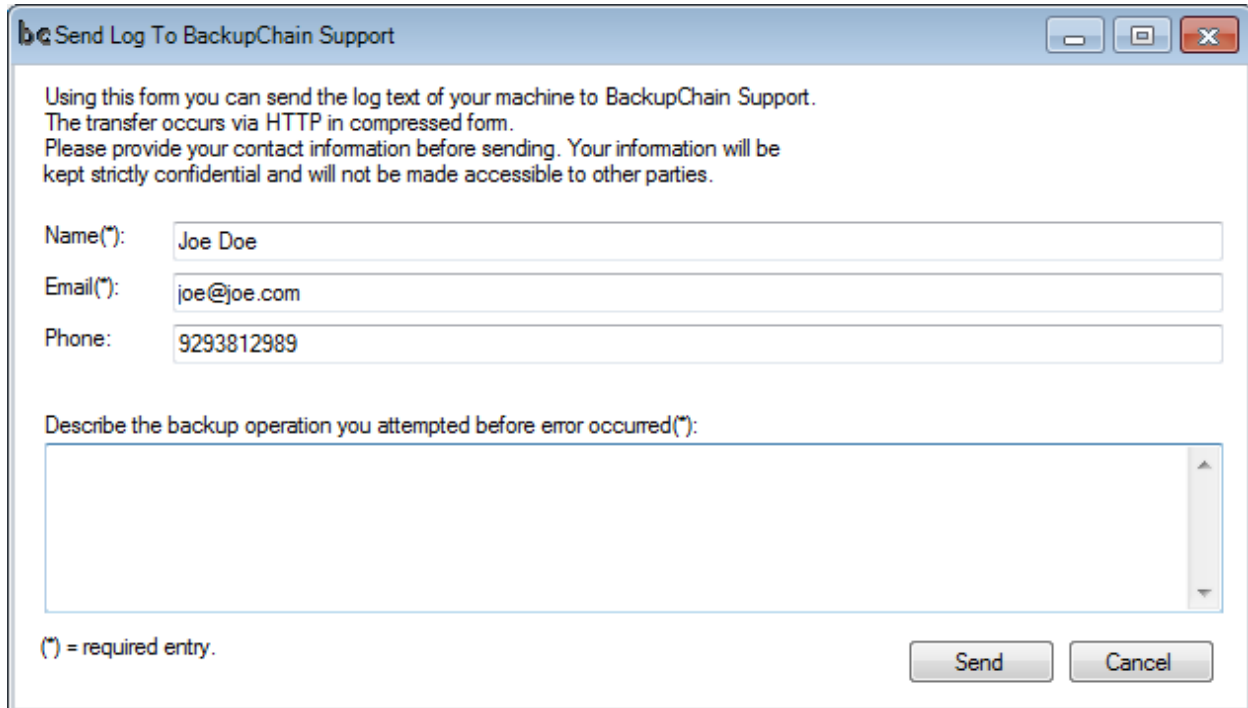
### Skipped Files (Files Already Backed Up)

By default, BackupChain skips files that have been processed in a previous cycle. Files are skipped if their time stamp or size has not changed since the last run.

The default logging options prevent skipped files from being logged. This prevents lengthy log files for users with hundreds of thousands or even millions of files. If logging skipped files is feasible in your setting you can switch it on in the Log Options screen.

### Sending Your Log File to BackupChain Support

To offer you better technical support, you can send your logs to the BackupChain support team where it will be analyzed for you in case you experience difficulties with your backup. Simply click “Send to BackupChain Support”, enter your name and details and provide a short description of the problem.



**bc Send Log To BackupChain Support**

Using this form you can send the log text of your machine to BackupChain Support.  
The transfer occurs via HTTP in compressed form.  
Please provide your contact information before sending. Your information will be kept strictly confidential and will not be made accessible to other parties.

Name(\*):

Email(\*):

Phone:

Describe the backup operation you attempted before error occurred(\*):

(\*) = required entry.

### Log Archiving

BackupChain automatically compresses and archives log files when they reach 10 MB. Then, the log files are kept in an archive folder until the archive reaches a certain limit (100 MB default, the setting may be changed in the Log Options screen).

The location of log files is C:\ProgramData\BackupChainService\logs\<task name>

As in: C:\ProgramData\BackupChainService\logs\Important File Backup

On system running XP or Windows Server 2003:

C:\Documents and Settings\All Users\Application Data\BackupChainService\logs\<task name>

As in C:\Documents and Settings\All Users\Application Data\BackupChainService\logs\Important Backup

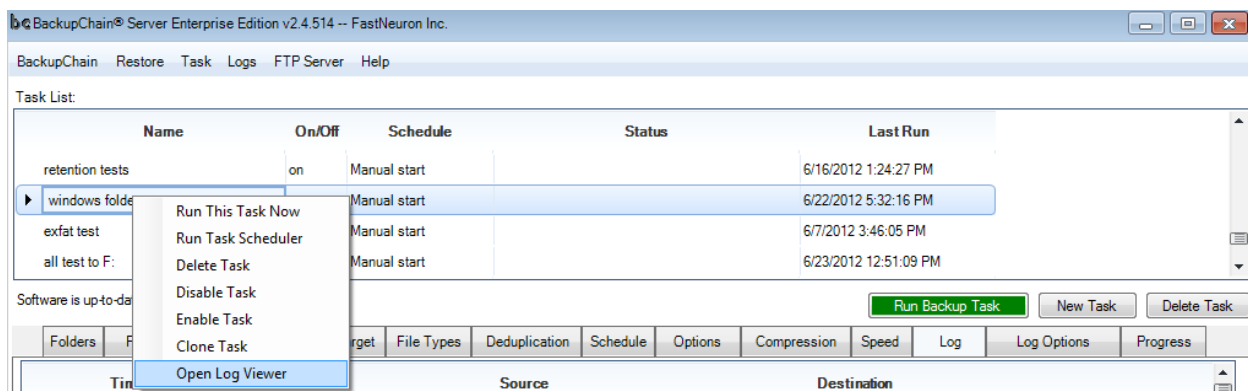
Use the Open Archive button to open, view, and delete older log lists.

## Clearing and Refreshing the Log

In case you wish to track log entries as they occur, hit the Log tab or click “Refresh” at the bottom.

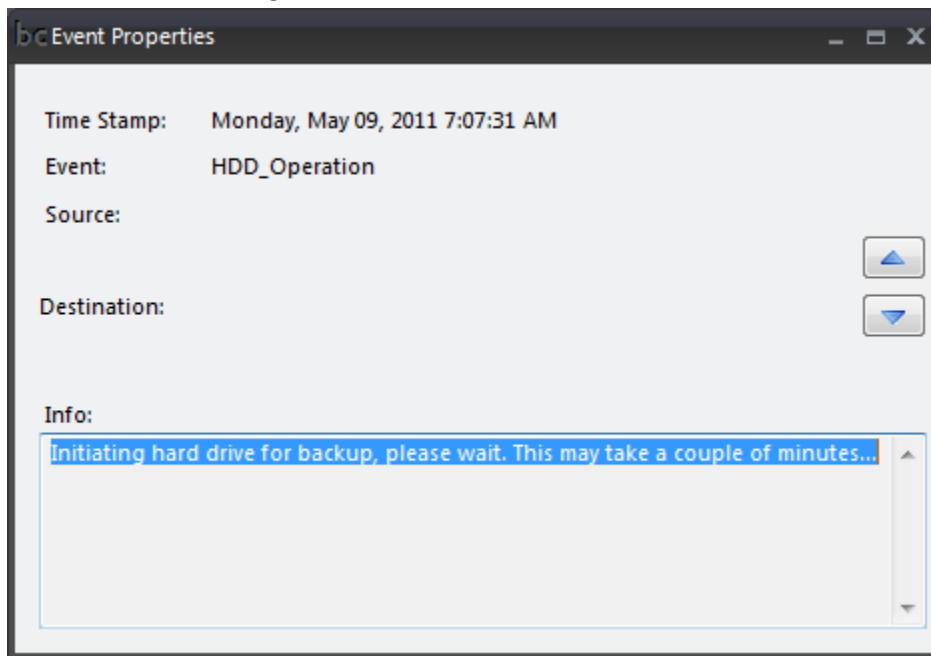
## Opening the Log in a Separate Window

You can also right-click on the task’s main line and select Open Log Viewer, in order to open the log in its own separate window:



## Opening a Single Event in Log

Sometimes there isn't enough space to read a long log entry, especially when path names are very long. You can double-click on a log entry to view it separately. Note that you can navigate to the next entry above and below using the two arrows.



## Log Options

Use the Log Options tab to set up your email notification and other log features:

Log Options tab settings:

- Email server settings:**
  - SMTP server host name: smtp.myemailserver.com
  - SMTP server port: 25
  - Send to email address(es): myself@mydomain.com
  - Subject line: BackupChain Alert
  - Sender's email address: myself@mydomain.com
  - Password: [masked]
  - User name: myself
  - Confirm password: [masked]
  - ☒ My SMTP server requires login/password
  - ☐ Use SSL (=STARTTLS. Ensure port number is correct when using this option)
  - Send Test Email
- Notification settings:**
  - ☒ Send an email when this task starts
  - ☒ Send an email when this task completes
  - ☒ Send an email with the log when errors occur
  - ☐ Send an email with the log when files have been backed up
  - ☒ Log files processed successfully
  - Max. Archive Size[MB]: 100
- HTML Email Format Configuration:**
  - ☒ Use this HTML template for task start notifications: C:\Program Files\FastNeuron Inc\BackupChain [Browse]
  - ☒ Use this HTML template for successful logs: C:\Program Files\FastNeuron Inc\BackupChain [Browse]
  - ☒ Use this HTML template for logs with warnings: C:\Program Files\FastNeuron Inc\BackupChain [Browse]
  - ☒ Use this HTML template for logs with errors: C:\Program Files\FastNeuron Inc\BackupChain [Browse]

Buttons: Save, Enable Scheduled Tasks

**Note:** Your Internet Service Provider (ISP) may be blocking port 25 for SMTP access. Usually such ISPs provide their own SMTP services that you need to use. Alternatively, your email provider may offer an alternative port number, other than 25. For Verizon, for example, use outgoing.verizon.net and port 587 instead of your email provider's address.

You may want to switch off "Log files processed successfully" if you have an unusually high number of files to back up.

### Customizable HTML Email Alerts

The bottom half of the Log Options screen offers a selection of cases where you may want to switch on HTML email alerts. The path to the HTML templates is the program path of BackupChain as shown above C:\Program Files\FastNeuron Inc\BackupChain

You can copy the template to another folder and edit and design it as you like.

You can design the HTML code as you like. BackupChain will insert information as using the following tags:

###TASK NAME###	The name of the task as entered in BackupChain
###NUMBER OF ERRORS###	The number of errors that occurred. Example: 0
###NUMBER OF WARNINGS###	The number of warnings. Example: 1
###NUMBER OF CYCLES###	The number of times the task ran if scheduled to run continuously.
###NUMBER OF DIRS CREATED###	The number of directories created in this cycle
###NUMBER OF DIRS SKIPPED###	The number of pre-existing directories.
###NUMBER OF FILES PROCESSED###	The number of files created in this backup cycle.
###NUMBER OF FILES SKIPPED###	The number of pre-existing, unchanged files.
###TASK CYCLE STARTUP TIME###	The time when the backup <i>cycle</i> started.
###TASK CYCLE FINISH TIME###	The time when the cycle ended
###BYTES READ###	The total amount of bytes read in fractions of the nearest unit. Example: 1.5 TB, or 129 MB
###BYTES WRITTEN###	The total amount of bytes written in fractions of the nearest unit. Example: 1.5 TB, or 129 MB
###LOG ROWS###	All log entries as stored in the current log file in HTML table format "<tr><td></td></tr>" ...

The easiest way to understand how the HTML customization works is to have a look at the contents of one of the HTML template files.

The above tag names are simply replaced with the actual text value. The exception is **###LOG ROWS###** where the log entries are written as table rows using the HTML <tr><td></td></tr> tags and it is assumed that you have surrounding table tags. The advantage of this method is you can customize the table and its headers and footers as you like.

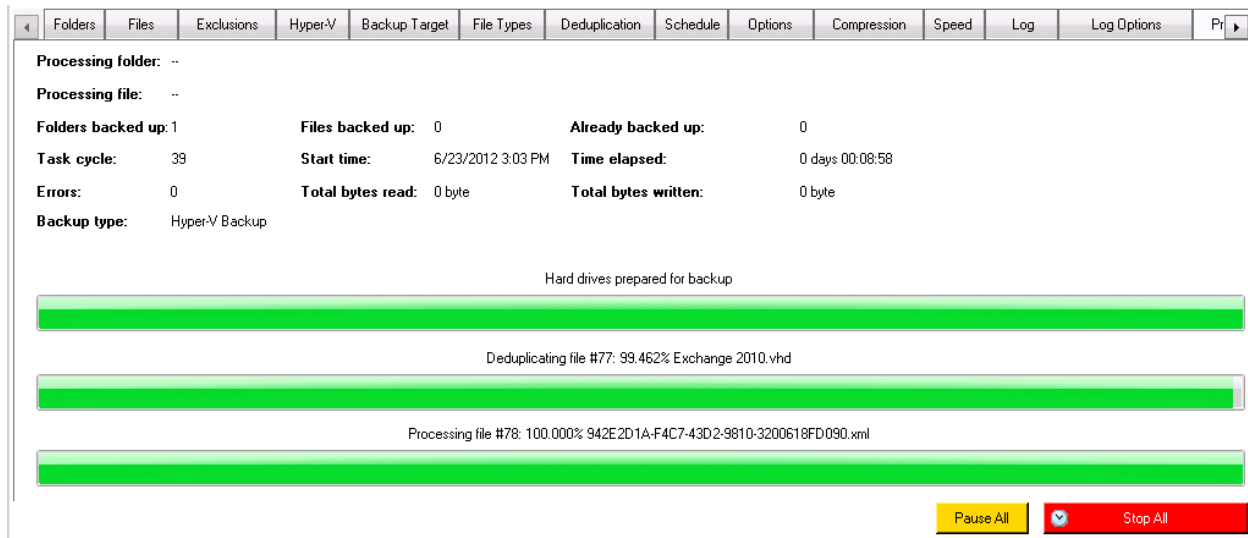
Note that the HTML log is also color coded using CSS styles encapsulated in the template file. The default HTML email alert looks similar to the one below:

BackupChain® Backup Software for IT Professionals		
Task personal files backup failed with 1 error(s)!		
Errors:		1
Warnings:		0
Cycles:		1
Folders created:		0
Folders already backed up:		0
Files created:		9
Files already backed up:		144861
Cycle startup time:		Saturday, June 23, 2012 10:31:41 AM
Cycle finish time:		Saturday, June 23, 2012 10:46:13 AM
Log Contents:		
6/23/2012	Startup	v2.4.514
10:31 AM		

## Progress Indication

You can check on the backup task by opening the Progress tab or by periodically refreshing the Log view, as discussed in earlier sections.

The Progress tab shows various counters and statistics:

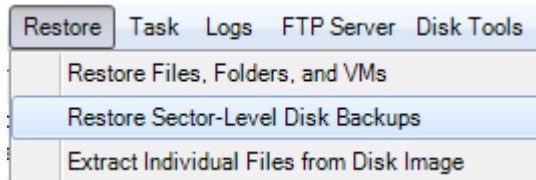


## Restoring Disk Images to Physical Disks

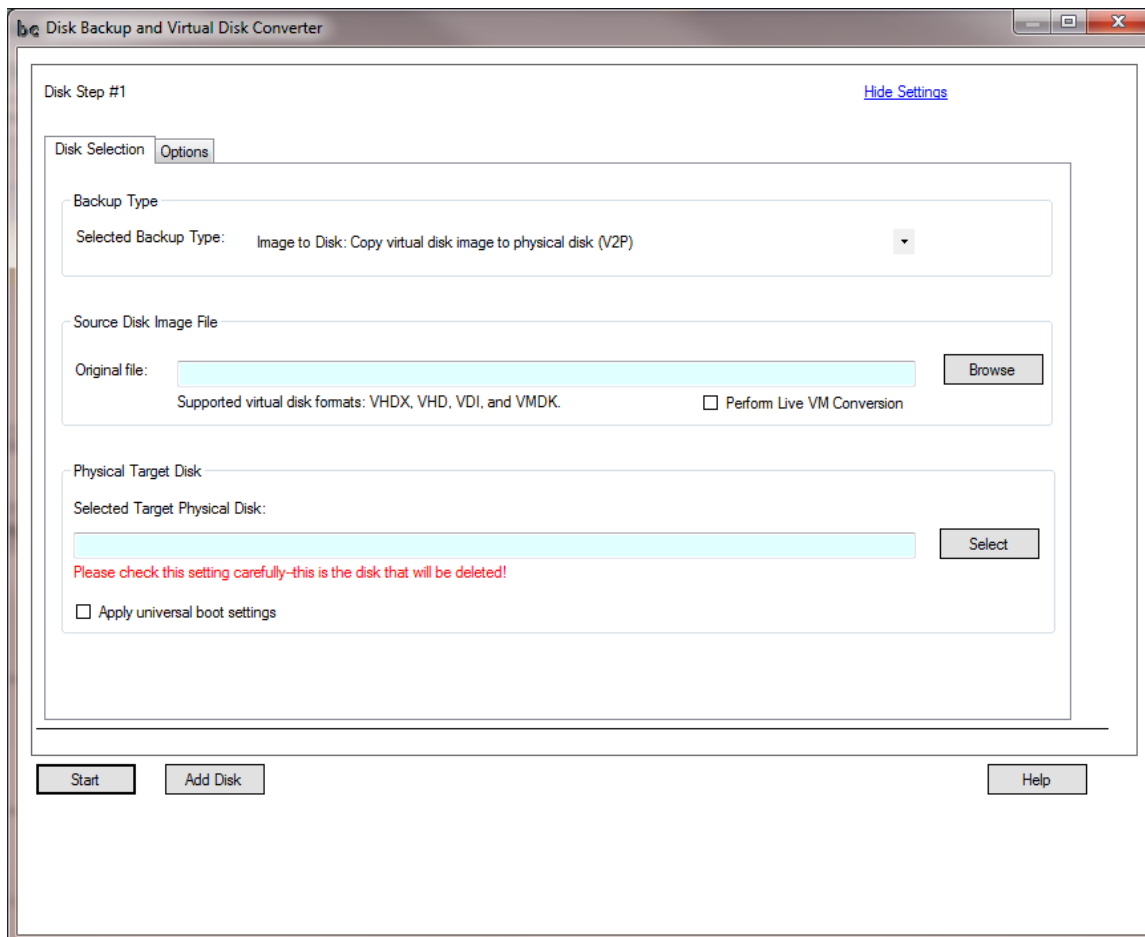
See page 21 for disk related information.

The general procedure is shown below. Note that it is also possible to set up a task to perform the same steps. The steps below show how to restore disk images to a physical disk as a once-off restore process.

Select Restore from the main menu, then Restore Sector-Level Disk Backups.



In the next screen, all you need to do is select the disk image file by clicking Browse, and then selecting the target disk by clicking Select:



Click “Start” to start the recovery process. If you want to restore several disk images to several disks at the same time, you can add additional steps to the process by clicking “Add Disk” before starting the process. The screen will then contain another section for the second disk, where you select the disk image and its respective physical disk target.

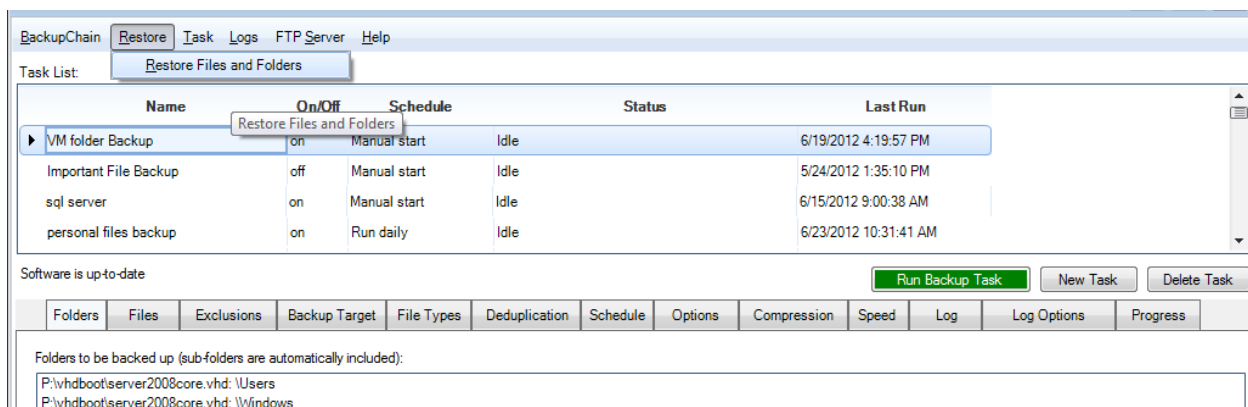
The option “Perform live VM conversion” is a special function that allows you to use a virtual disk while the VM is running and copy the contents of that disk to a physical disk. The VM can run during the process and is not affected in any way. If you choose to convert a VM’s virtual disk to a physical computer (V2P conversion), you should also enable the option “Apply universal boot settings”, which causes BC to modify the Windows boot settings in a way that will help adapt to the new hardware where you will install and boot the physical target disk.

## Restoring Files

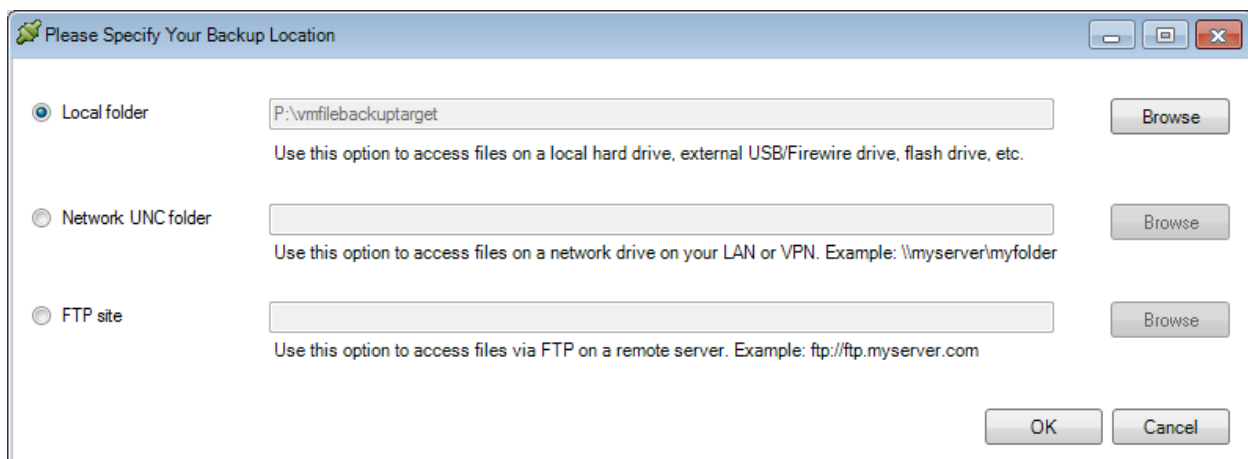
You can access backed up files directly from the backup folder if the files are in a standard format, such as ZIP, or in their plain original file formats. All files of all types may also be restored using BackupChain's restore function.

Optional: Select the backup task from the Backup Task List.

Select Restore from the main menu and proceed with Restore Files and Folders:

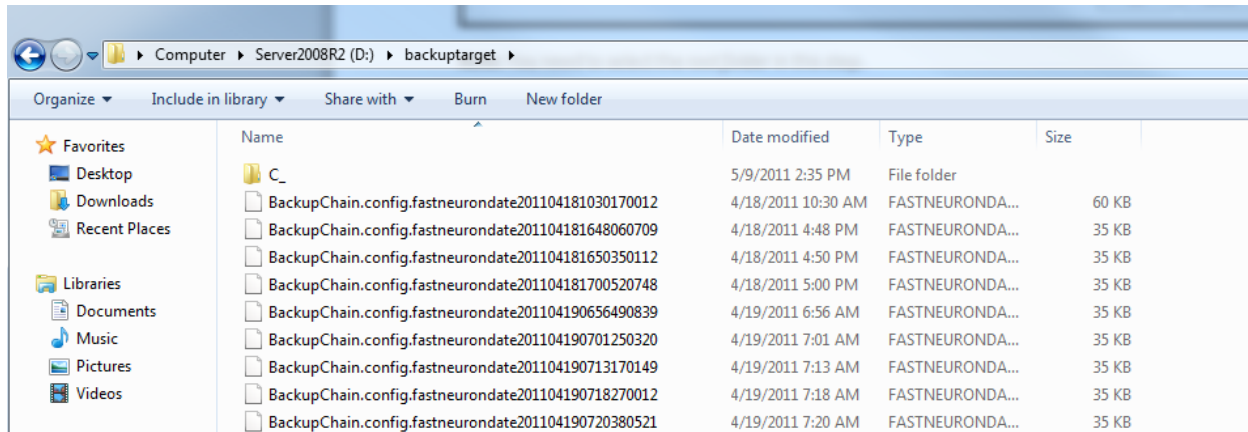


Then you need to fill in the details about the backup location. This information is usually preset with the task settings:



**Note:** You need to select the *root folder* in this step.

If you open the folder in Windows Explorer, the root folder may look like this:

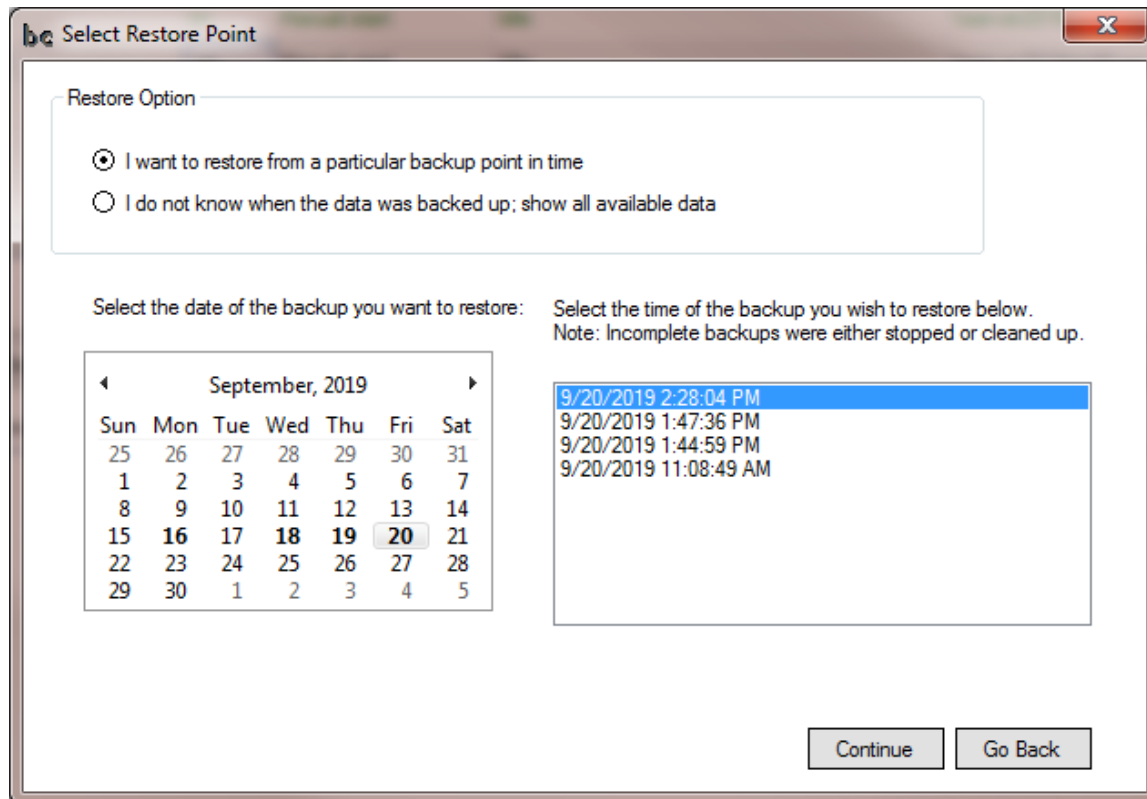


Notice the C\_ folder (for C: drive) and the BackupChain.config files. These files are necessary for restore operations.

Once you confirm the backup folder location, the backup set selection screen will open:

## Selecting a Backup Set

BackupChain can restore a file/folder structure as it was at the time of backup, that is, it will restore only files that existed at the time of backup and restore the version of the file as it existed at the time of backup. Folders will be restored following the same principle.



Similar to above, you will be presented with a calendar view. Today's date is shown in a color coded (blue) box. In the example above we see backups are available for the 16<sup>th</sup>, 18<sup>th</sup>, 19<sup>th</sup>, and 20<sup>th</sup> (bold). When we select the 20<sup>th</sup> (the most recent day is automatically preselected) BackupChain opens a list of backups to select from. On the 20<sup>th</sup>, there are several backups, the latest was taken at 2:28:04 PM.

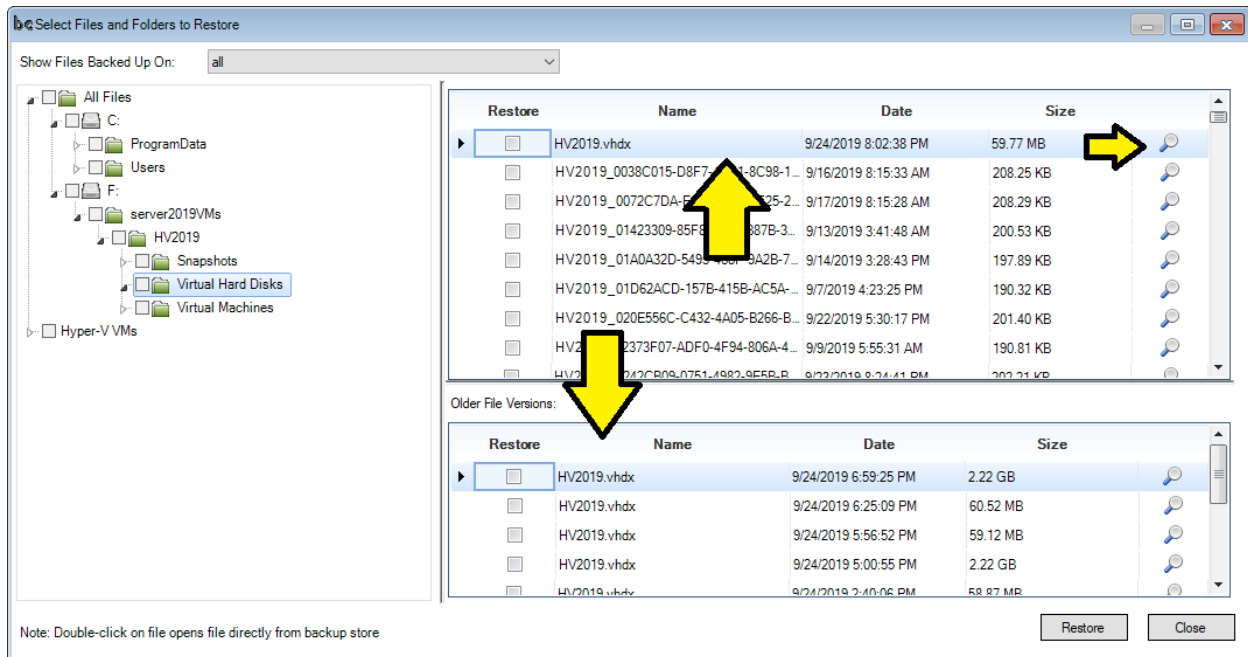
**Note:** If we click **Go Back** now, BackupChain returns to the previous screen where the backup folder selection was made.

Choosing "I do not know when the data was backed up; show all data" will remove the calendar and present the cumulative view of all backup sets available in the backup store. This means that we won't be able to restore the exact file/folder structure at a given time, but we can restore any file and folder and any file version we want.

This is useful when we don't know for sure when a file or folder was deleted or backed up.

## Restore Screen

Next, when you enter the Restore Screen, you open the folder structure to the left and navigate to the path you would like to restore:



To restore *an entire folder*, check the box in the tree to the left *only*. For example, you could select the node “HV2019” to obtain the *latest version* of each file in the folder. The latest version depends on the Restore Point filter at the top of the restore screen.

To restore a single file, click on the folder and you will see a file list to the right. At the top of our example is a file dated 9/25/2019 8:02:38 PM. Notice that as soon as you select a file at the top, the bottom half of the screen splits, and you receive a list with older versions of the same file appearing in reverse order, the newer ones at the top.

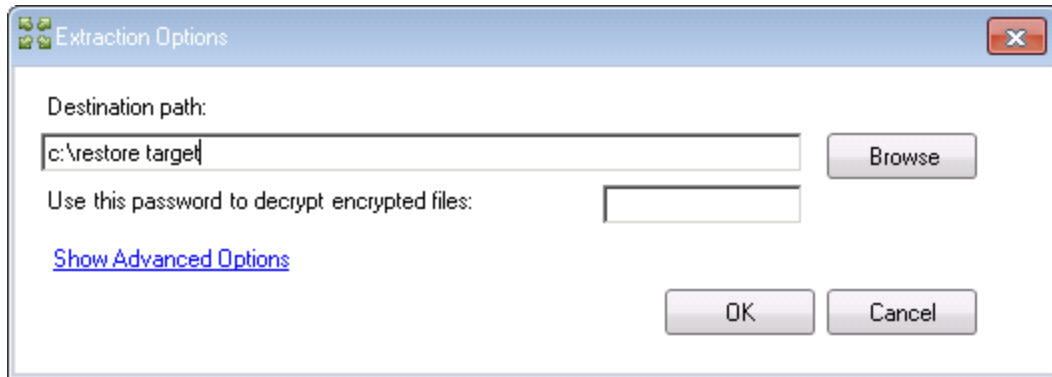
**Important:** If you want the latest file select the file at the top, by clicking the Restore box left of the file. Do not select the folder. To restore an older file version, select a file from the bottom list and check the Restore box, see example above. Do not select the file at the top half of the screen.

**Hint:** The entire screen and all three panels are resizable.

**Hint:** Use the date filter at the top to select a particular backup set or point in time.

Double-clicking on a file or clicking on the magnifying glass at the right of a file will open the Granular Restore option if it is a virtual machine disk and you have BackupChain Server Enterprise Edition installed, or it will selectively open and restore the selected individual file only. More information on Granular Restore may be found in the next sections that follow.

To proceed with the file restore click the Restore button at the bottom of the screen:



The Extraction Options Screen appears where you can enter a destination path. You may also enter a UNC network path as target. Note that the BackupChain's Monitor application runs with your own user credentials and in your user session; hence, you may also use mapped drives and other network shares that you normally access.

## Advanced Extraction Options

Select "Show Advanced Options" to change advanced extraction options, for example to enable restoring ACLs:

**Extraction Options**

Destination path:

Use this password to decrypt encrypted files:

Confirm password:

[Hide advanced options](#)

**Update Settings**

☐ Extract all files and replace if they already exist  
☒ Extract only new files and new versions of existing files.  
☐ Extract only new versions of existing files. Other files will not be restored.

**File Retention Settings**

☒ Ask before overwrite      ☐ Skip existing files  
☐ Overwrite without prompt      ☐ Rename old file when there is a name conflict

**Miscellaneous Settings**

☐ Extract all files into the same destination folder (don't build folder tree)  
☐ Restore files to their original location (ignore destination path specified above)

Folder for temporary files:

☐ Restore Directory ACLs      ☐ Restore File ACLs  
☒ Do not stop if disk read errors are encountered  
☐ Verbose logging

“Update Settings” controls how the files are to be restored. You have the option to overwrite all existing files without warning, extract only new files or new versions of existing files, or only new versions of existing files (refresh).

The section “File Retention Settings” determines what to do when a name clash occurs. The default is to ask before overwriting but you may also chose skipping files or automatic renaming.

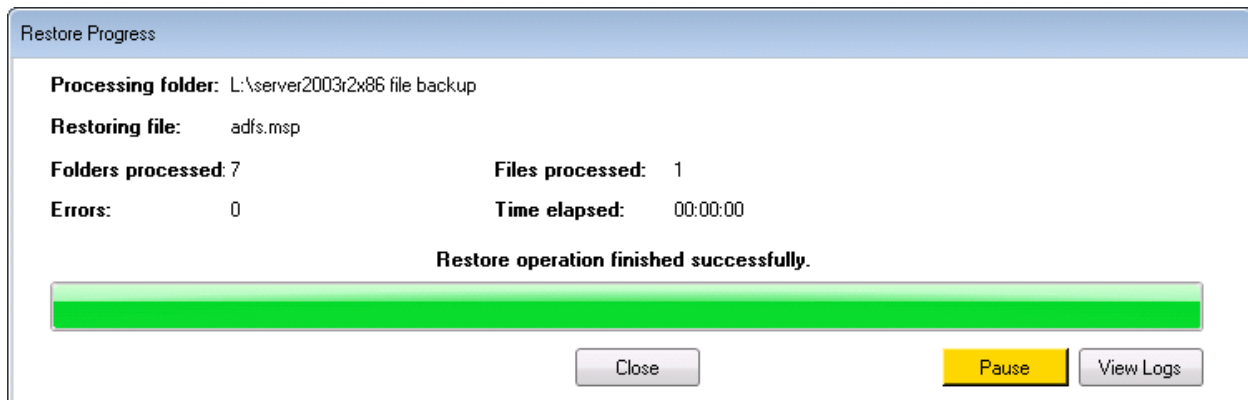
The section “Miscellaneous Settings” contains three options:

1. The option “Don’t build folder tree” restores all files into a single folder.

2. Restore files to original location will use the folder information from the backup store to put the files back to the same original folder.
3. Password for decryption: Enter here the exact same password as entered in the backup task.
4. Temporary files folder: When restoring deduplicated files, BackupChain needs space for temporary files. Especially when you work with very large files you may need to provide a temporary file folder on a different (and faster) drive, if C: doesn't have enough space left.
5. Restore ACL for directories and files restores the access control lists for each file and folder.  
Note this is only available if both file source and destination is NTFS.

## Restore Progress

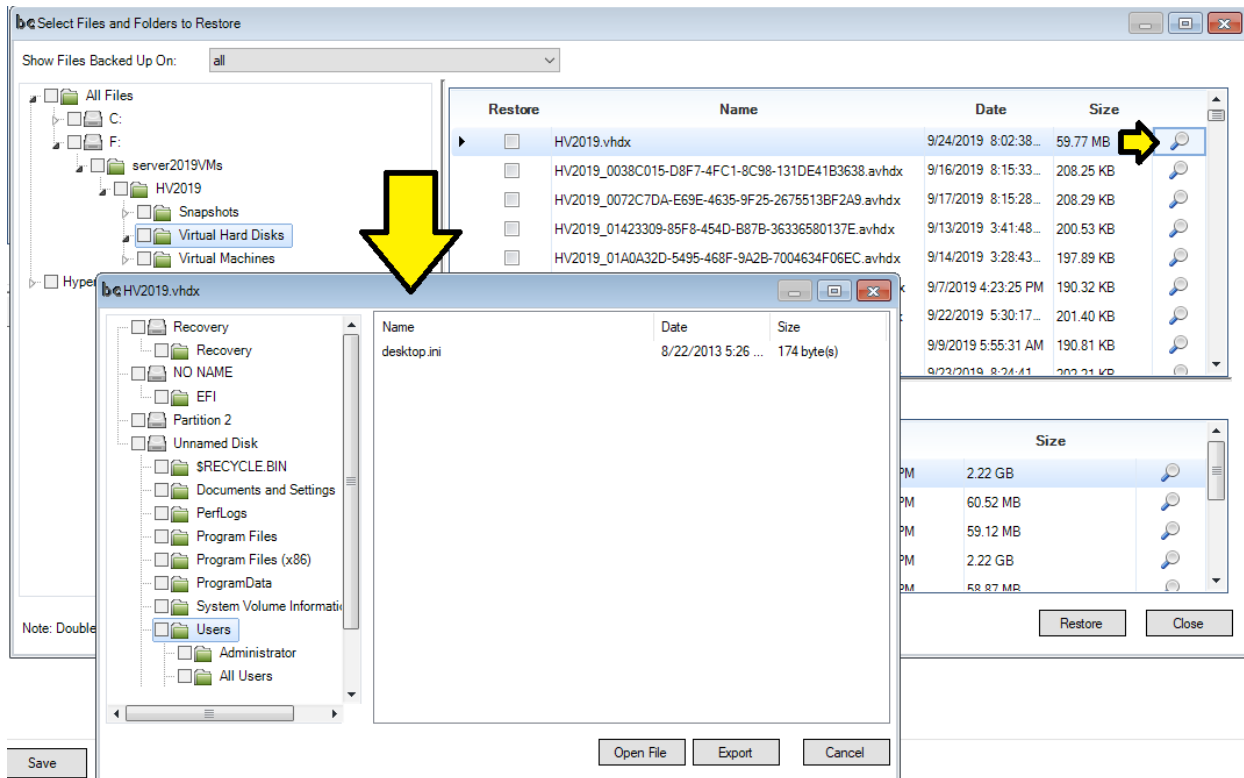
When you proceed with the restore operation, the restore progress screen opens:



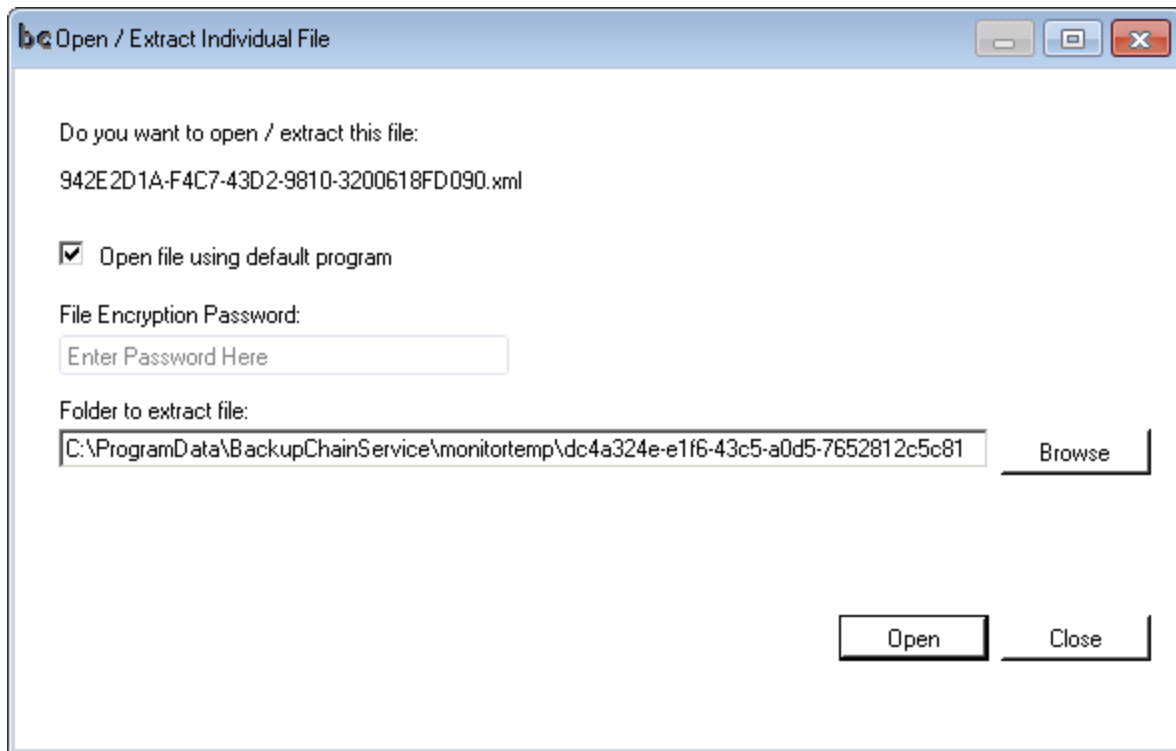
In case of an error, check the logs via the View Logs screen for more information. The log viewer will open where you can export as HTML, amongst other options.

## Restoring a Single File

If you want to restore a single file from a backup folder, simply double click on the file or click on the magnifying glass. Note: If you are using BackupChain Server Enterprise Edition and you select a virtual disk file (\*.VDI, \*.VMDK, \*.VHD, \*.VHDX) you can open the Granular Restore option and restore individual files and folders from inside a deduplicated or plain file virtual machine backup.



Once you click on the file you will see older file versions at the bottom half of the screen. In order to directly open one of those files, double click either on the latest version (above) or one of the older versions (list below). Instead of double-clicking you could also click the magnifying glass. For virtual disks, the screen above opens and you can pull out files and folders from the VHD without having to restore the entire VHD. For all other files that aren't virtual disks, the following screen opens:



If you are dealing with an encrypted file you need to enter the password now. As you can see above, BackupChain uses a temporary folder on the system drive to restore the file. However, this may not be convenient for very large files. In those cases you may want to change the folder before clicking Open.

The option "open file using default program" can be unchecked so you can access the file directly from disk with any tool you like; otherwise, the default program registered with the file type will be called to open the file.

## Tutorials

In this section we present a couple of helpful tutorials for common backup scenarios.

### How to Set Up Sector-Level Disk Backups

Entire disks (physical or virtual) can be copied to one another using BackupChain. A “classic” disk backup uses a proprietary container file format; however, in BackupChain you can back up a physical hard drive to an open-standard virtual disk for the purposes of backup, for example, you could back up your system drive to a VHD or VHDX.

Later when disaster strikes and you need to restore, simply use BackupChain’s disk converter to copy the VHD back to a physical disk.

Alternatively, BackupChain also offers live disk to disk backup between physical disks. You could set up a schedule and have BackupChain copy from one disk to the other every night. In case you ever need to “go back”, all you need to do is detach the original disk and perhaps check your boot settings to ensure your PC/server will boot from the other disk. If you accidentally deleted files on the source disk, the previous night’s data is immediately available on the backup disk you have.

In the special case of VHD and VHDX formats you can also add the VHD to the Windows Boot Manager and directly boot from it. This way you don’t have to copy the VHD back to a physical disk.

There are many options to manage each type of possible disaster using BackupChain. Disk backup comes handy when you need to protect system disks; however, file backup is also very useful and often more efficient than disk backup when you want to protect file server data.

Please refer to the section Sector-Level Disk Backup Strategies and Creating a New Disk Backup Task for detailed how-to information.

### How to Convert a Physical Machine to a Virtual Machine (P2V)

To convert a physical server to a virtual machine you can either create a new disk backup task (see page 29) or use the Disk Converter tool (Main menu -> Disk Tools->Disk Backup & Disk Converter).

For each physical disk you need to convert, you would enter the following conversion steps. In the example below we have only one disk, which is disk #3 and holds drive letters Z:, F:, J:, D:, and V: with an overall capacity of 7.28 TB:

Disks	Imaging Options	Schedule	Options	Speed	Log	Log Options	Notes	Progress
<div> <div>Disk Step #1</div> <div>           Operation: Disk to Image            Source: Disk #3: 7.28 TB (Z:\, F:\, J:\, D:\, V:\), GPT, EFI(Boot...            Destination: W:\temp\disk_4.vhdx         </div> <div> <a href="#">Edit Settings</a> </div> </div>								
<div> <div>Add Disk</div> <div>Help</div> </div>								

Click 'edit settings' to see the detailed settings for that backup step:

Disks	Imaging Options	Schedule	Options	Speed	Log	Log Options	Notes	Progress
<div> <div>Disk Step #1</div> <div> <a href="#">Hide Settings</a> </div> </div>								
<div> <div>Disk Selection</div> <div>Options</div> </div>								
<div> <div>Backup Type</div> <div>           Selected Backup Type: Disk to Image: Copy physical disk to virtual disk image (P2V)         </div> </div>								
<div> <div>Source Disk</div> <div>           Selected Source Physical Disk:            Disk #3: 7.28 TB (Z:\, F:\, J:\, D:\, V:\), GPT, EFI(Boot), Model: ST8000NM0055-1RM112 ATA Device, Serial: AZ41H97M           <div>Select</div> </div> </div>								
<div> <div>Target Disk Image File</div> <div>           Target File: W:\temp\disk_4.vhdx           <div>Browse</div> </div> </div>								
<div> <div>Virtual Disk Format</div> <div> <input type="radio"/> VHD (≤ 2TB)           <input checked="" type="radio"/> VHDX (≤ 64TB)           <input type="radio"/> VMDK (≤ 2TB)           <input type="radio"/> VDI (≤ 2TB)         </div> </div>								
<div> <div>Virtual Disk Type</div> <div> <input type="radio"/> Same as Original           <input type="radio"/> Pre-allocated, Fixed Size           <input type="radio"/> Pre-allocated, Sparse           <input checked="" type="radio"/> Dynamically Expanding         </div> </div>								
<div> <input type="checkbox"/> Apply universal boot settings         </div>								

To get to the above screen, either open the Disk Backup & Disk Converter from the main menu, or click “New Task” and create a new sector-level disk backup task. Then select “source is a physical disk” as shown above and click the “select” button to view all available disks.

**Note:** Dynamic disks must be converted all combined in one step by adding additional disks to the above screen using the Add Disk button. Dynamic disks in Windows (not to be confused with expanding virtual disks, see <https://technet.microsoft.com/en-us/library/cc737048> for a definition) allow spanned, striped, and mirrored volumes that may span several disks. If you want these disks imaged you must select all of them to be converted simultaneously. You can add additional conversion steps (i.e. disks) by clicking the “Add Disk” button.

Note there are three basic settings to be filled out in the above screen:

1. Backup type: in this case “Disk to Image”
2. The source disk: “disk #3”
3. The target image file: “W:\temp\disk\_4.vhdx”

The above example converts the physical disk to a disk image file “disk\_4.vhdx”. The VHDX virtual disk format can grow up to 64 TB, whereas all other formats are limited to about 2 TB. Depending on your virtualization platform of choice you may want to choose:

VHD	Windows Server 2008 or Windows 7 and later Example: Hyper-V or Virtual PC
VHDX	Windows Server 2012 or Windows 8 and later Hyper-V
VMDK	VMware Workstation, Server, ESX, ESXi
VDI	VirtualBox

Note that some later versions of VirtualBox and VMware may be able to use VHDs as well.

If you are backing up the disk for the purposes of disaster recovery, as long as the disk is under 2TB you could use any format. Performance is best with the VHDX format, however.

The virtual disk type is preset to “dynamically expanding” which means the virtual disk will grow to accommodate all data on the original drive and will use only as much storage as necessary to hold all information.

The tab “Options” provides additional functions to fine-tune your disk backup.

“Prepare all services for backup” provides application consistency by notifying all VSS aware services to prepare for live backup. Use this option especially when you have Microsoft SQL Server, Exchange Server, Oracle (VSS aware versions), and other VSS aware services running.

“Skip disk space marked as free” instructs BackupChain to skip those file system blocks that are specifically marked free by the operating system.

Disks	Imaging Options	Schedule	Options	Speed	Log	Log Options	Progress
-------	-----------------	----------	---------	-------	-----	-------------	----------

Backup / Conversion Step #1:

Source Disk Target Disk Options

☒ Prepare all services for backup (application consistency)

☒ Skip disk space marked as free

Step #5: Verification (Optional)

Verification Method: None

Folders to exclude:

Hint: Use separate lines for each path. Don't enter drive letters, for example: \Windows

At the bottom of the above screen you also have the option to use verification. BackupChain will perform the full conversion and then verify file by file if requested. You can exclude certain folders from being verified by entering them without a drive letter, such as:

\temp

to skip all temp folders on the root folder.

### Automatic cleanup of old virtual disk backups

Disks	Imaging Options	Schedule	Options	Speed	Log	Log Options	Progress
-------	-----------------	----------	---------	-------	-----	-------------	----------

Backup Versioning of Virtual Disk Targets

☐ Clean up backup version history before backup (not recommended)

Disk Backups to Keep: 1

In the case of virtual disk targets you can control how BackupChain deletes old backups in the Imaging Options tab. The option “Disk Backups to Keep” determines how many versions you want to have in the backup target folder. “ALL” keeps them indefinitely (not recommended). You can enter any number as needed.

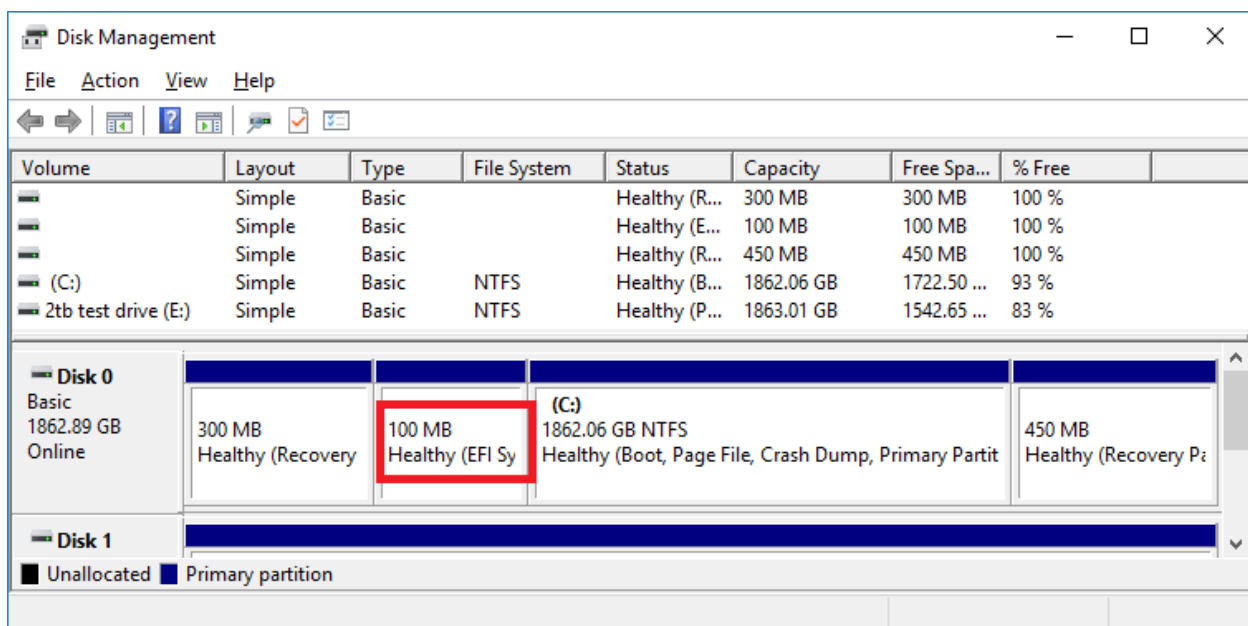
Note the option “clean up backup version history before backup” will allow BackupChain to delete the oldest backup **before** starting the new backup. This is not recommended in the case of keeping just “1” backup in the history because if the backup is stopped or fails, you will be left with no backup at all.

The default strategy in BackupChain is to always ensure you have at least one good backup under all circumstances; however, in some settings available backup storage is very limited and the cleanup option may be the only way to get backups to work at all.

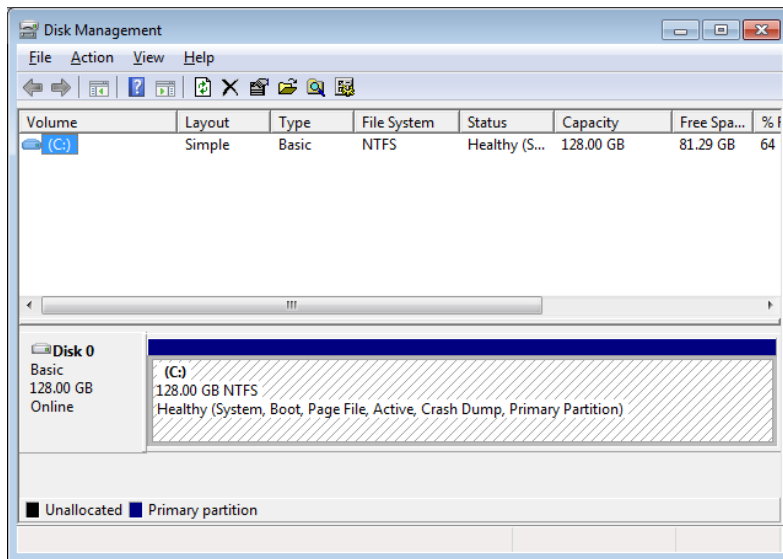
### Booting the virtual disk as virtual machine (P2V)

Please familiarize yourself with the nature of the server's disk layout before continuing with P2V. Open the Windows Disk Management via the Control Panel and have a look at the boot partition.

The example below shows the system drive Disk 0 is a Basic disk (hence it may be backed up by itself in isolation) and uses an EFI boot loader, which is common on newer hardware:



A system without EFI boot loader would look as follows:



Note that EFI boot is not supported on some virtualization platforms. EFI / UEFI can be booted in Generation 2 VMs in Hyper-V Server 2012 R2 / Windows Server 2012 R2 and later. If you want to convert a physical server/PC and run it as VM on earlier versions of Windows, such as Windows Server 2012 or 2008 R2, it would need to have a regular boot loader without EFI.

Note: EFI bios is implemented in VMware Workstation and in VirtualBox as well.

### Create a P2V VM in Hyper-V Server 2016

Note this step only needs to be done once. Once you have the VM in place, BackupChain can replace the virtual disk in subsequent backup cycles automatically. When you need the VM in a disaster recovery scenario, simply boot it up and it's immediately ready to go.

As mentioned above, if your physical machine uses EFI and you wish to use Hyper-V to run the VM, you have to have Windows Server 2012 R2 or later. In this example we will create a Generation 2 VM in Hyper-V:

The screenshot shows the 'New Virtual Machine Wizard' window with the 'Specify Name and Location' step selected in the left-hand navigation pane. The main area contains instructions for naming and locating the VM. The 'Name' field is populated with 'p2v machine'. The 'Location' field shows the default path 'C:\ProgramData\Microsoft\Windows\Hyper-V\'. A checkbox for 'Store the virtual machine in a different location' is unchecked. A warning icon and text at the bottom of the main area advise selecting a location with enough free space for checkpoints. At the bottom of the window, the 'Next >' button is highlighted with a blue border.

**New Virtual Machine Wizard**

**Specify Name and Location**

Before You Begin  
**Specify Name and Location**  
Specify Generation  
Assign Memory  
Configure Networking  
Connect Virtual Hard Disk  
Installation Options  
Summary

Choose a name and location for this virtual machine.


The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name:

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

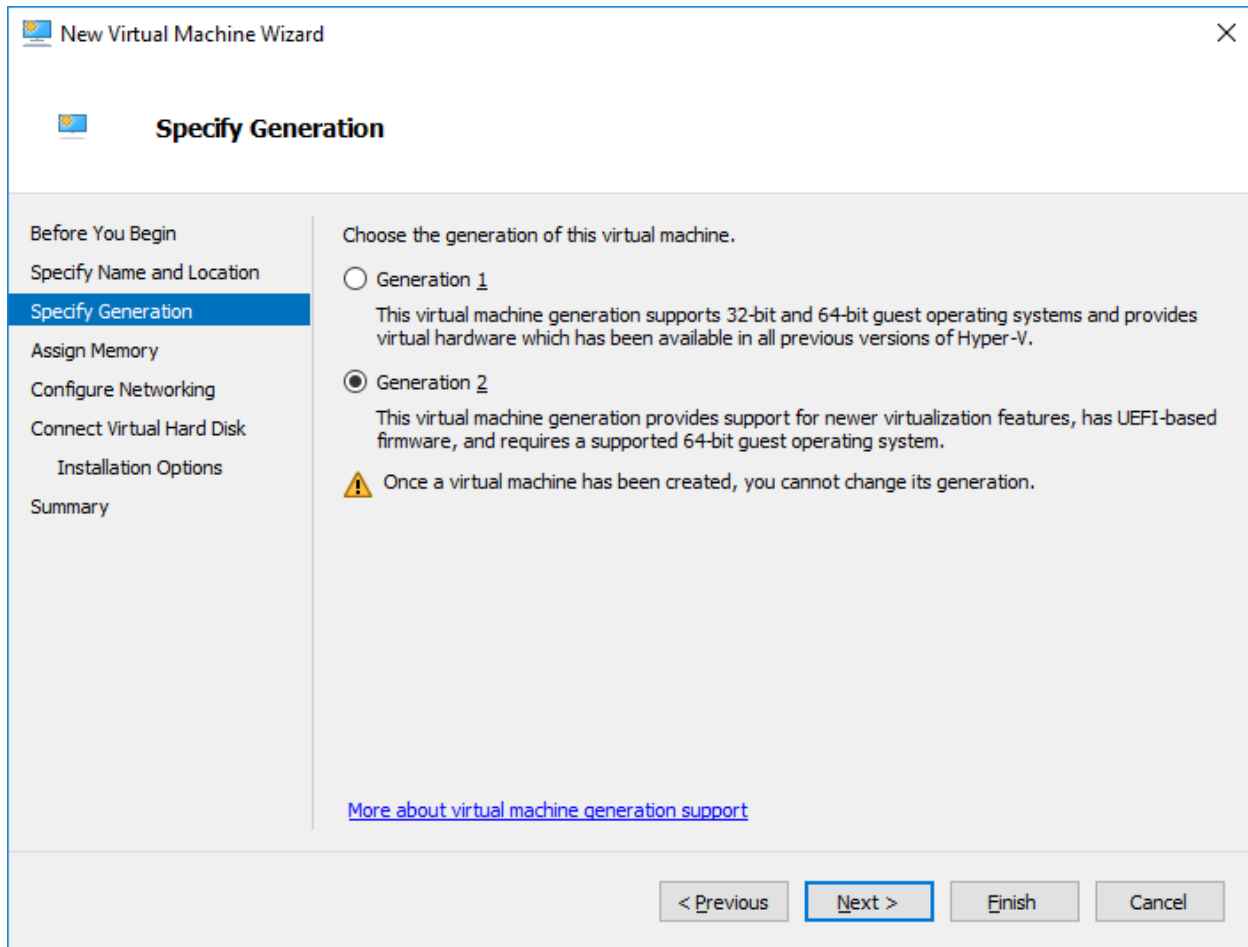
☐ Store the virtual machine in a different location

Location:

 If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

< Previous   **Next >**   Finish   Cancel

Enter name and click “next”:



Select “generation 2” if you need EFI. Note that Hyper-V only supports SCSI controllers in generation2 VMs. Depending on your physical server configuration this may require a change in boot configuration.

Then click Next set a reasonable amount of RAM, disconnect the LAN for now, and in the screen “Connect virtual hard disk” select the VHDX create by BackupChain, see example below:

**New Virtual Machine Wizard**

**Connect Virtual Hard Disk**

Before You Begin  
Specify Name and Location  
Specify Generation  
Assign Memory  
Configure Networking  
**Connect Virtual Hard Disk**  
Summary

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

☐ **Create a virtual hard disk**  
Use this option to create a VHDX dynamically expanding virtual hard disk.

Name:   
Location:    
Size:  GB (Maximum: 64 TB)

☒ **Use an existing virtual hard disk**  
Use this option to attach an existing VHDX virtual hard disk.

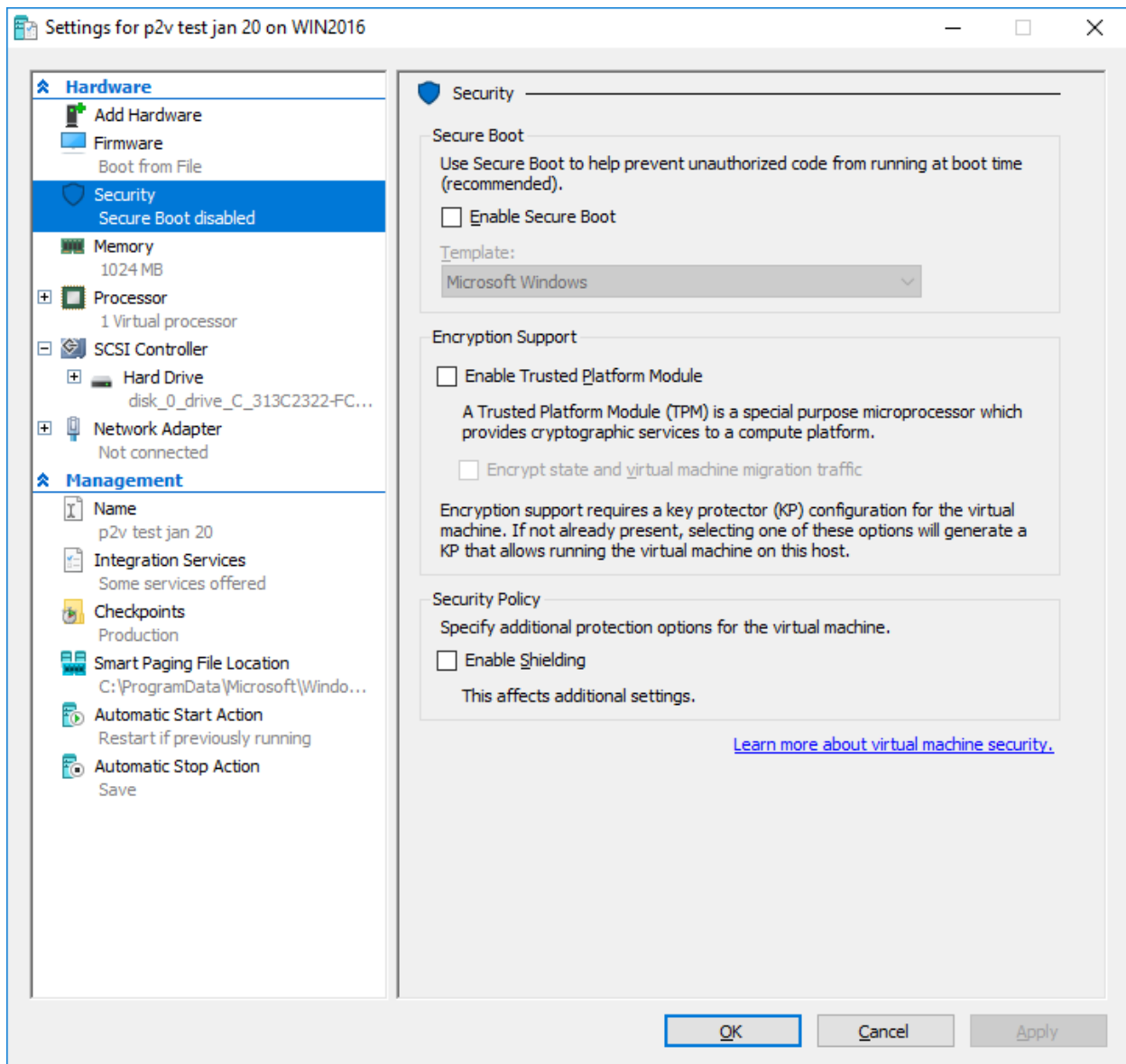
Location:  

☐ **Attach a virtual hard disk later**  
Use this option to skip this step now and attach an existing virtual hard disk later.

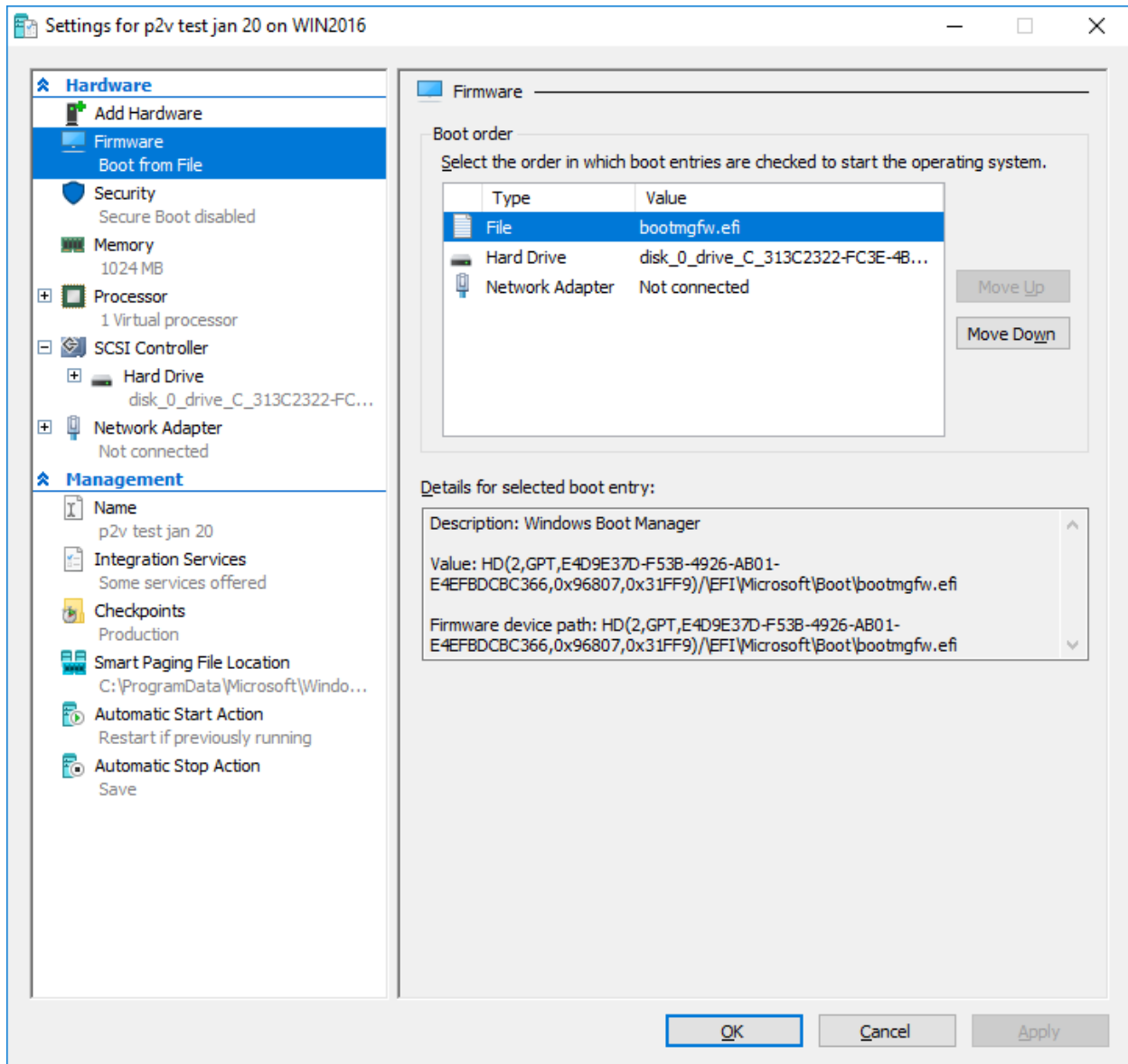
< Previous   **Next >**   Finish   Cancel

Then click finish. In the specific case of “generation 2” VMs we need to change the VM settings one time.

In the security settings, disable secure boot, shielding and TPM:



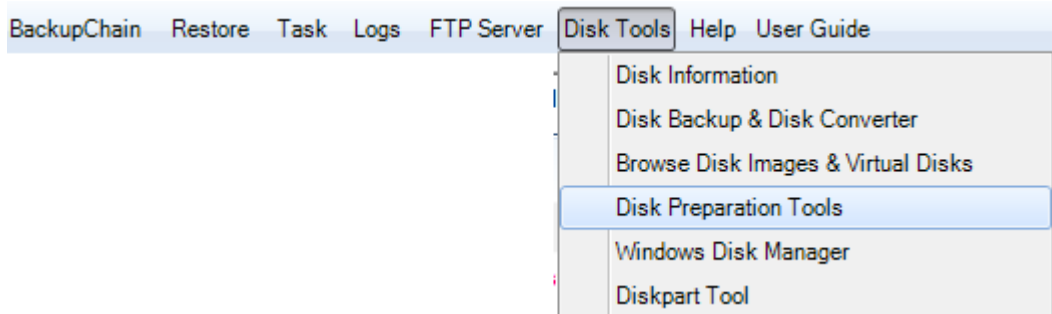
And the firmware section should point to the Windows boot manager on disk:



The VM is now ready to boot. In case the VM boots with BSOD you may need to change the boot settings as explained below:

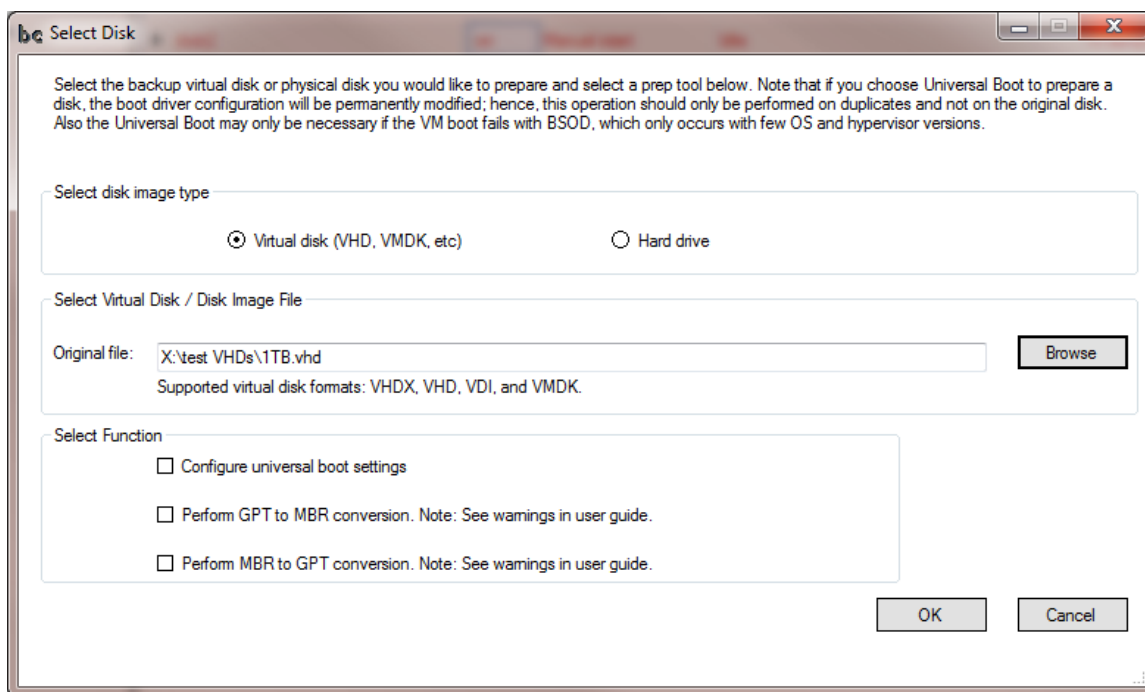
### Changing VM Boot Settings

For some physical machines, depending on their operating system and boot configuration, you may need to prepare the VM's boot settings by using the "Disk Preparation Tools" in BackupChain:



Open it via the main menu as shown above.

Then select the virtual disk file, click “configure universal boot settings”, and click OK as shown below:



Note: if you had copied the physical server to another physical disk instead of a virtual disk, you could now select the backup physical disk to be prepared (grayed out option above). You would use this feature if you wanted to move the disk to another physical machine or if you wanted to attach the physical disk to a VM and boot from it.

After this process is done, the VM’s boot configuration is altered to permit IDE boots as well. This is necessary especially on older virtualization platforms, such as Hyper-V on Windows Server 2008 R2 or VMware Workstation without the EFI bios option enabled.

Note: Unlike Hyper-V, VMware Workstation and ESX allow running the VM off an IDE controller even when the EFI option is ON.

## Create a P2V VM on VMware Workstation

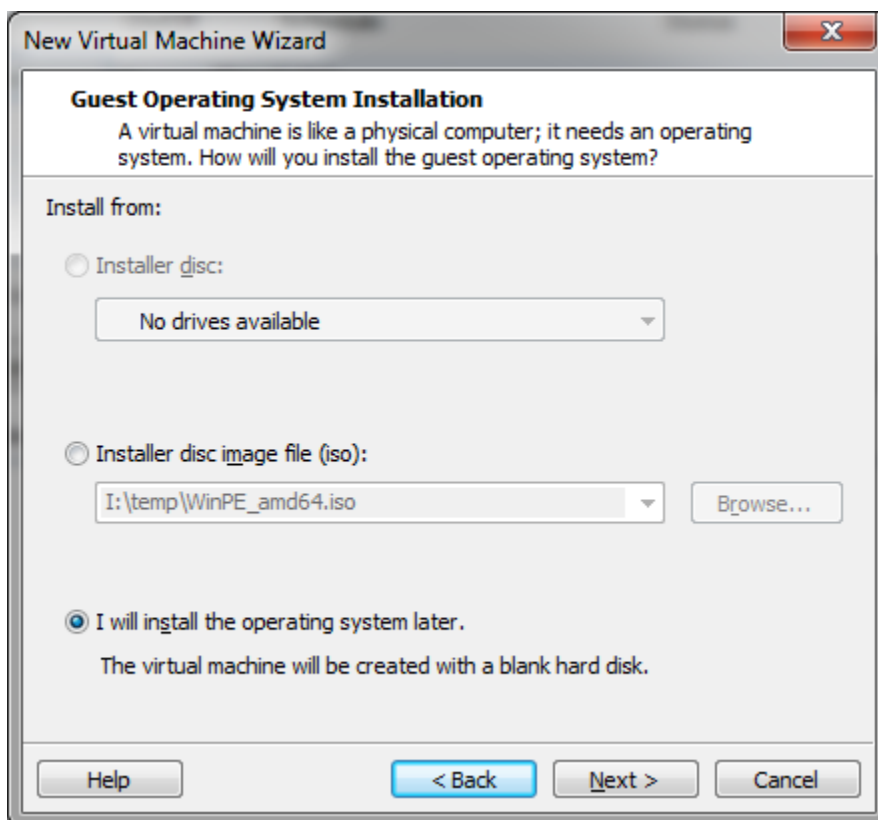
Setting up the VM on hypervisors other than Hyper-V is very similar.

Note, this step only needs to be done once. Once you have the VM in place, BackupChain can replace the virtual disk in subsequent backup cycles automatically. When you need the VM in a disaster recovery scenario, simply boot it up and it's immediately ready to go.

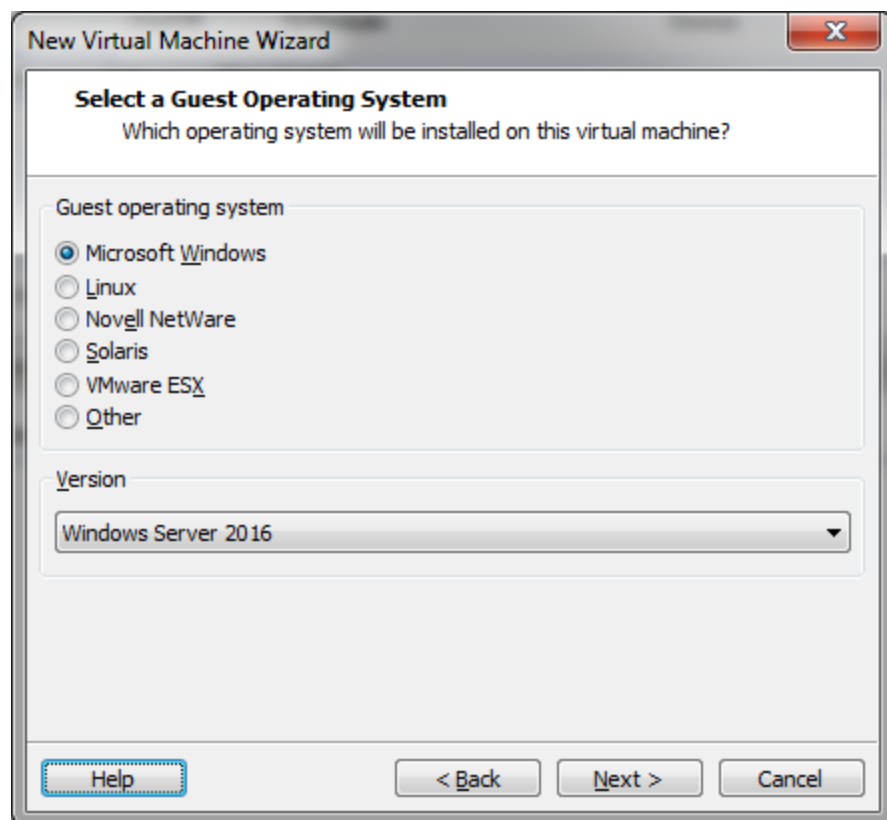
You basically create a new “dummy” VM that points to the virtual disk. If EFI is necessary you need to turn it on in the VM settings.

**Note:** Always attach the virtual disk to an IDE controller first.

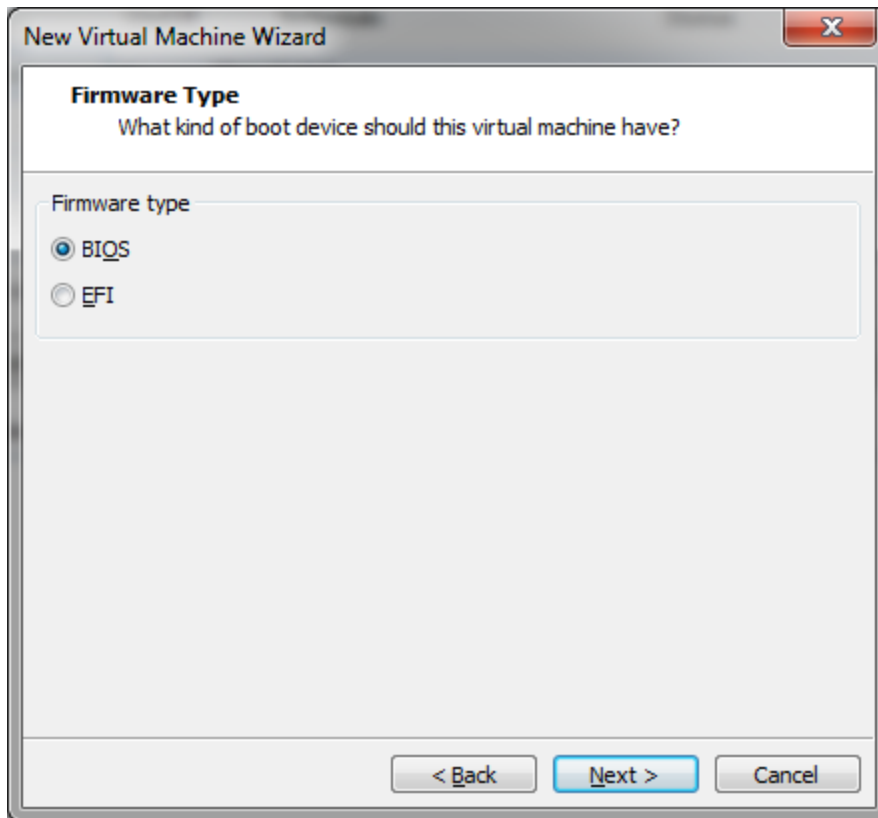
In VMware Workstation, create a new VM:



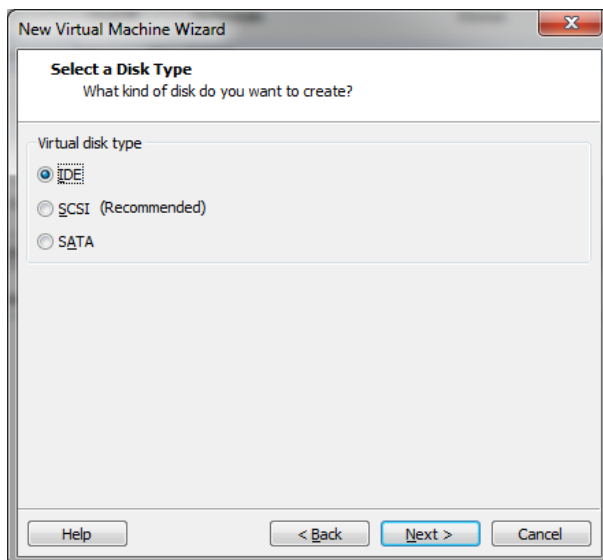
Skip the OS installation, and select a guest OS for hardware compatibility:



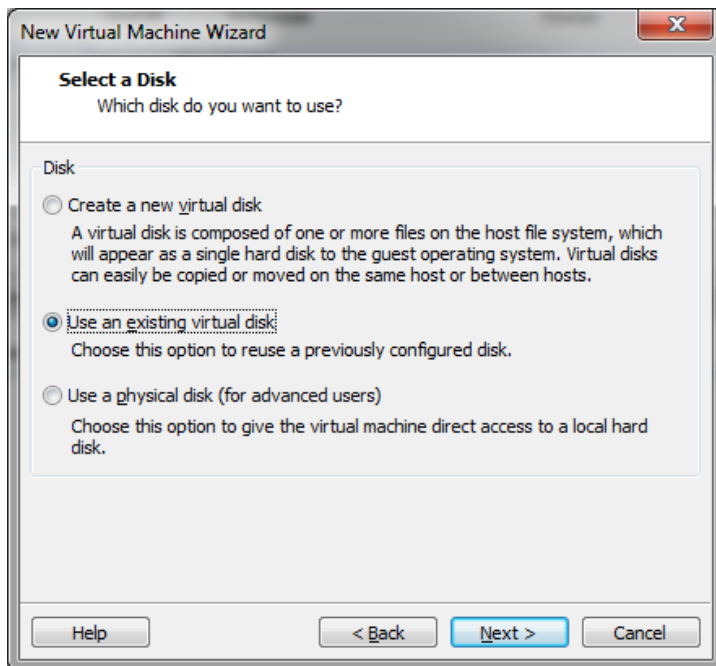
Then name the VM in the following screen and select the appropriate BIOS



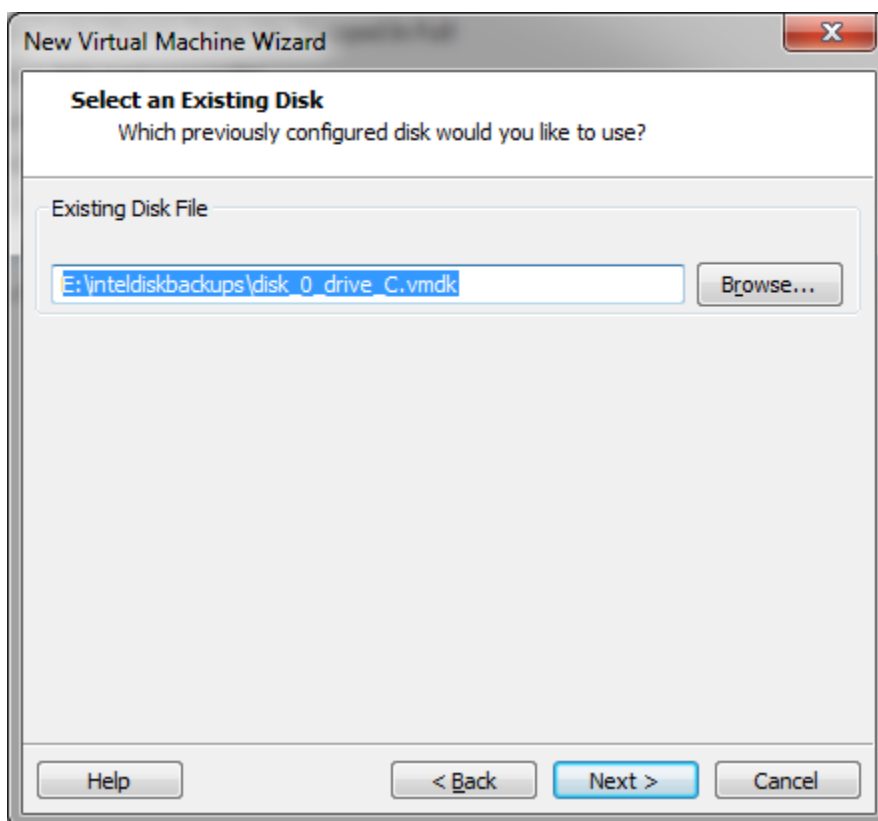
Unlike Hyper-V, you can change this BIOS setting later if need be. Then skip through the next pages, assign LAN and memory and attach the virtual disk to an IDE controller:



Then select "use an existing disk"



And select the virtual disk created by BackupChain:

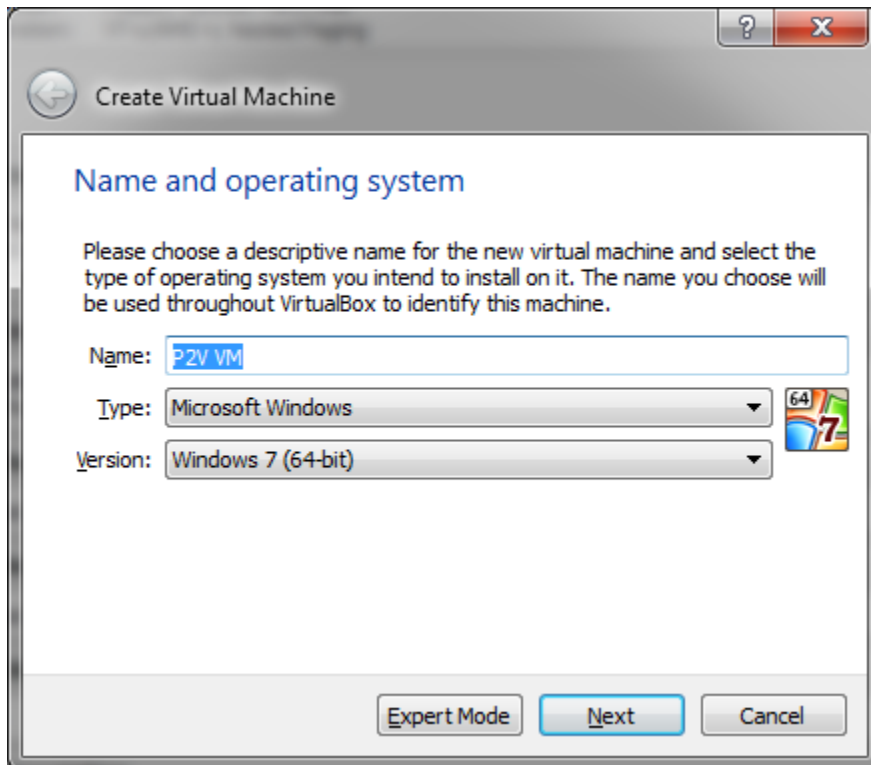


The VM is now done and may be booted. In case the VM boots with BSOD you may need to change the boot settings as explained in the section above, page 144.

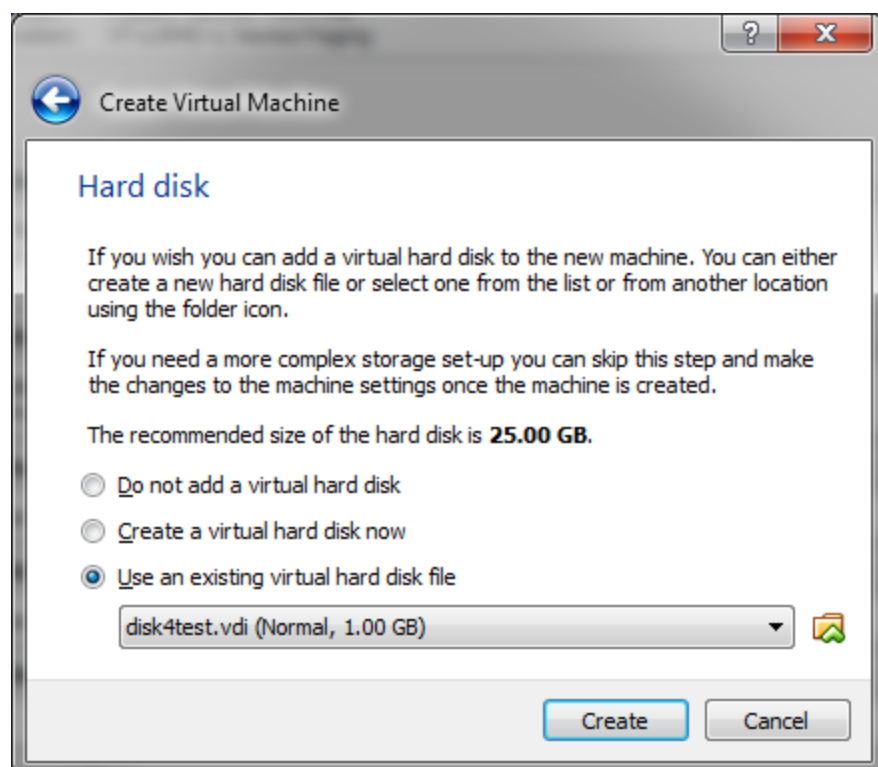
## Creating a P2V VM in VirtualBox

Note, this step only needs to be done once. Once you have the VM in place, BackupChain can replace the virtual disk in subsequent backup cycles automatically. When you need the VM in a disaster recovery scenario, simply boot it up and it's immediately ready to go.

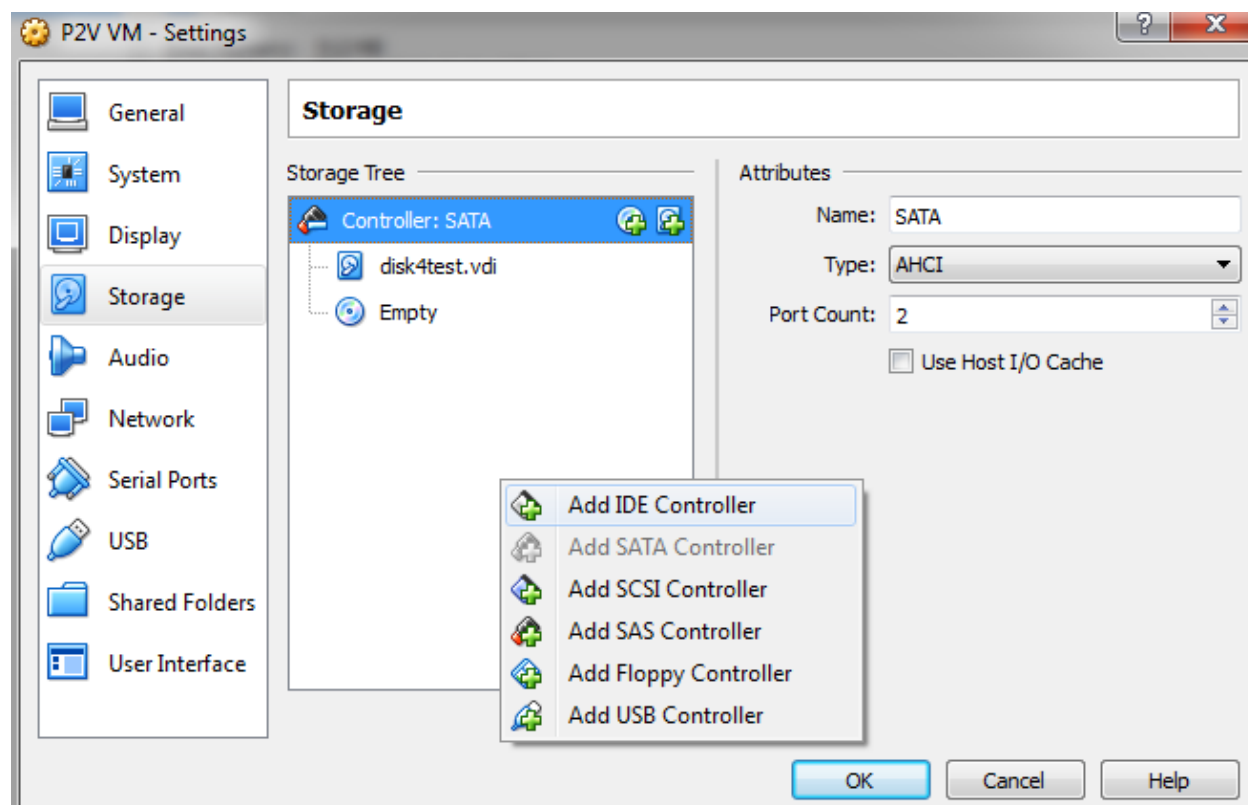
As with all other hypervisors, the strategy is the same. Create a new VM with reasonable RAM and other settings, and point to the virtual disk (VDI) created by BackupChain. Mount the virtual disk to an IDE or SATA controller. If boot issues occur, you may need to change the boot settings as explained in the section above, page 144, and check the EFI Bios setting if need be.



Then move on to the hard disk settings and select the VDI file created by BackupChain:



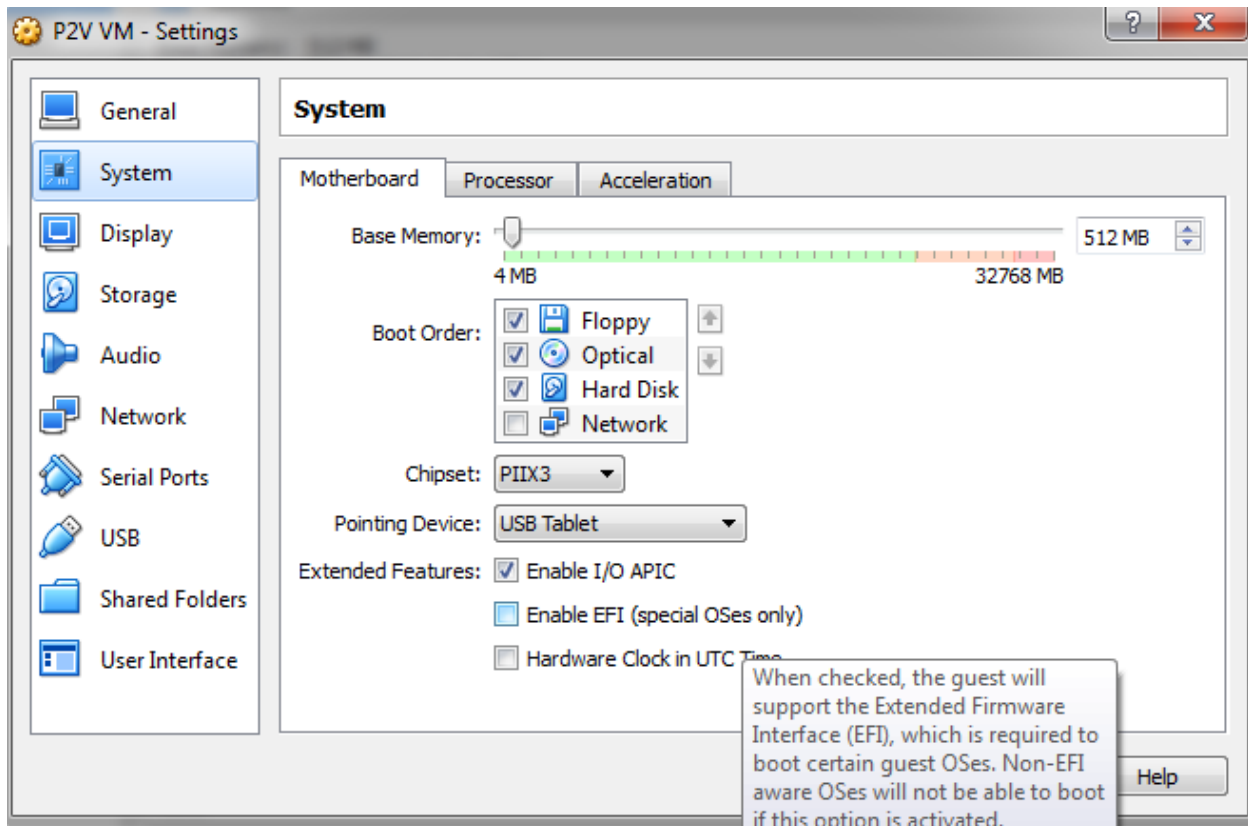
If need be, you can create an IDE controller and attach the VDI to it, if the SATA controller doesn't work with your VM:



Once you have the controller added, delete the VDI from the SATA controller and attach it to the IDE controller instead.

The VM is now done and may be booted. In case the VM boots with BSOD you may need to change the boot settings as explained in the section above, page 144.

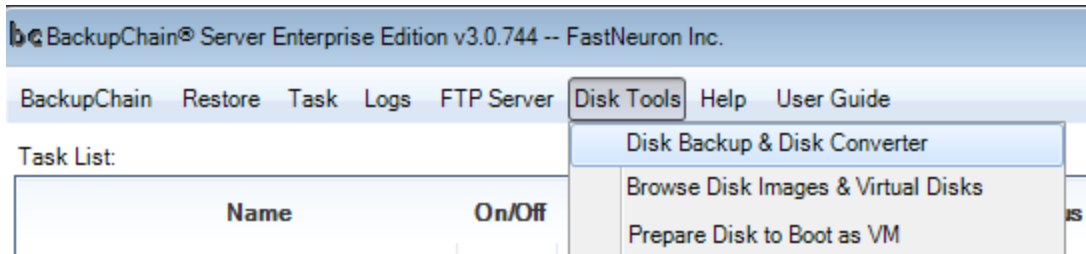
For operating systems using the EFI boot method, you need to enable it here:



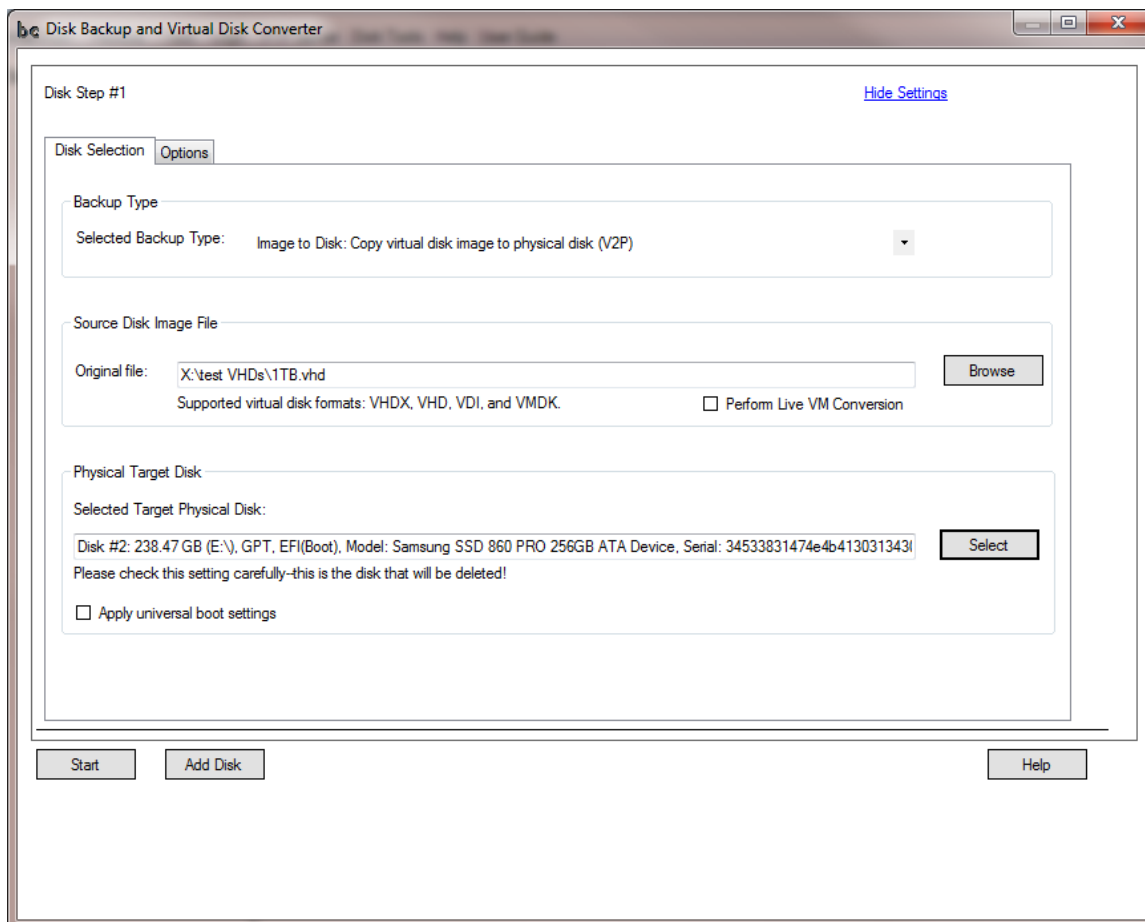
## How to Restore a Disk: Copy a Virtual Disk to a Physical Disk (V2P)

Copying a virtual disk image to a physical disk is essentially a restore operation if the virtual disk was created from a physical disk. However, you can use the same steps shown below to convert a VM to a physical machine by copying its virtual disk to a physical drive.

Either create a new disk backup task as shown in the previous section or open the “Disk Backup & Disk Converter” to do a manual, once-off restore (the steps will be identical):



When the Disk Backup and Virtual Disk Converter opens, select “Image to Disk: Copy virtual disk image to physical disk (V2P)” and browse to the file or enter the file name as shown below:



Turn off “Perform Live VM Conversion” since there is no need to take a snapshot. The virtual disk will be read as-is.

Then elect the physical disk, which will be the destination disk.

If you have several disks you want to restore simultaneously, click “add disk” and repeat the above steps for each disk.

Then click “Start” to start the process. When the process finishes, the physical disk is now ready to be booted from and may be detached from the server and installed to the target machine.

## Converting a Virtual Machine to a Physical Server (V2P)

Follow the steps as shown in previous section to copy the virtual disk contents to a physical disk.

**Note:** When converting a *virtual machine’s virtual disk* to a physical disk for the purposes of converting the VM into a physical server, try attaching the disk to an IDE controller first. Once Windows boots you can install any RAID drivers and other drivers the machine needs. Then attach to the other drive controller if necessary.

**Note:** Check your BIOS boot settings. You may need to switch off RAID and AHCI mode and switch to IDE in order to get the disk to boot on a physical machine.

In some cases it may be necessary to run the “Prepare Disk to Boot as VM” tool on the *physical disk* via the main menu Disk Tools->Prepare Disk to Boot as VM->select hard drive and click OK.

**Helpful Hints:** If the physical machine that you created from a virtual disk fails to boot and gives BSOD errors, try creating a dummy virtual machine in VMware Workstation/Player, VirtualBox, or Hyper-V with the *physical disk* attached to a virtual IDE controller. On older Windows versions this helps load safe mode where Windows will then update its own drivers properly. On newer versions of Windows (7 or Server 2008 and later) this is likely not necessary. Also once in safe mode you can uninstall VMware tools or Hyper-V Integration Services, and you could install the hardware drivers supplied with your target motherboard if need be.

## Tips to prevent BSOD when booting on new hardware

Another option once the physical disk is booted into a VM is to use the Windows utility sysprep with ‘generalize’ option to prepare Windows for new hardware (click reseal). You will find sysprep in the Windows CD, usually in the folder Support\Tools\deploy.cab. You could use 7-zip to extract all necessary files for sysprep out of the cab file.

On older Windows operating systems, such as XP or Windows Server 2003, you may need to install some basic out-of-the-box drivers in order to get Windows to boot again. A very helpful article is KB314082 (<https://support.microsoft.com/en-us/help/314082>). Once you boot the VM from the physical disk, use the info provided in the article to place standard IDE drives back into the system:

Extract the Atapi.sys, Intelide.sys, Pciide.sys, and Pciidex.sys files from the %SystemRoot%\Driver Cache\i386\Driver.cab file, or copy the files to the %SystemRoot%\System32\Drivers folder.

In Microsoft Windows Explorer, right-click the Mergeide.reg file in the floppy drive, and then click Merge. The reg file contents are available on the page linked above.

Then shutdown the VM and attach the disk directly to the target server's IDE or SATA port.

## Granular Backup and Restore

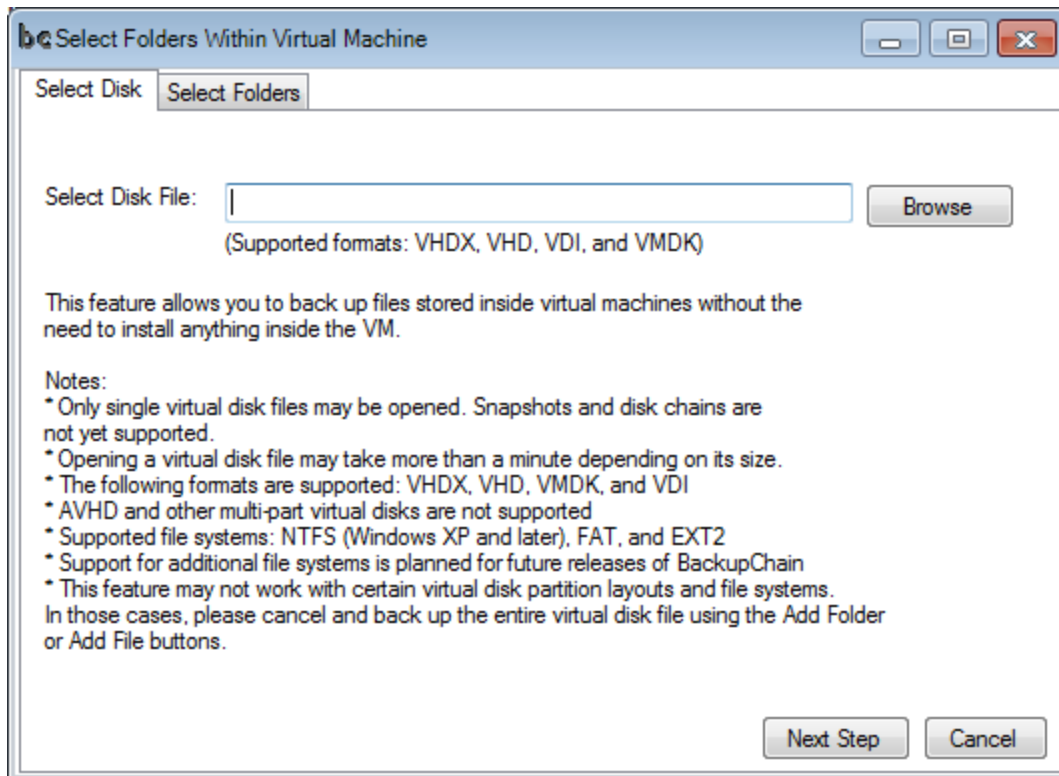
**Granular Backup and Granular Restore are features available only in BackupChain Server Enterprise and Platinum Editions.**

**BackupChain's Granular Backup and Granular Restore features work with VDI, VMDK, VHDX, and VHD files. Snapshots and chained virtual disks are not supported.**

**Granular Backup** is a feature that allows you to back up one or more files or folders from inside a virtual machine without backing up the entire virtual disk. In addition, no software installations are necessary inside the VM. You can back up files and folders inside a VM just like local files with the same spectrum of options. For example, you can back up files from inside a VM to an FTP site using deduplication.

**Granular Restore** is the feature needed to extract one or more files and folders from deduplicated and compressed backups, or plain file backups. Note: You cannot use Granular Restore on ZIP format backups. You cannot use this feature via FTP. If you use the recommended settings when creating the backup, or the 'no file processing option' Granular Restore should work fine.

Not all types of file systems are supported. An up-to-date list of limitations appears on the user interface of BackupChain when you add folders stored inside virtual machines to the backup. (Folders or Files tab, click Add Folders->Add folder stored inside virtual machine):



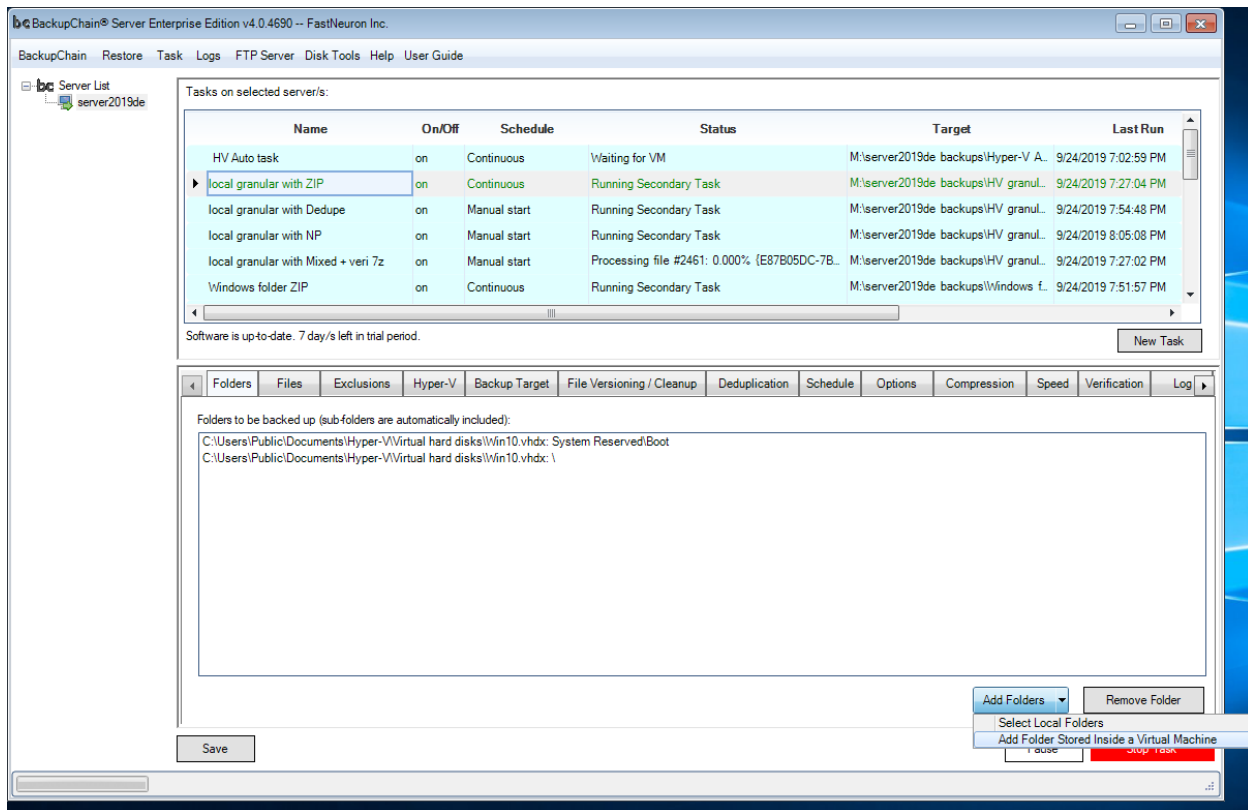
Since this is an actively supported feature, later releases will be supporting additional file systems and virtual disk formats. Your BackupChain software version may already support more systems than shown in the screenshot above.

## How to Configure a Granular Backup

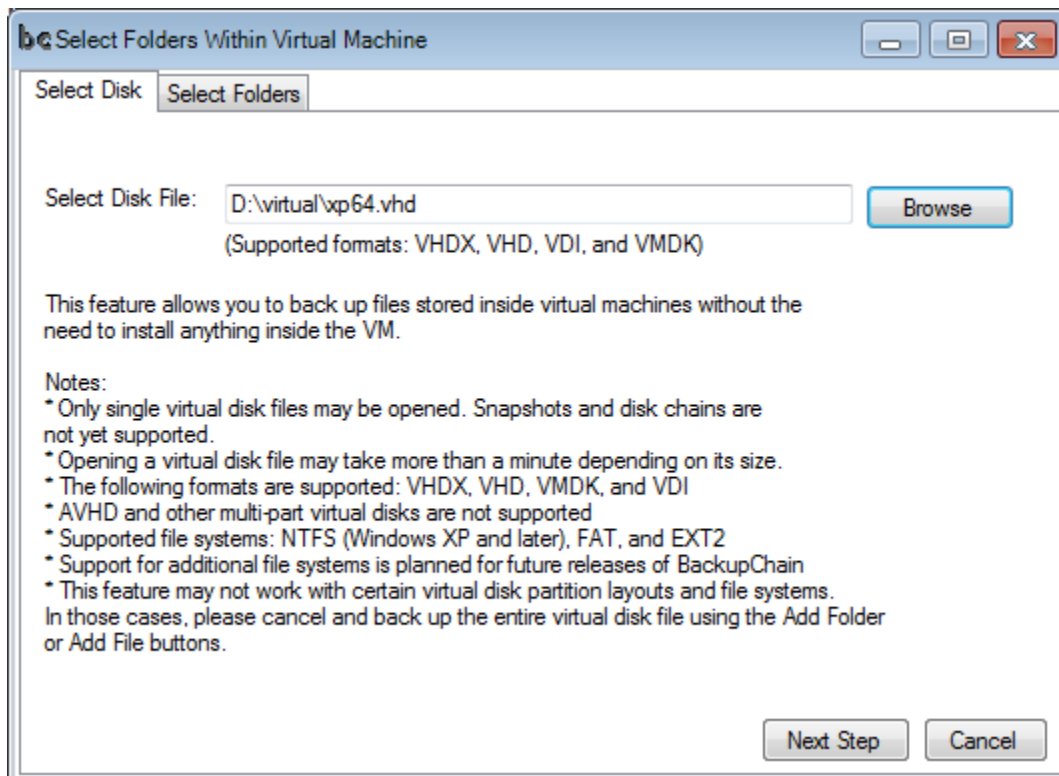
**Note: Granular Backup and Granular Restore are features available only in BackupChain Server Enterprise Editions.**

Granular Backups have been discussed already in other sections. This is a short walkthrough and applies to all virtualization platforms, such as Hyper-V, VirtualBox, VMware Server, VMware Workstation, and Virtual PC:

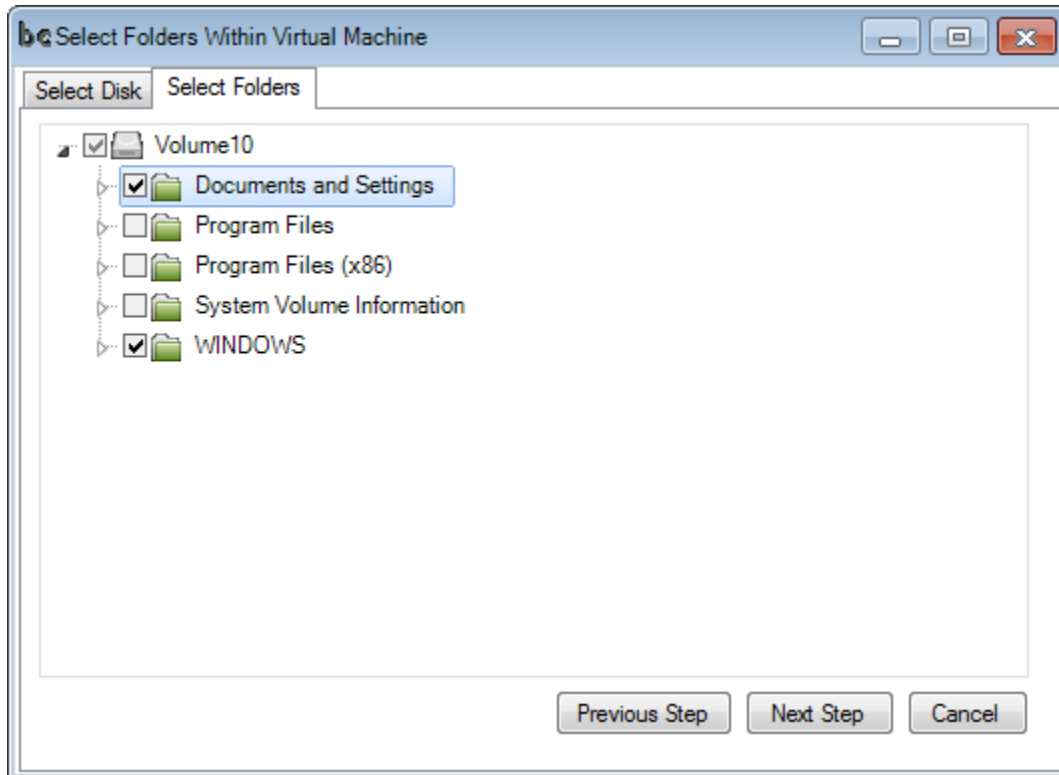
To add a folder stored inside a virtual machine, open the Folders tab and click Add Folders -> Add Folder Stored Inside a Virtual Machine:



Then navigate to the virtual disk file (\*.VDI, \*.VMDK, \*.VHDX, or \*.VHD):



Click Next Step and wait for the screen to load. Now you may select the partition and the folders or files you want backed up:



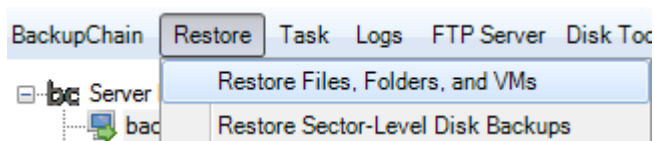
Note: to select individual files inside a virtual machine instead of folders, you need to start the same process in the Files tab instead of the Folder tab of BackupChain.

## How to use Granular Restore to Extract Individual Files from Virtual Machine Backups

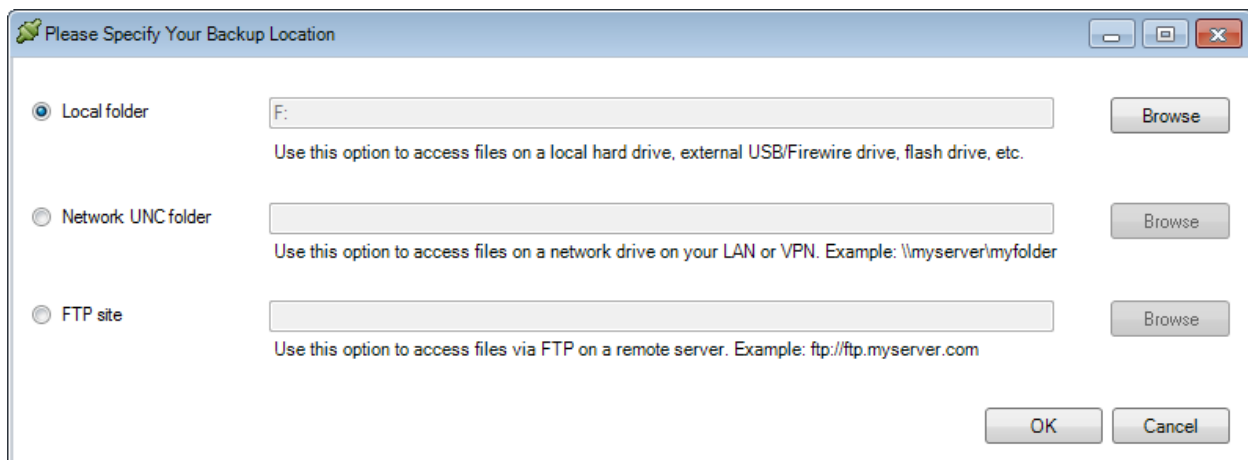
**Note: Granular Backup and Granular Restore are features available only in BackupChain Server Enterprise Editions.** Limitations may apply, see previous section. You cannot use this feature on ZIP files. It works on deduplicated backups (FastNeuronDelta files) and plain files (VHD, VHDX, VMDK, VDI). You cannot use Granular Restore via FTP.

This feature works for all supported virtualization platforms: Hyper-V, VirtualBox, VMware Server, VMware Workstation, and Virtual PC; however, not all file systems are supported, see previous section.

Select Restore from the Main Screen:



Then enter the backup folder. Note: The backup folder info will be preset if you select the backup task first before clicking restore.



Proceed by clicking OK and select a Restore Point:

Select Restore Point

Restore Option

☒ I want to restore from a particular backup point in time  
☐ I do not know when the data was backed up; show all available data

Select the date of the backup you want to restore:

Select the time of the backup you wish to restore below.  
Note: Incomplete backups were either stopped or cleaned up.

September 2019

Mo	Tu	We	Th	Fr	Sa	Su
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

9/24/2019 8:05:37 PM (Complete)

9/24/2019 7:02:59 PM (Complete)  
9/24/2019 6:28:25 PM (Complete)  
9/24/2019 6:00:06 PM (Complete)  
9/24/2019 5:05:52 PM (Complete)  
9/24/2019 2:44:27 PM (Complete)  
9/24/2019 2:07:34 PM (Complete)  
9/24/2019 1:10:53 PM (Complete)  
9/24/2019 11:36:53 AM (Complete)  
9/24/2019 10:23:32 AM (Incomplete)

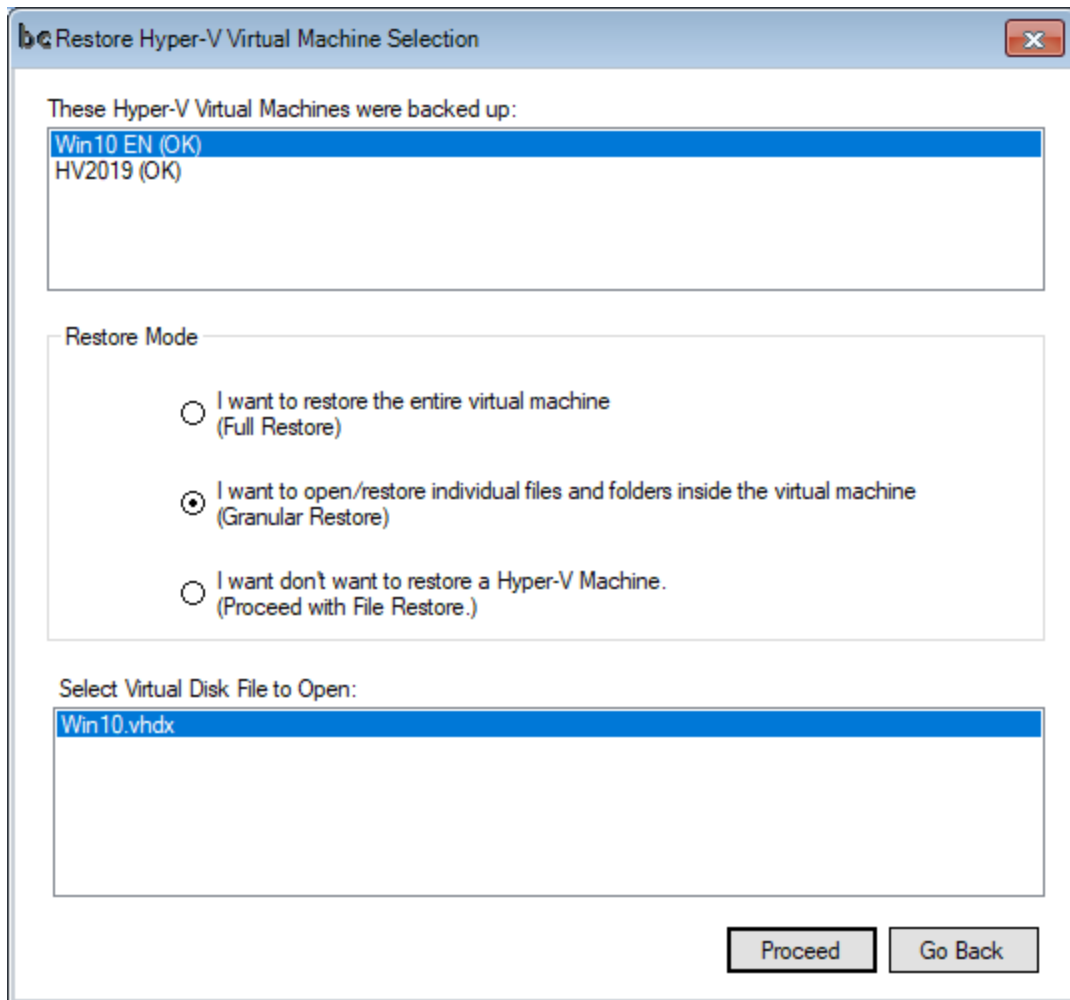
Loading backup list..  
The oldest restorable VM backup is dated: 9/24/2019 10:23 AM

Continue
Go Back

You can also skip the Restore Point selection by choosing “I do not know when the data was backed up” in this screen. In that case all available file versions will appear in the Restore Screen.

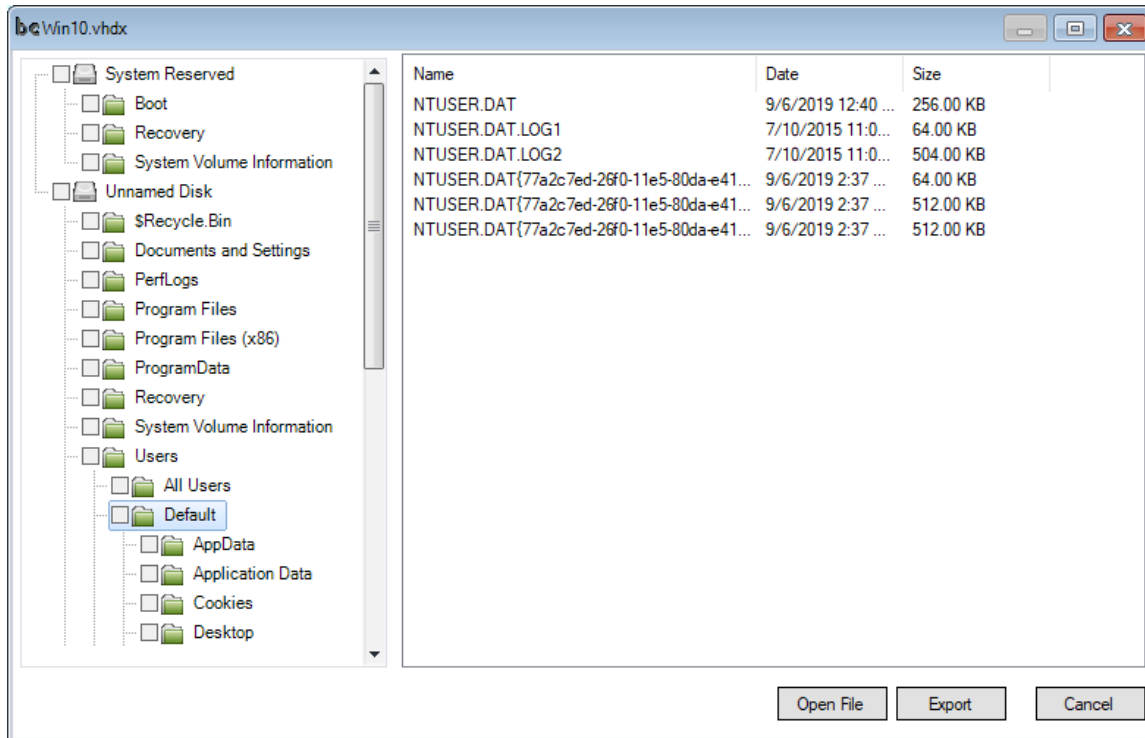
Note that in the special case of virtual machine backups, BackupChain will load all restore point info in the background and update you with the latest restorable backup. In the above example, it’s 9/24/2019 10:23 AM. The backups before that are no longer fully restorable. They may be partially restorable, depending on your exact backup cleanup settings.

Now click Continue. **In the special case of Hyper-V backups**, a screen will appear that contains additional info about each VM backed up at the chosen Restore Point earlier:

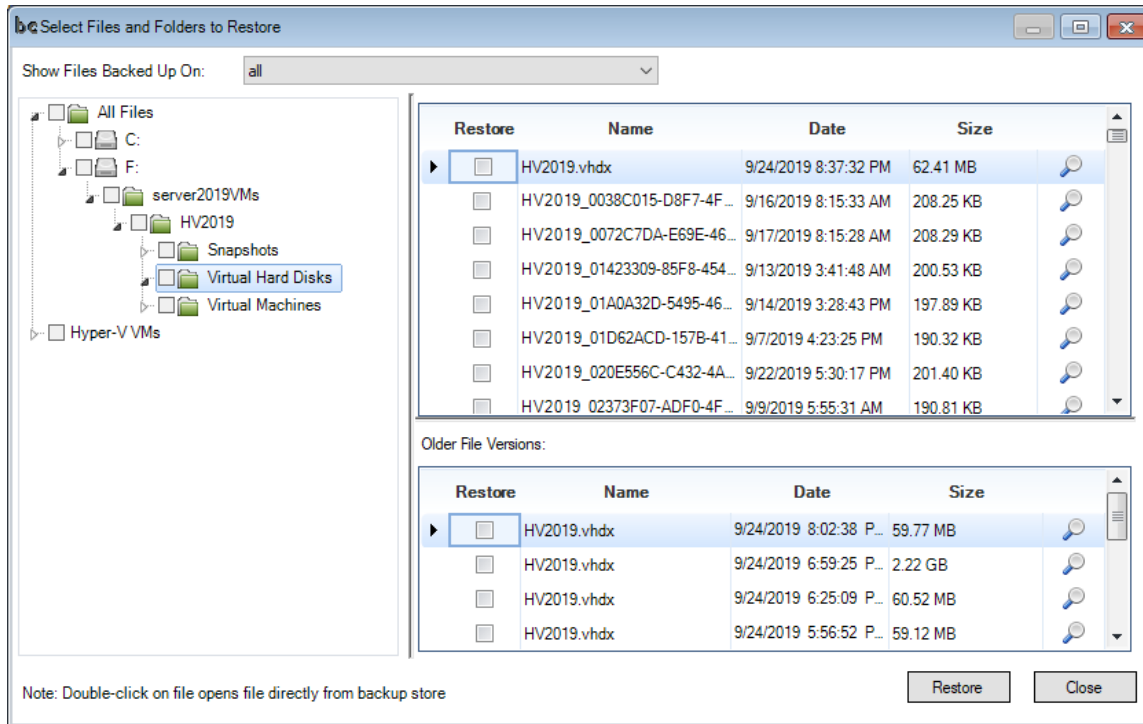


Choose from the top list the VM. The (OK) behind the name means the backup of that particular VM at the chosen Restore Point in time was successful. Select the VM and then the option "Granular Restore". At the bottom you will see a list of the VM's VHDs. You need to choose one in order to continue.

You will then see the VM's internal file system at the time of backup where you can export files and folders directly from the backup, without having to restore the entire virtual disk:

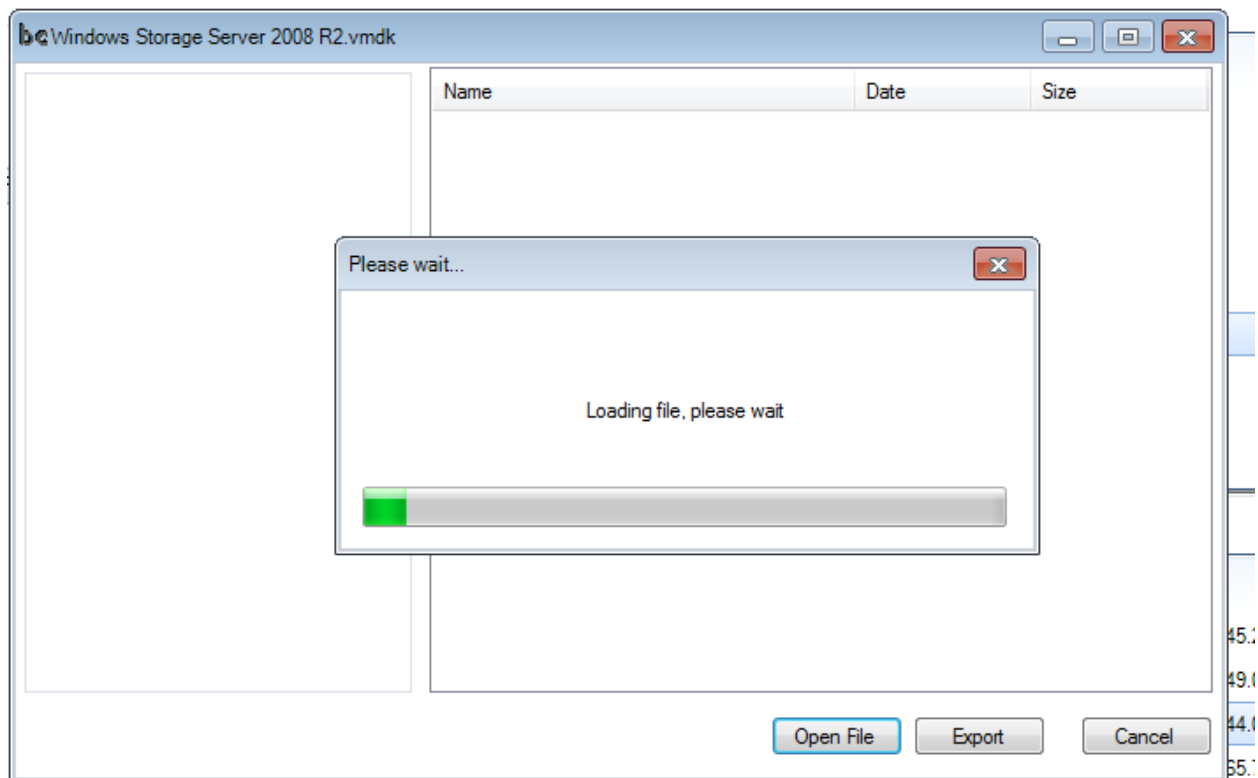


In the case of virtual machine backups other than Hyper-V (such as VMware or VirtualBox), you will see a Windows Explorer-like view of your backup data. Navigate to the virtual disk of interest. As soon as you select the virtual disk, if multiple versions exist, the screen will split in half and you will see older file versions at the bottom:

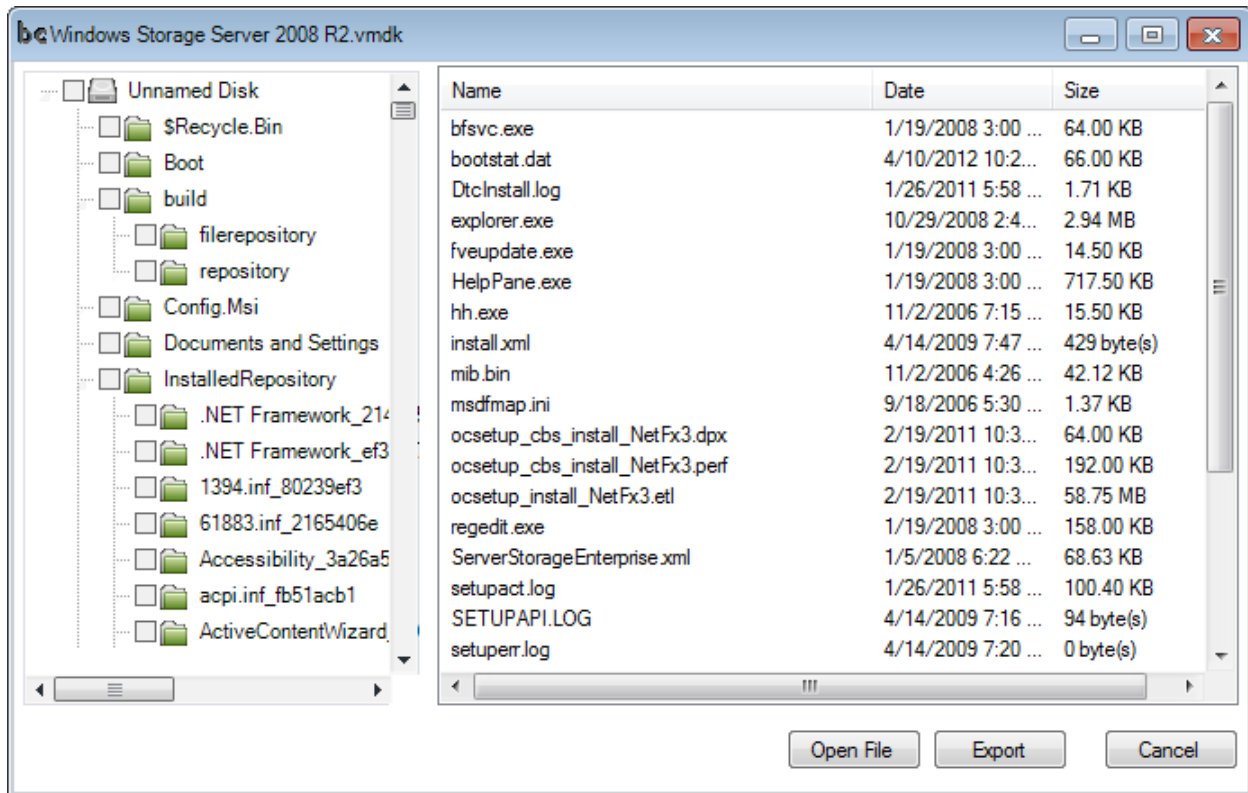


Now either click on the magnifying glass or double-click on the VMDK, VHDX, VHD, or VDI file.

The Granular Restore screen will start loading. It may take a minute or two on very large backups:



Once done loading, you can freely navigate through the VM's virtual disk without restoring the entire VMDK:



Using the above screen you can directly Open files or Export entire folders or a file selection to your local hard drive.

## Hyper-V Virtual Machine Backup and Restore

Hyper-V virtual machines may be backed up using two different methods.

One method is to back up Hyper-V's files and folders manually.

BackupChain also offers a fully automatic way to back up and restore your virtual machines in Server and Platinum Editions. Server Enterprise and higher also offer an automatic VM selection feature for Hyper-V backups.

### Hyper-V Live Backup Prerequisites

In order for live backup to be available in the guest VM:

1. Install the latest Hyper-V Integration Services (For hosts older than Windows Server 2016)
2. Install the latest Windows updates to your host server.
3. Avoid using snapshots because they are not recommended for production systems. If you do use snapshots, store them in the same folder as the main VHDs.
4. Be aware that in Server 2008 / R2, when you delete snapshots Hyper-V hides from the user interface but they are still in operation until the VM is shut down for a while.
5. Ensure NTFS is used throughout.
6. Hyper-V integration services are necessary to use live backup. On some guest operating systems Hyper-V provides no live backup support. (Whether live backup takes place or a saved state backup is entirely up to Hyper-V to decide at runtime). Please check whether integration services exist for your particular guest OS and host Windows version. If you encounter a case where Hyper-V does not support live backup for a particular guest OS, you can switch off the "Backup" option in the VM's integration options in Hyper-V Manager. This will prevent the VM from going into a saved state and provide you with a crash consistent VM backup. Application consistency, however, can only be achieved with integration services running properly and the "backup" option in Hyper-V being switched on.

## File-based Approach for Hyper-V Backup

### Backup

The file-based approach is not recommended unless you are an advanced user. It is not recommended for cluster shared volumes. Most users should use the Automatic Hyper-V Backup feature instead, see next section below.

Note that you can only back up live virtual machines when they are stored locally. Live backup does not work over the network (only exception SAN and CSV backups); this means you cannot *pull* VMs stored on another server. VMs must be running locally in order to be backed up live. Offline backups (when VMs are shut down) do work over the network, however.

1. Open the New Backup Wizard and create a new “Hyper-V Backup (Server)” task using the New Task button:

**Create a New Backup Task Wizard -- BackupChain**

Select Backup Type | Help | **Hyper-V** | Select Folders | Default Settings | Options | Target | Finished

**Welcome to BackupChain's Backup Task Wizard!**

This wizard guides you through the main functions of BackupChain and assists you in setting up a backup task. Backup tasks store all your settings for future use. Tasks may be scheduled or may be run manually whenever you need to run a backup. Once saved, you may fine-tune your backup task later in the Main Screen, where all features of BackupChain are available.

Create Task on Server: **server2019de**

Enter a Task Name:

Please select the purpose of this backup task:

**I want to back up documents and file server data...**

☐ **File-Level Backup**  
(File Server and Version Backup. Use for file server data, documents, etc. Files are placed individually in backup folder. Do not use for VMs)

**I want to back up virtual machines...**

☒ **Hyper-V Backup (Server)** (Automatic or Granular Backup) ☐ **Hyper-V Backup (Client)** (File-based, recommended only for Windows 8-10 + Pro Edition) ☐ **VMware Backup** (VMware Workstation, Player, VMware Server backup) ☐ **VirtualBox Backup**

**I want to back up the Windows boot disk or sector-level backup...**

☐ **Disk to Image Backup (Sector-Level)** (Sector-based backup of a physical disk into a disk image file. This is usually only done to back up operating system disks) ☐ **Disk Cloning (Sector-Level)** (Sector-based copy of a physical disk to another physical disk. This can be used for Windows operating system boot disks as well as data disks) ☐ **Restore Disk Image Backup (Sector-Level)** (Restore a disk image file to a physical disk)

**I want to convert physical and virtual machines / disks...**

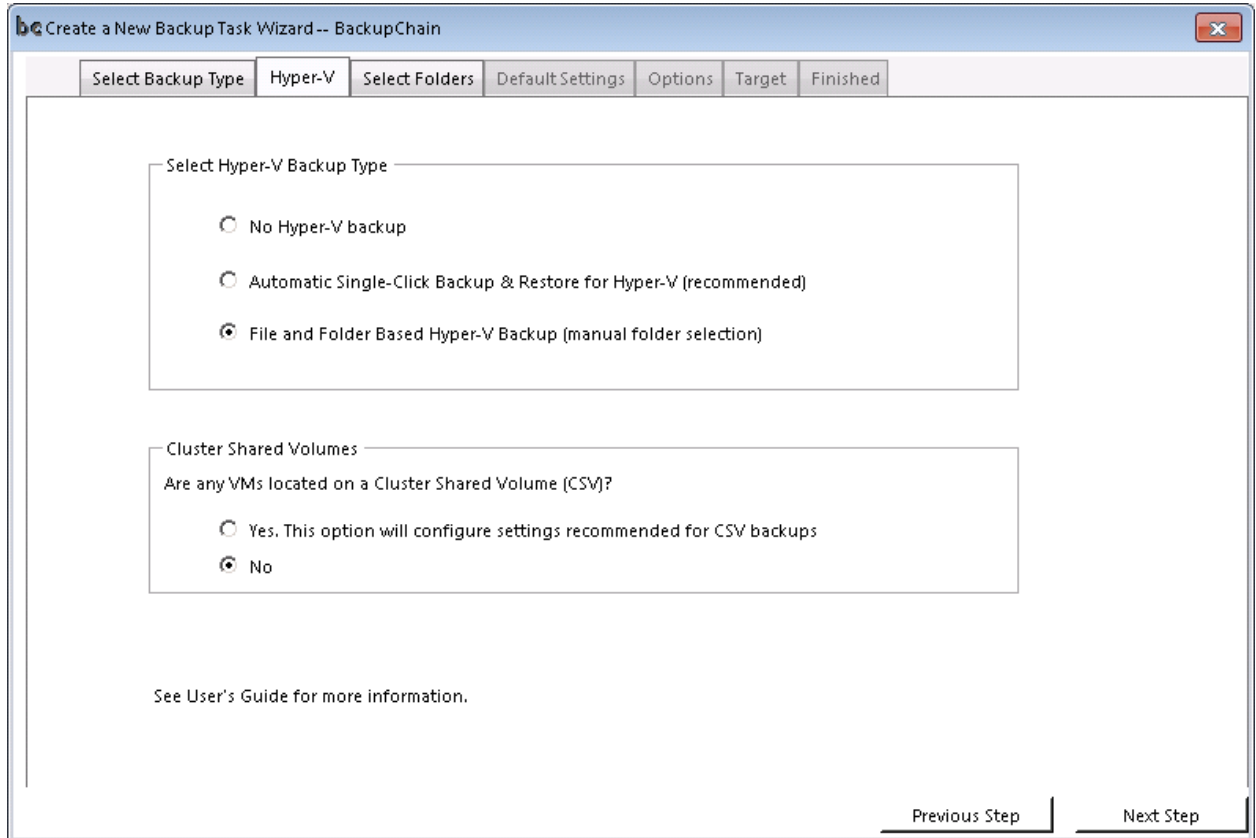
☐ **P2V** (Physical disk to virtual disk conversion) ☐ **V2P** (Virtual disk to physical disk conversion) ☐ **V2V** (Virtual disk format conversion)

**Other backup task types:**

☐ **SQL Server Backup** (Backup SQL Server and MSDE Databases) ☐ **Universal Backup** (Backup all VSS aware services. Use only if no other backup type suits)

**Go Back** **Next Step**

2. Now determine the type of Hyper-V backup you want to use. It's strongly recommended to use "Automatic Single-Click Backup and Restore" instead of the file and folder based method but since this tutorial describes the file-folder method, we'll continue with the file-folder type:



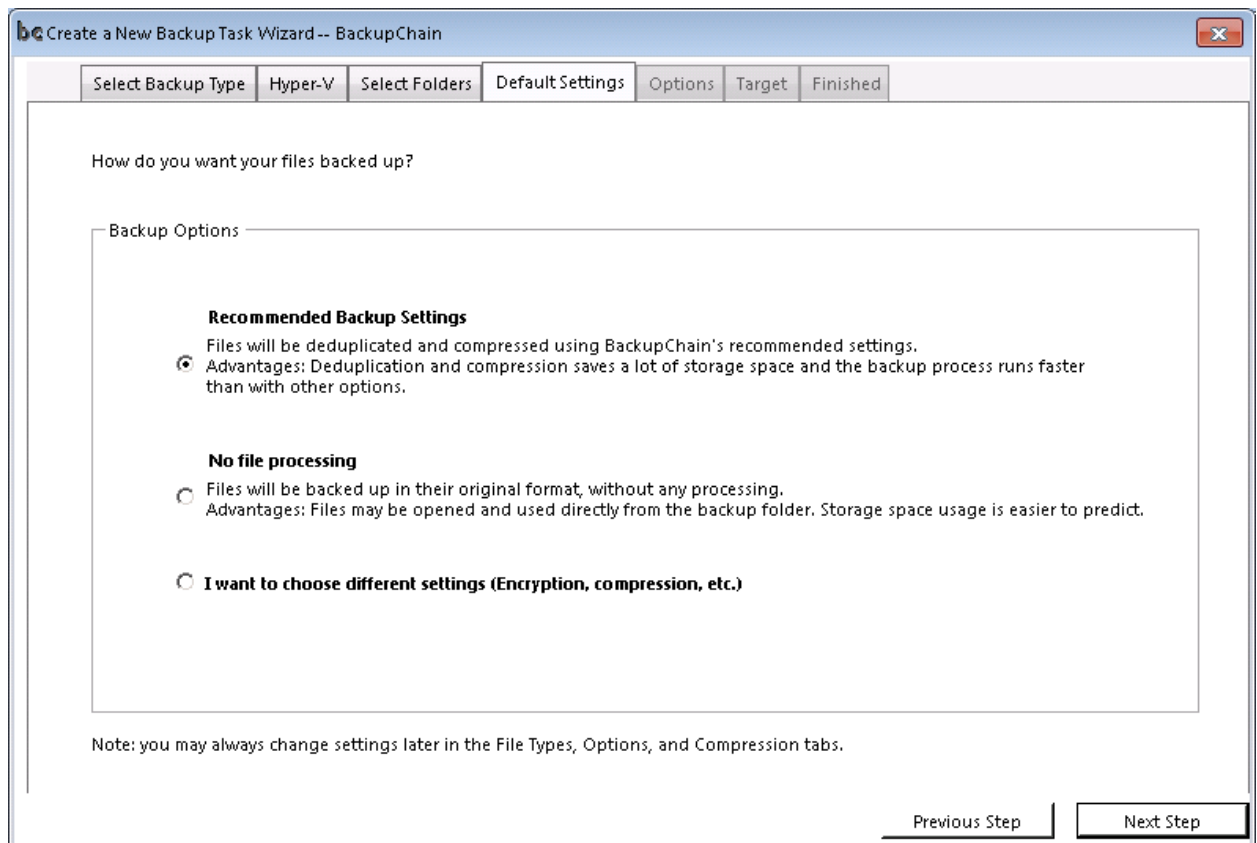
If your VMs are located on a cluster shared volume, select the CSV option at the bottom.

3. Select the folder containing the virtual machine files (VHDs, and Virtual Machine and Snapshots folders)



Note: You cannot pull files over the network. VMs must be installed locally or on a CSV in order for live backup to work.

4. Next, accept default settings or use custom settings:



Recommended backup settings will turn on deduplication, data compression, and a retention period of 10 file versions (i.e. after the 11<sup>th</sup> backup of a file the oldest backup is deleted).

“No file processing” switches off deduplication and data compression and uses a retention period of 10 file versions.

If you choose custom settings the following screen opens:

bc Create a New Backup Task Wizard -- BackupChain

Select Backup Type | Hyper-V | Select Folders | Default Settings | **Options** | Target | Finished

Please choose among the following options. These are minimum settings to get you started.  
More advanced settings can be specified later if necessary.

**Deduplication**

☒ On ☐ Off

**Compression Settings**

☐ No Compression (Usually slower)  
☒ Fastest Compression  
☐ Standard Compression  
☐ High Compression (Slower)

**Resource Usage**

☐ Maximum Speed (Uses more resources and RAM)  
☒ Minimal System Impact (Slower)  
☐ Reduce Hard Drive Stress (Slowest)

**Automatic Cleanup**  
 Keep this many backups of each file in the backup store: 10  
 Enter a number or ALL to keep all file changes.  
 A setting of 10 will keep up to 10 backups of each file

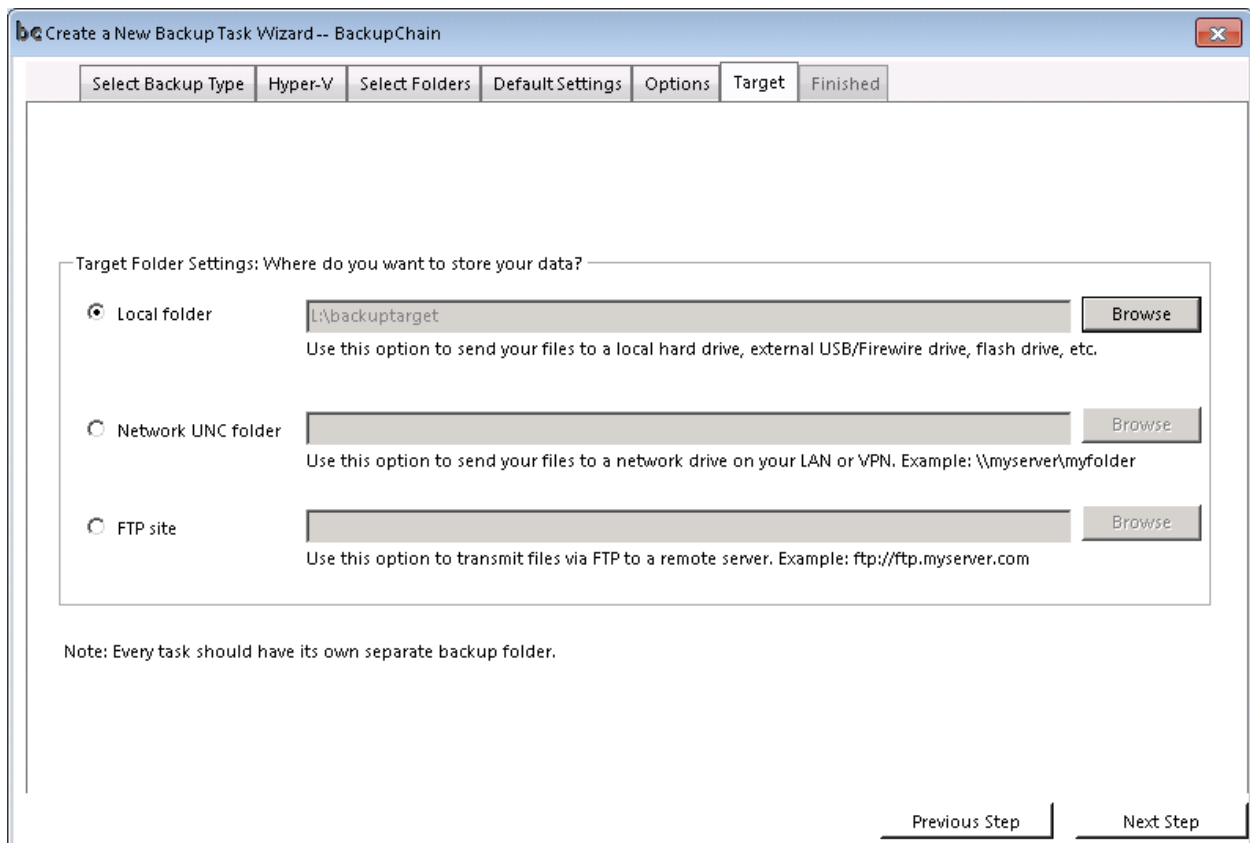
☐ Encrypt files with military strength encryption (AES 256, HIPAA compliant)

Password:  Confirm password:

Previous Step | Next Step

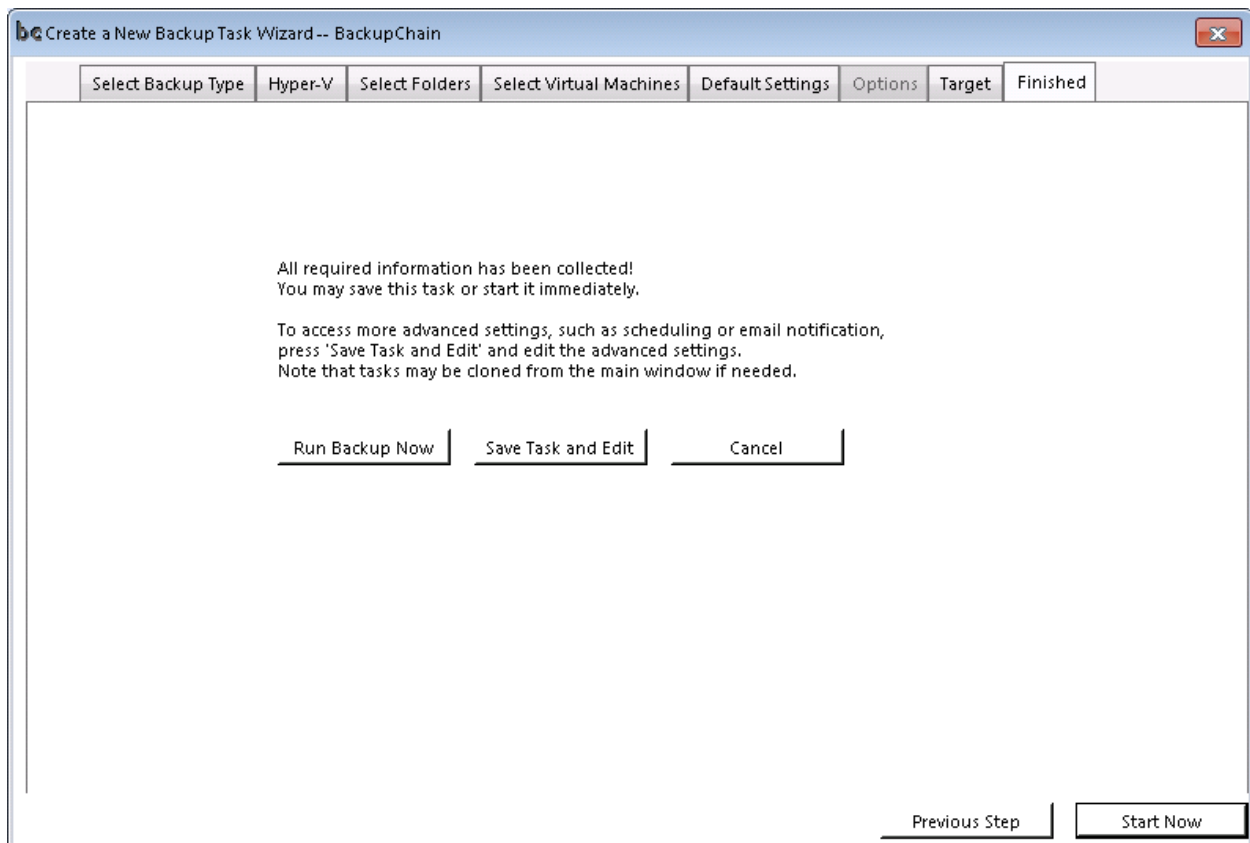
Here you can preset the basic settings of your task in just one screen, such as encryption, deduplication and data compression. All the fine-tuning may be done later in the Main Screen of BackupChain.

Now we are ready to proceed and set the backup target:



In our example above, we use a local drive but you could send your backups to a network device or FTP site instead as well. Note that deduplication does work over standard FTP.

Then click Next Step:

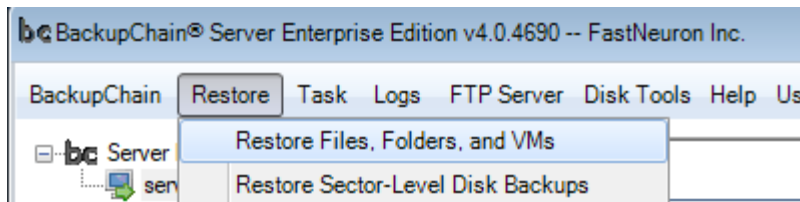


If you want to run the task immediately, click Start Now. Otherwise click Save Task and Edit, to return to the Main Screen where you can add a schedule to the task and change numerous other settings.

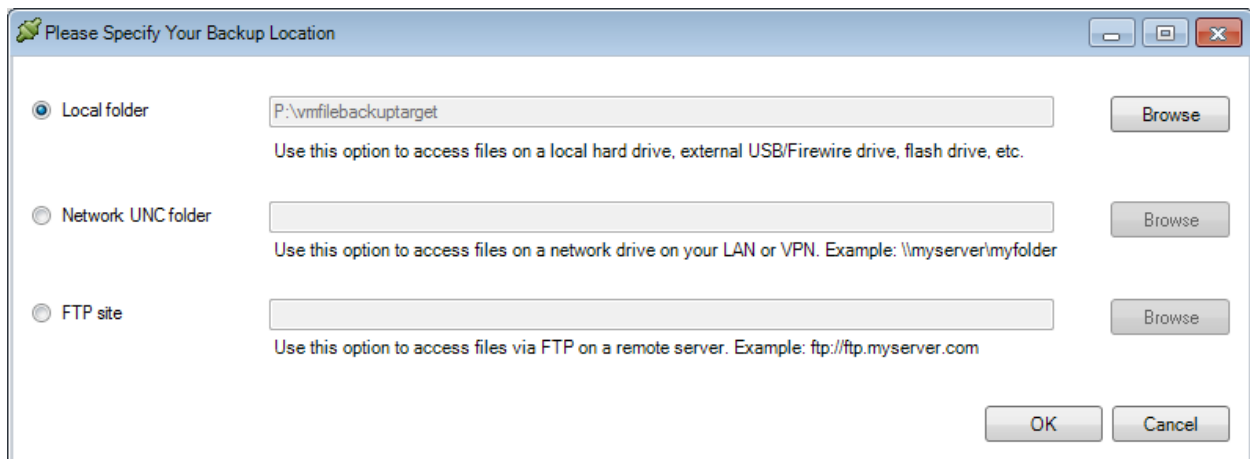
### Restoring Hyper-V VMs using the File-Based Method

To restore a Hyper-V virtual machine *using the standard file restore process*, select the backup task from the Backup Task List (unless restoring on a new machine) and select Restore from the main menu.

Proceed with Restore Files and Folders:

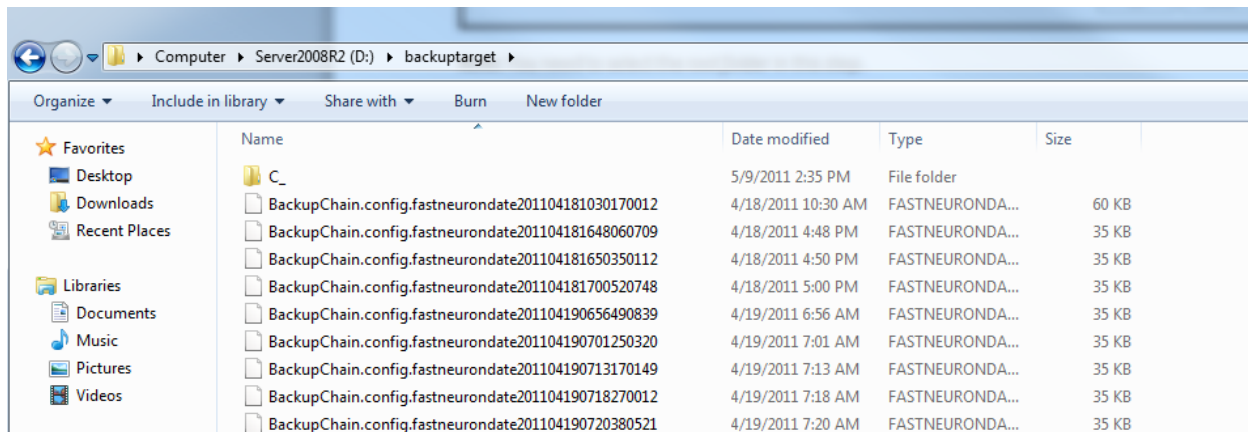


Then you need to fill in the details about the backup location. This information is usually preset with the task settings:



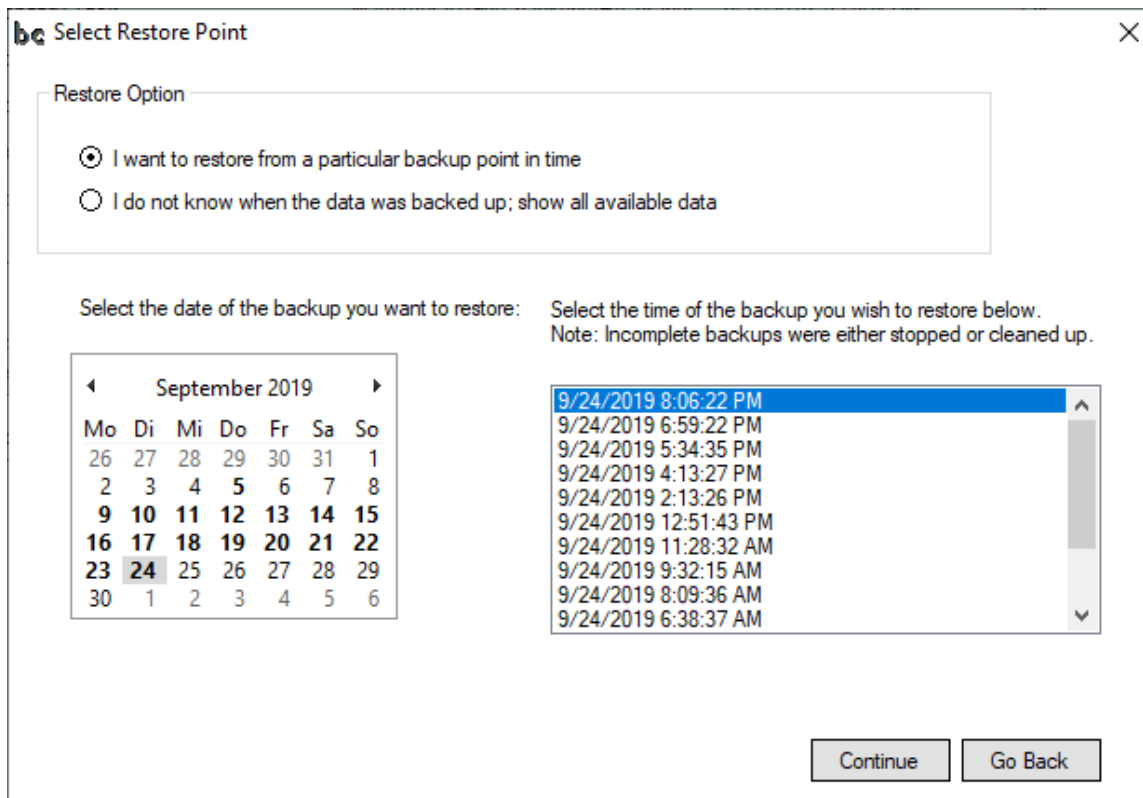
**Note:** You need to select the *root folder* in this step.

If you open the folder in Windows Explorer, the root folder may look like this:



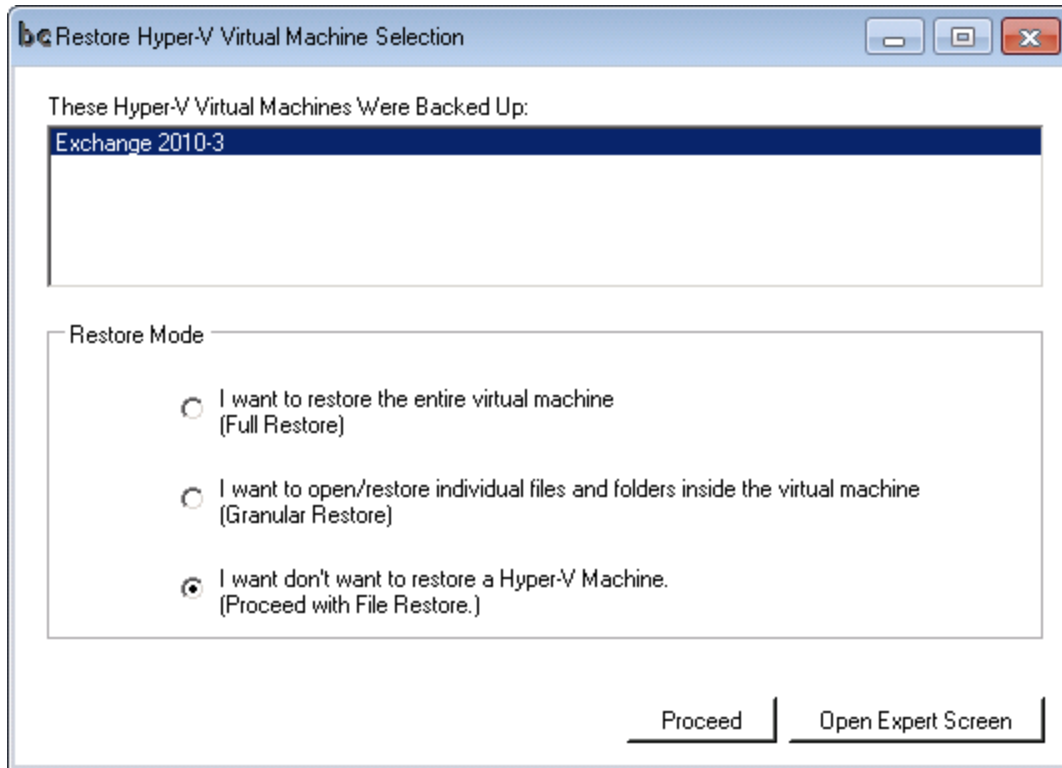
Notice the C\_ folder (for C: drive) and the BackupChain.config files. These files are necessary for restore operations.

Proceed and the backup set selection opens:

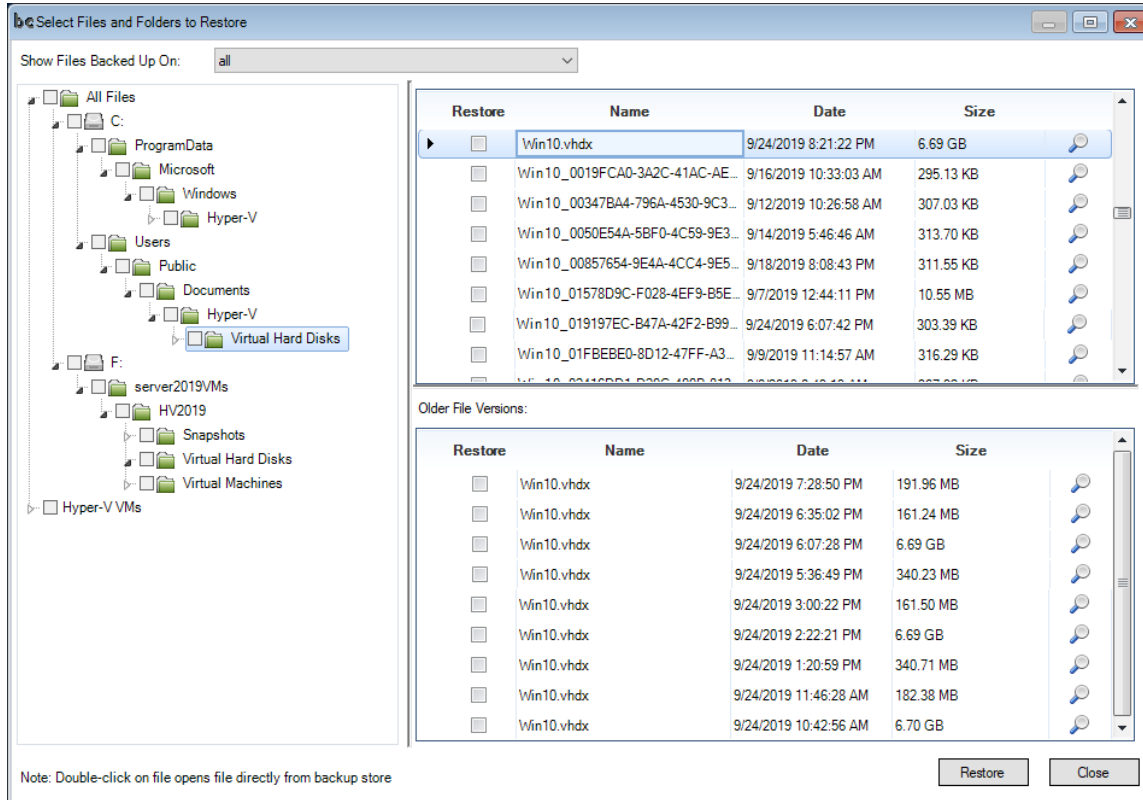


Either select “I do not know when the data was backed up” to obtain the full view of all existing backups, or select a particular day and time.

Once you select a restore point you will be presented with the option to automatically restore the entire Hyper-V virtual machine, the option to open Granular Restore (available only in BackupChain Server Enterprise Edition), or to proceed with File Restore. In this tutorial we choose File Restore:

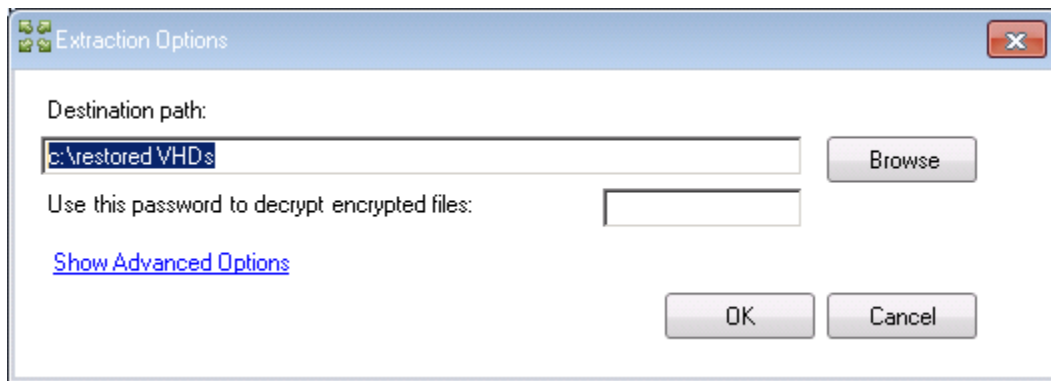


Proceed and click OK and the Restore Screen opens:



Navigate to the folder containing the virtual machine files and *check* the folder. This will restore all files within this folder as well as all subfolders. The restore process will restore the latest version of each file in the folder. The “latest version” is determined by the date filter at the top of the restore screen. Now proceed by clicking Restore.

If the virtual machine contains snapshots, you need to restore all the files to the same folder, such as C:\VHD. **WARNING:** Even though the default restore setting does not overwrite files without your permission, you still need to be careful not to overwrite files accidentally!



Click OK and let the restore process finish.

Now add a new Hyper-V machine via the Server Manager and connect to the existing virtual disk:

The screenshot shows the 'New Virtual Machine Wizard' window with the 'Specify Name and Location' step selected. The left sidebar lists the steps: 'Before You Begin', 'Specify Name and Location' (highlighted), 'Specify Generation', 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area contains instructions for naming and locating the VM. The 'Name' field is set to 'Restored VM'. The 'Location' field shows 'C:\ProgramData\Microsoft\Windows\Hyper-V\' with a 'Browse...' button. A warning icon and text advise selecting a location with enough free space for checkpoints. At the bottom, there are buttons for '< Previous', 'Next >' (highlighted), 'Finish', and 'Cancel'.

New Virtual Machine Wizard

**Specify Name and Location**

Before You Begin  
Specify Name and Location  
Specify Generation  
Assign Memory  
Configure Networking  
Connect Virtual Hard Disk  
Installation Options  
Summary

Choose a name and location for this virtual machine.


The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name:

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☐ Store the virtual machine in a different location

Location:

 If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

< Previous   Next >   Finish   Cancel

Try to assign the same or similar settings, such as number of CPUs and RAM, and start the machine.

Instead of creating a new virtual disk, select the one that BackupChain restored:

New Virtual Machine Wizard ✕

**Connect Virtual Hard Disk**

Before You Begin

Specify Name and Location

Specify Generation

Assign Memory

Configure Networking

**Connect Virtual Hard Disk**

Summary

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

☐ **Create a virtual hard disk**

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name:

Location:  Browse...

Size:  GB (Maximum: 64 TB)

☒ **Use an existing virtual hard disk**

Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location:  Browse...

☐ **Attach a virtual hard disk later**

Use this option to skip this step now and attach an existing virtual hard disk later.

< Previous

**Next >**

Finish

Cancel

## Automated, Single-Click Hyper-V Backup

The automated Single Click Backup & Restore feature for Hyper-V reduces the effort and takes care of all the steps outlined in the previous section.

Start with the Backup Wizard:

1. Create a new Hyper-V Backup (Server) task:

**Create a New Backup Task Wizard -- BackupChain**

Select Backup Type | Help | **Hyper-V** | Select Folders | Select Virtual Machines | Default Settings | Options | Target | Finished

**Welcome to BackupChain's Backup Task Wizard!**

This wizard guides you through the main functions of BackupChain and assists you in setting up a backup task. Backup tasks store all your settings for future use. Tasks may be scheduled or may be run manually whenever you need to run a backup. Once saved, you may fine-tune your backup task later in the Main Screen, where all features of BackupChain are available.

Create Task on Server: **backupchain-PC**

Enter a Task Name:

Please select the purpose of this backup task:

**I want to back up documents and file server data...**

☐ **File-Level Backup**  
(File Server and Version Backup. Use for file server data, documents, etc. Files are placed individually in backup folder. Do not use for VMs)

**I want to back up virtual machines...**

☒ **Hyper-V Backup (Server)** (Automatic or Granular Backup) ☐ **Hyper-V Backup (Client)** (File-based, recommended only for Windows 8-10 + Pro Edition) ☐ **VMware Backup** (VMware Workstation, Player, VMware Server backup) ☐ **VirtualBox Backup**

**I want to back up the Windows boot disk or sector-level backup...**

☐ **Disk to Image Backup (Sector-Level)** (Sector-based backup of a physical disk into a disk image file. This is usually only done to back up operating system disks) ☐ **Disk Cloning (Sector-Level)** (Sector-based copy of a physical disk to another physical disk. This can be used for Windows operating system boot disks as well as data disks) ☐ **Restore Disk Image Backup (Sector-Level)** (Restore a disk image file to a physical disk)

**I want to convert physical and virtual machines / disks...**

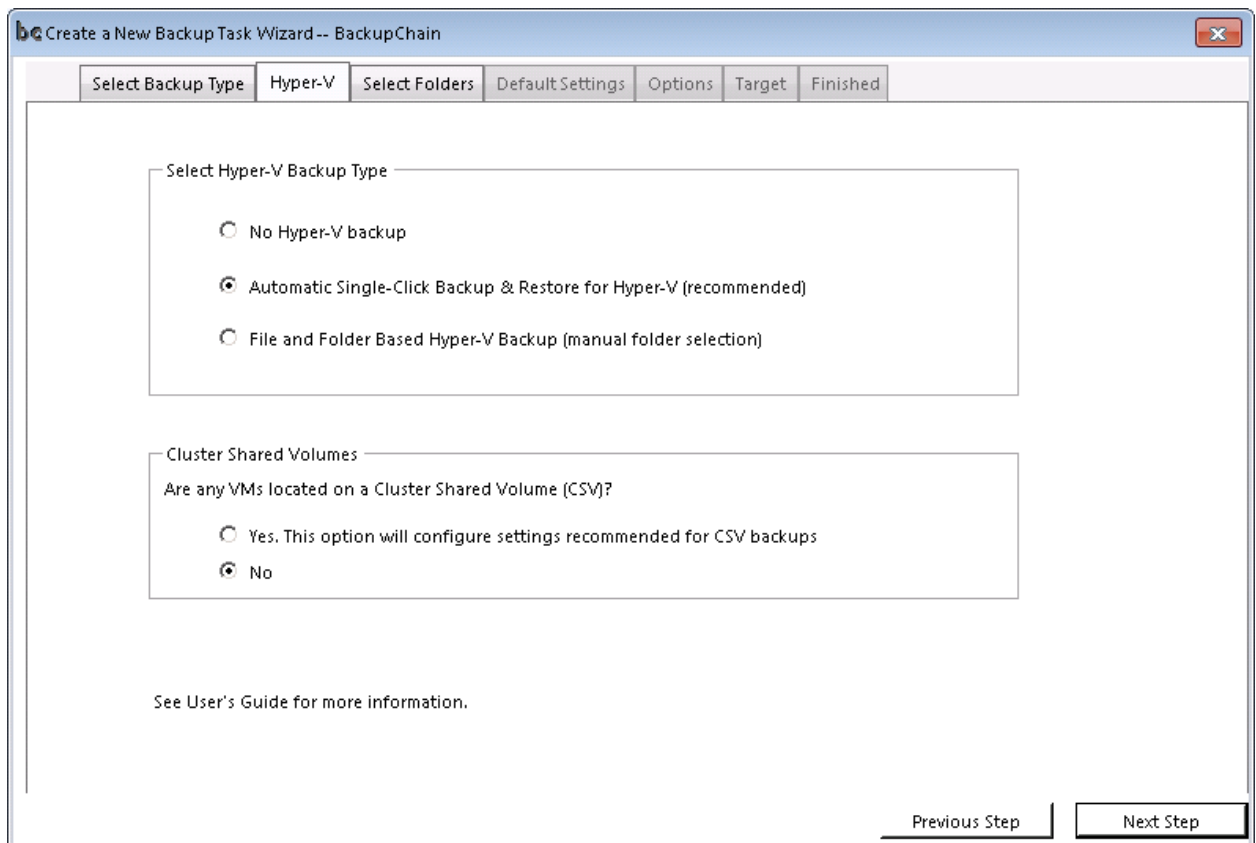
☐ **P2V** (Physical disk to virtual disk conversion) ☐ **V2P** (Virtual disk to physical disk conversion) ☐ **V2V** (Virtual disk format conversion)

**Other backup task types:**

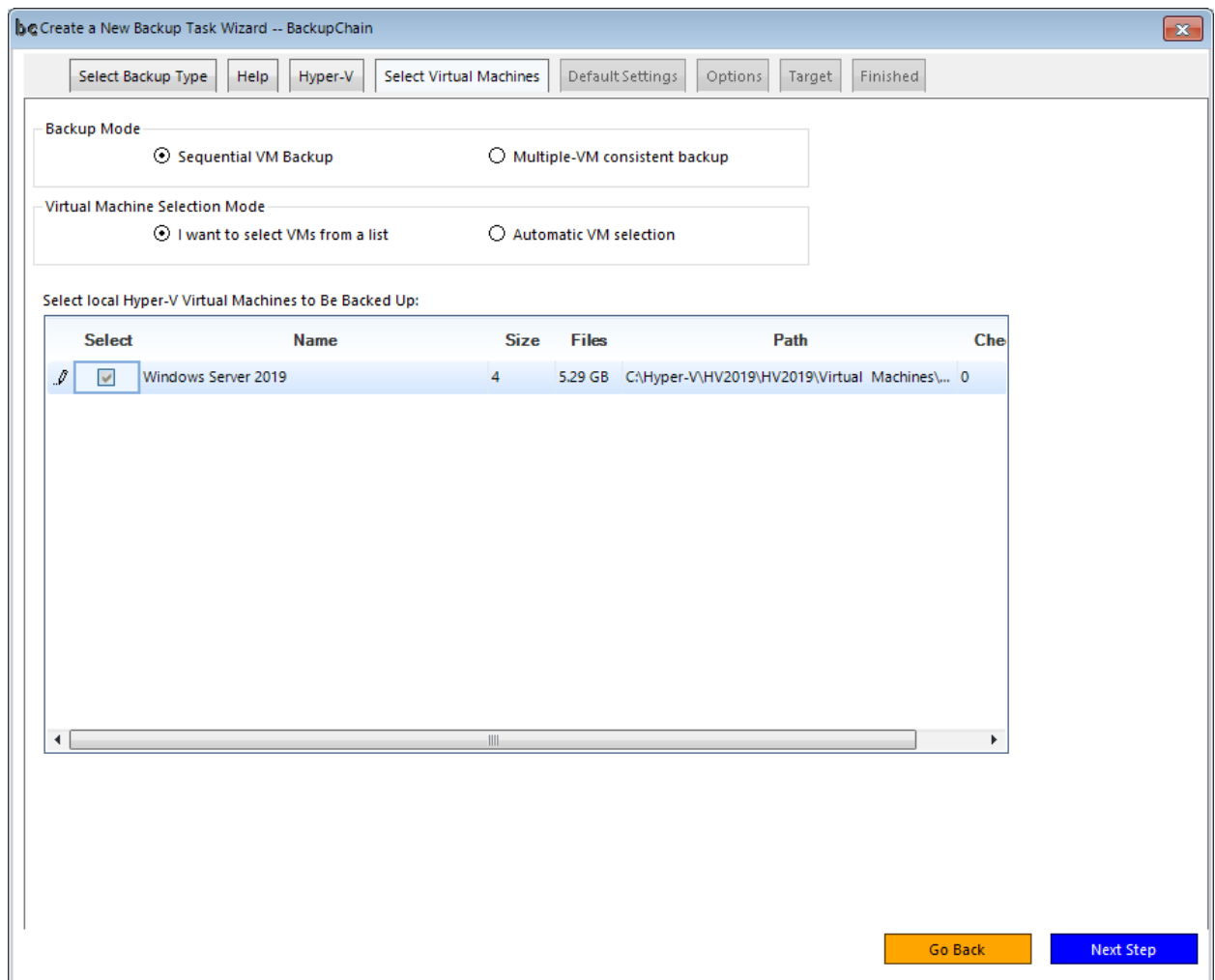
☐ **SQL Server Backup** (Backup SQL Server and MSDE Databases) ☐ **Universal Backup** (Backup all VSS aware services. Use only if no other backup type suits)

**Go Back** **Next Step**

2. Select Automatic Hyper-V Backup and turn on CSV mode in case you are using cluster shared volumes:



3. Then, you can either select the VM from a list or use the automatic select feature (note the option is checked “I want to select VMs from a list”):



Alternatively you can use “Automatic VM Selection” in Server Enterprise editions and higher:

Create a New Backup Task Wizard -- BackupChain

Select Backup Type | Help | Hyper-V | Select Virtual Machines | Default Settings | Options | Target | Finished

**Backup Mode**

☒ Sequential VM Backup ☐ Multiple-VM consistent backup

**Virtual Machine Selection Mode**

☐ I want to select VMs from a list ☒ Automatic VM selection

**Automatic VM Selection Settings**

This feature is enabled in these editions: Server Enterprise (this trial version) and Platinum

☒ Back up all virtual machines running on this host  
(All VMs will be backed up. Filter options below are optional)

☐ Include only VMs with this text in their name:  
(Do not use \* char.; use one line for each filter)

☐ Exclude VMs with this text in their name:  
(Do not use \* char.; use one line for each filter)

☐ Do NOT back up replica VMs

☐ Do NOT back up VMs that are shut down

☐ Wait for VM if it is being backed up by another task (avoid backing up the VM twice at the same time)

☐ Log a warning if no VMs are selected for backup

Go Back Next Step

The above screens require no additional configuration if you want all VMs backed up automatically. You can specify inclusion and exclusion filters based on name.

For example, you could set up the following naming convention in your company. If a VM name contains the word 'Production', it's a production VM and it will be always backed up. In that case you would add the word Production as inclusion filter above.

Or you could define an exclusion filter to work like this: Let's say you want all VMs that use the word "Testing" or "Do not back up" skipped. You would then define an exclusion filter with two lines, one for Testing and one for "Do not back up", without entering the quotes.

The option "Do NOT back up replica VMs" prevents replica VMs from being backed up. This is useful when you are already backing up at the replica target VM separately and want to keep the server load to a minimum.

The option “Wait for VM” is there to cover the circumstance where a VM cannot be backed up in parallel. Note that services inside the VM have to participate in order to obtain an application consistent backup of the VM. Some services may place exclusive locks inside their internal data structures that may prevent parallel simultaneous backups from running. The wait option, hence, recognizes that a VM is being backed up and waits for it to complete before proceeding.

**Note:** the option “Do NOT back up VMs that are shut down” can lead to data loss. Consider the case where a VM is always backed up while running. At some point it’s shut down and the backups no longer include that VM. The changes since the last backup would be lost if the VM becomes damaged.

“Log a warning if no VMs are selected for backup” is an option to protect you from undesired configurations. For example, a typo in the inclusion filter may result in no VMs being recognized and hence no VMs being backed up. A warning is then logged to alert you to that possibility. You can switch this option off, for example, if hosts often have all of their VMs moved off for maintenance and you don’t wish to receive warnings in that case.

### *Sequential VM Backup vs. Multiple-VM Consistent Backup*

It’s important not to use the simultaneous option unless it’s absolutely necessary. There is usually no speed gain from using this option. The default option is to back one VM at a time, whereas the simultaneous option backs up all VMs simultaneously. Obviously the load on your server will be much higher when a simultaneous backup is performed. **The simultaneous option should only be used if you need a consistent backup across multiple virtual machines.** This is usually only the case if you have several database servers linked together, or a similar setup that requires data consistency across several virtual machines.

**Important:** Selecting “Sequential VM Backup” is the recommended option and reduces the load on your server but takes longer to complete. This option remains checked when using a Universal Backup task; conversely, it can only be unchecked when the task was created as a Hyper-V Backup task type.

You can proceed with the Backup Wizard with standard or custom options as discussed in earlier chapters and complete the task.

### *Cluster Shared Volumes*

Cluster Shared Volume backups are fully supported in BackupChain Server Edition and Server Enterprise Edition.

**It is recommended to limit read and write I/O speeds or to use separate network adapters for backup traffic, in order to keep the server network balanced.**

You may need to use the domain administrator account for your iSCSI provider service in order to get the backup task to start successfully, depending on the iSCSI service you are using.

For live backups with VSS engagement (the recommended way to back up), you need to run BackupChain on the cluster node that actually hosts the VM you want to back up. You could back up virtual machines from another node as well using the file-based approach (discussed in previous section) but that approach “from a distance” does not involve VSS and hence will only give you a crash consistent live backup. A crash consistent backup is similar to a power loss event in a physical machine. Most production grade applications can handle a power loss event without data loss, such as a SQL Server database server. To achieve an application consistent live backup which will also notify the VM internally of the backup event, you need to run the backup on the same node that hosts the virtual machine you wish to back up. Application consistent backups require the VSS integration and this integration can only be managed from the VM’s host. VSS aware applications, such as database services and Exchange, prepare for live backup, flush their caches, and bring their file stores into a consistent state before the backup begins.

Do not perform a live migration while a backup is running because live backups cannot be processed when a VM switches hosts. Also, you need to configure BackupChain on the new cluster node when you reassign virtual machines to new hosts (select VM in Hyper-V tab table or use the Automatic VM Selection feature).

Note: On older Windows Server (pre 2012) operating systems you need to schedule CSV backups to run without overlaps because CSVs do not allow nodes to back up simultaneously.

### **General CSV Characteristics**

You cannot back up VMs running on another node, even if they share the same storage on a SAN.

Application consistent backups require backup software to run locally on the node that hosts the VM.

### **Windows Server 2008 and R2 Specifics**

- You may only run one backup across all nodes of an entire cluster shared volume.
- You can back up several VMs simultaneously; however, these must be running on the same node. In other words, do not overlap backups running on several nodes simultaneously. You need to schedule them to run without overlap.

### **Windows Server 2012 and Later Specifics**

- Do not add local or other CSV paths to a backup task.
- You must select a Hyper-V Backup task type in the task wizard. You cannot use Universal Backup task types to back up CSV VMs.

### *Dealing With VM Migrations (Live, Manual, Automatic / CSV)*

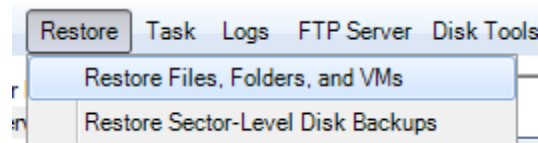
Beginning with Version 4, BackupChain offers an Automatic VM Selection feature. By standardizing the names of your VMs, you can define filters to include or exclude VMs automatically from backups.

For example, if you only want production VMs backed up, you could use a suffix in the VM name, like this: Exchange\_Server\_Production. The ending “\_Production” can be used as an inclusion filter in the backup task’s Hyper-V tab so that BackupChain picks up that VM automatically. Likewise, you could define an exclusion filter to avoid backing up VMs that are for testing only, by calling the VM Exchange\_Test and defining an exclusion filter having the text: \_Test

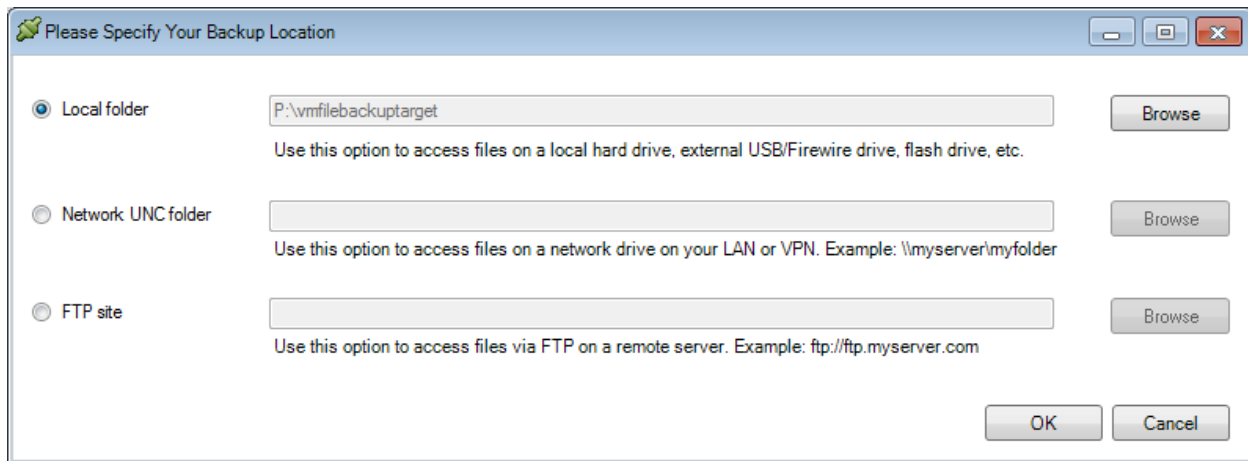
By using the Automatic VM Selection feature, you no longer have to update backup configurations when VMs move. Note there is a warning option at the bottom of the Hyper-V tab that will cause BC to log a warning if no VMs were found. This is a safety feature to avoid the situation where filters may be set incorrectly by accident and no VM ends up being selected. Because there are legitimate scenarios when this can occur, such as when all VMs are moved off the server for maintenance, you can decide to turn off that feature, after you have confirmed that VMs are selected for backup as desired.

### *Restoring VMs*

To restore using the Single-Click Backup & Restore, select the backup task from the Backup Task List (unless restoring on a new machine) and select Restore from the main menu. Proceed with Restore Files and Folders:

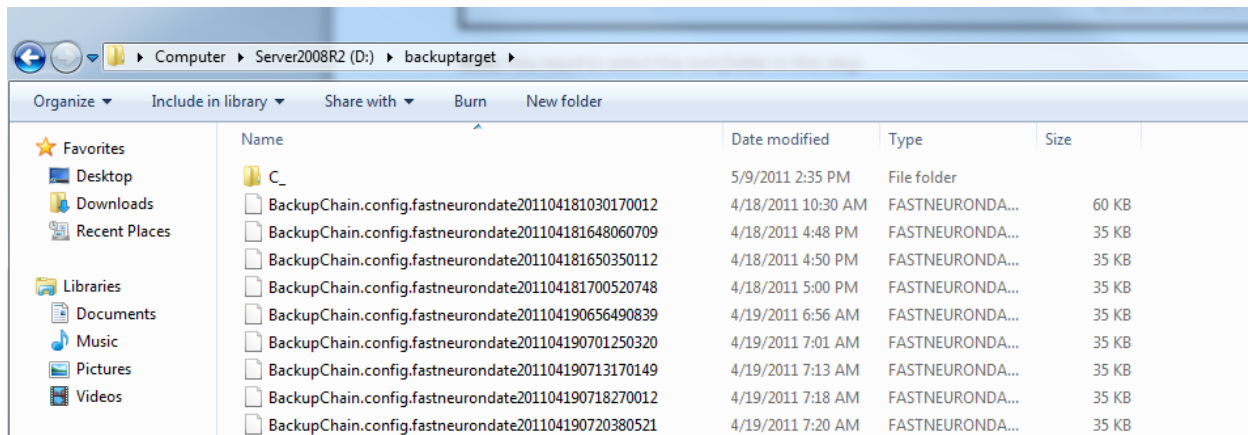


Then you need to fill in the details about the backup location. This information is usually preset with the task settings:



**Note:** You need to select the *root folder* in this step.

If you open the folder in Windows Explorer, the root folder may look like this:



Notice the C\_ folder (for C: drive) and the BackupChain.config files. These files are necessary for restore operations.

Proceed and click OK and the Restore Point Selection Screen opens:

Select Restore Point

Restore Option

☒ I want to restore from a particular backup point in time  
☐ I do not know when the data was backed up; show all available data

Select the date of the backup you want to restore:

Select the time of the backup you wish to restore below.  
Note: Incomplete backups were either stopped or cleaned up.

September 2019

Mo	Di	Mi	Do	Fr	Sa	So
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

9/24/2019 9:52:04 PM (Complete)

9/24/2019 8:40:41 PM (Complete)  
9/24/2019 8:05:37 PM (Complete)  
9/24/2019 7:02:59 PM (Complete)  
9/24/2019 6:28:25 PM (Complete)  
9/24/2019 6:00:06 PM (Complete)  
9/24/2019 5:05:52 PM (Complete)  
9/24/2019 2:44:27 PM (Complete)  
9/24/2019 2:07:34 PM (Complete)  
9/24/2019 1:10:53 PM (Complete)

Loading backup list..

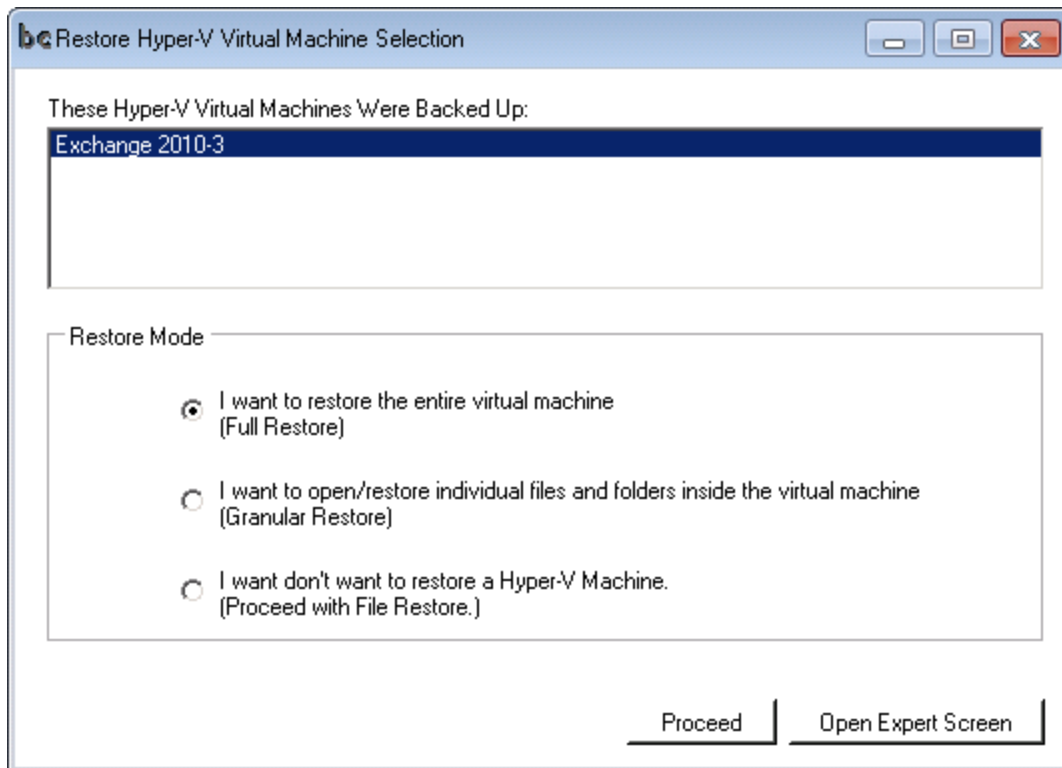
The oldest restorable VM backup is dated: 9/24/2019 1:10 PM

Continue

Go Back

While all backup restore points are being read, the screen will update and show the oldest fully restorable VM backup (shown in orange above). Prior backups might be partially restorable, depending on your backup settings. On the right, the selected day and time shows “(Complete)” when the backup was successful and all files were found in the backup folder.

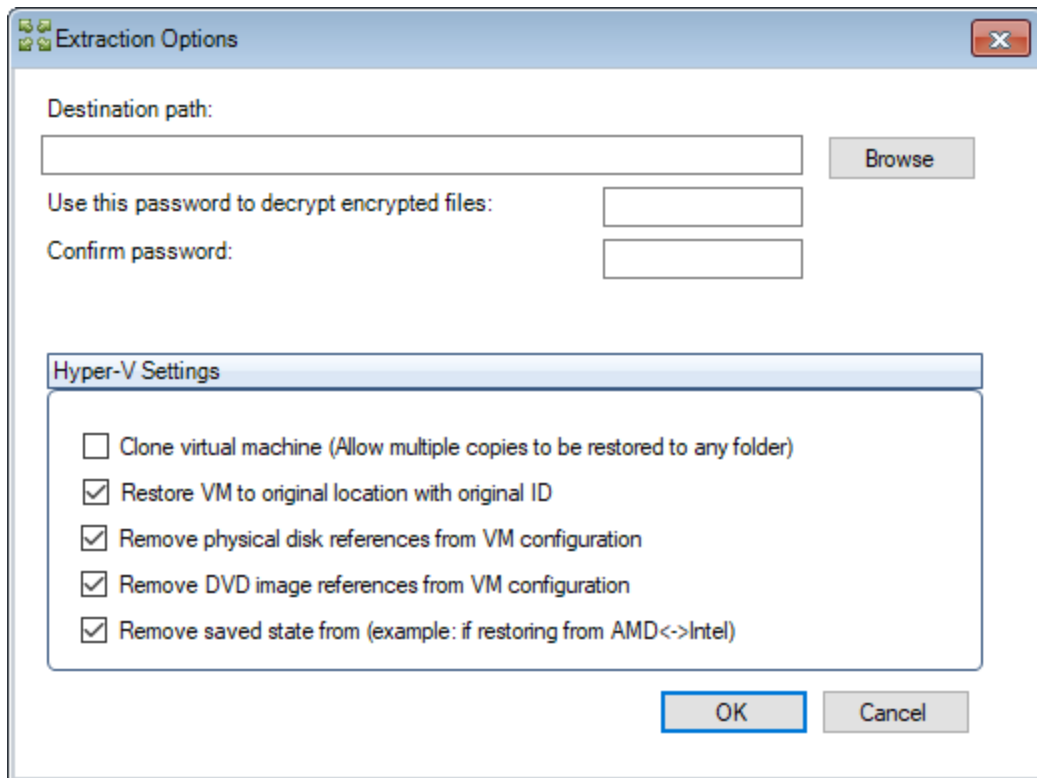
Please select the restore point and proceed. From the virtual machine selection screen, select the virtual machine you want to restore and leave the Full Restore option selected. If you want to restore just a subset of a virtual machine, such as a folder or a file from inside the VM, you need to select Granular Restore. Note: Granular Restore is only available in BackupChain Server Enterprise Edition.



**Case #1: We want to restore to the original location, and we want the VM to have the original identity.**

**Important Note: You must delete the original VM by hand before you proceed, if you are restoring the original VM identity. VM clones can be restored side-by-side with the original (see case #2 below).**

In the extraction options select "Restore files to their original location" in Miscellaneous Settings and check "Clone virtual machine" in Hyper-V Settings:



And we are ready to go. **Note the destination path is kept empty and the option “restore VM to original location is checked.**

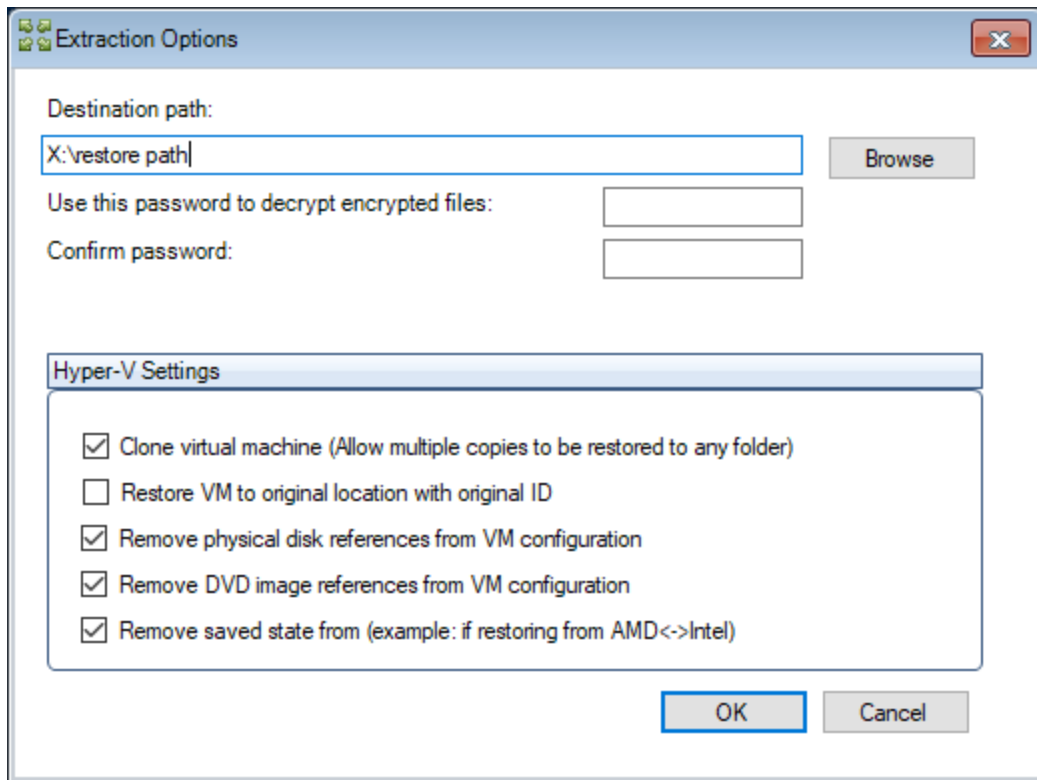
Notice that the option “Clone virtual machine” in Hyper-V Settings should always be checked in order to create a new identity. You can re-create the original identity as well and it makes sense to do so if the VM was deleted or if you are restoring to a new server.

**Note:** If your VM was originally saved directly in C:\ProgramData\Microsoft\Windows\Hyper-V\Virtual Machines, you must restore it to a new location, such as C:\RestoredVMs. It is generally not recommended to create virtual machines in the “default” folder; rather, create a new folder for virtual machine data, ideally on a separate drive for better performance.

**Note:** Restoring to a cluster shared volume is supported; however, you need to add the VM manually to the Failover Cluster Manager. The VM will appear automatically in the Hyper-V Manager instead.

#### **Case #2: Restore with a new identity but to a new, separate folder.**

Follow the same step as above but specify a target folder and ensure the option select “Restore files to their original location” in Miscellaneous Settings remains unchecked.



If you uncheck the 'clone virtual machine' option, the VM will be restored using its original identity. Ensure the original VM is no longer on the network to prevent computer name clash.

### *Starting the machine*

The restored machine should appear in the Server Manager's Hyper-V role screen. If it doesn't, refresh the screen or right click on the Hyper-V Manager and stop the management service. This doesn't affect running virtual machines and you can start again as soon as it stops.

Once the new machine appears you may want to review and update the virtual machine network connection settings. **The network connection is removed** to avoid network IP and computer name clashes when the VM is restored on the original server. You can always add the network controller back to the VM without rebooting the VM at any time. You may also want to allocate a new MAC address for the cloned VM but it may not be necessary if dynamic allocation is being used on your host.

**Note:** When powering up a restored VM, if you receive a "Windows has not been shut down correctly" it's because the "booted" flag hasn't been cleared from the hard disk image. Be assured that the VM is in a good condition.

## Windows 10 Hyper-V Backup and Restore using the Professional Edition

Backup of Windows 8 and Windows 10 Hyper-V VMs is identical to the file-based approach for Hyper-V Backup on Servers.

### Backup

Note that it is possible to use the Server Editions of BackupChain on Windows 10 and use the Automatic Hyper-V Backup features discussed in previous sections. However, for typical PC-usage, such as for development and testing, the Professional edition offers a wide range of features to get the job done well.

Note that you can only back up live virtual machines when they are stored locally. Live backup does not work over the network (only exception SAN and CSV backups); this means you cannot *pull* VMs stored on another server. VMs must be running locally in order to be backed up live. Offline backups (when VMs are shut down) do work over the network, however, when accessed via a UNC path.

1. Open the New Backup Wizard and create a new “Hyper-V Backup (**Client**)” task using the New Task button:

**bc Create a New Backup Task Wizard -- BackupChain**

Select Backup Type | Help | Hyper-V | Select Folders | Select Virtual Machines | Default Settings | Options | Target | Finished

**Welcome to BackupChain's Backup Task Wizard!**

This wizard guides you through the main functions of BackupChain and assists you in setting up a backup task. Backup tasks store all your settings for future use. Tasks may be scheduled or may be run manually whenever you need to run a backup. Once saved, you may fine-tune your backup task later in the Main Screen, where all features of BackupChain are available.

Create Task on Server: **backupchain-PC**

Enter a Task Name: **Windows 10 Hyper-V VM Backup**

Please select the purpose of this backup task:

**I want to back up documents and file server data...**

☐ **File-Level Backup**  
(File Server and Version Backup.  
Use for file server data, documents, etc.  
Files are placed individually in backup folder.  
Do not use for VMs)

**I want to back up virtual machines...**

☐ **Hyper-V Backup (Server)**    ☒ **Hyper-V Backup (Client)**    ☐ **VMware Backup**    ☐ **VirtualBox Backup**  
(Automatic or Granular Backup)    (File-based, recommended only for Windows 8-10 + Pro Edition)    (VMware Workstation, Player, VMware Server backup)

**I want to back up the Windows boot disk or sector-level backup...**

☐ **Disk to Image Backup (Sector-Level)**    ☐ **Disk Cloning (Sector-Level)**    ☐ **Restore Disk Image Backup (Sector-Level)**  
(Sector-based backup of a physical disk into a disk image file. This is usually only done to back up operating system disks)    (Sector-based copy of a physical disk to another physical disk. This can be used for Windows operating system boot disks as well as data disks)    (Restore a disk image file to a physical disk)

**I want to convert physical and virtual machines / disks...**

☐ **P2V**    ☐ **V2P**    ☐ **V2V**  
(Physical disk to virtual disk conversion)    (Virtual disk to physical disk conversion)    (Virtual disk format conversion)

**Other backup task types:**

☐ **SQL Server Backup**    ☐ **Universal Backup**  
(Backup SQL Server and MSDE Databases)    (Backup all VSS aware services. Use only if no other backup type suits)

**Go Back**    **Next Step**

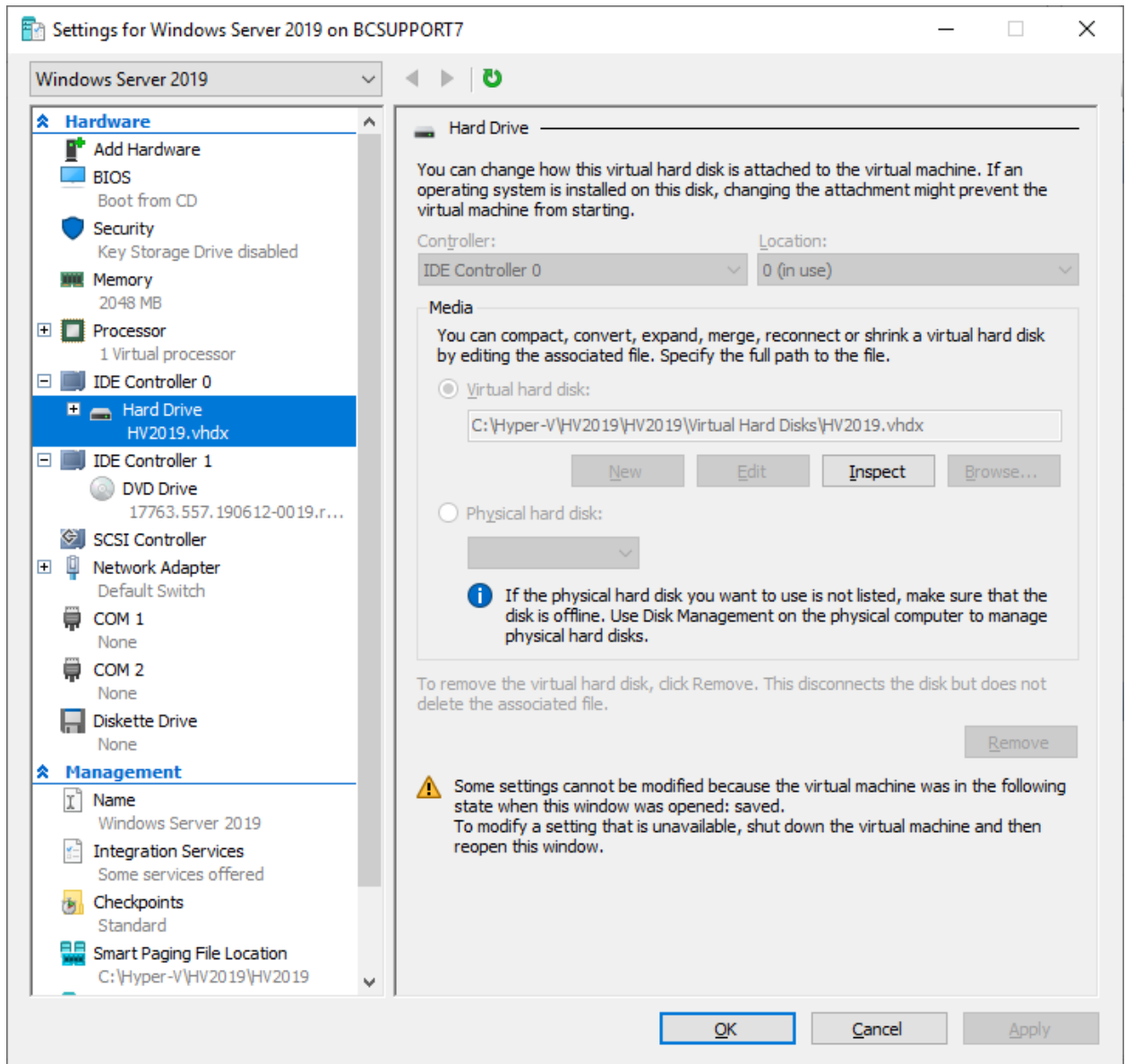
2. Select the folder containing the virtual machine files (VHDs, and Virtual Machine and Snapshots folders)



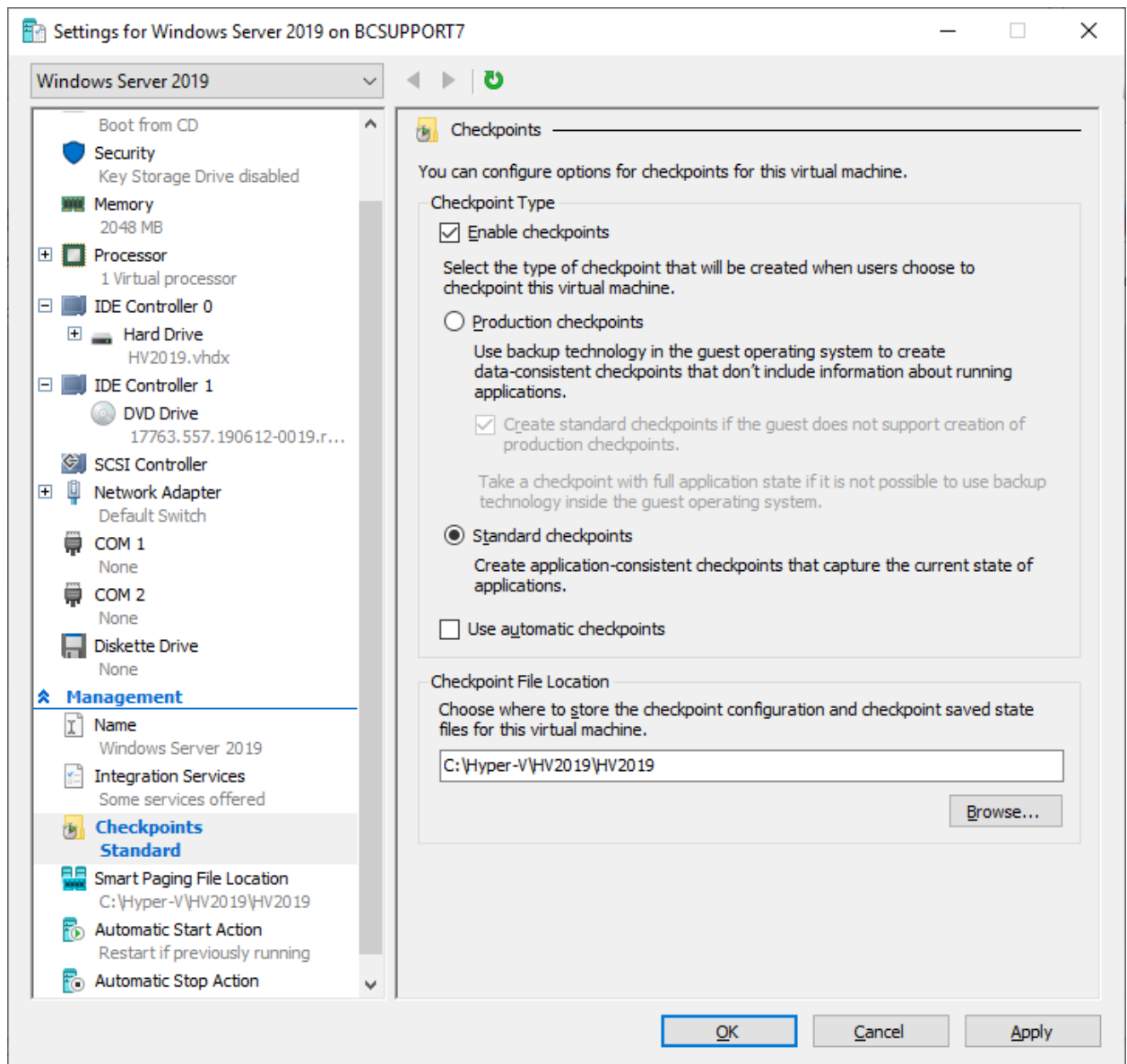
Note: You cannot pull files over the network. VMs must be installed locally or on a CSV in order for live backup to work.

### *Where are the VM files located?*

If you are not certain where the VM files are stored, you can check the VM's settings in Hyper-V:



At a minimum, you need to include the VM folder containing the virtual disk (see C:\Hyper-V\HV2019... folder above) and the check point folder in the "Checkpoints" section:



Both the checkpoint and virtual disk folders are usually inside the same subfolder created for the VM, unless you did not specify a folder when you created the VM.

In that case the VM is on drive C: (not a recommended practice but works) and stored in the already preselected default folders:

C:\ProgramData\Microsoft\Windows\Hyper-V and C:\Users\Public\Documents\Hyper-V

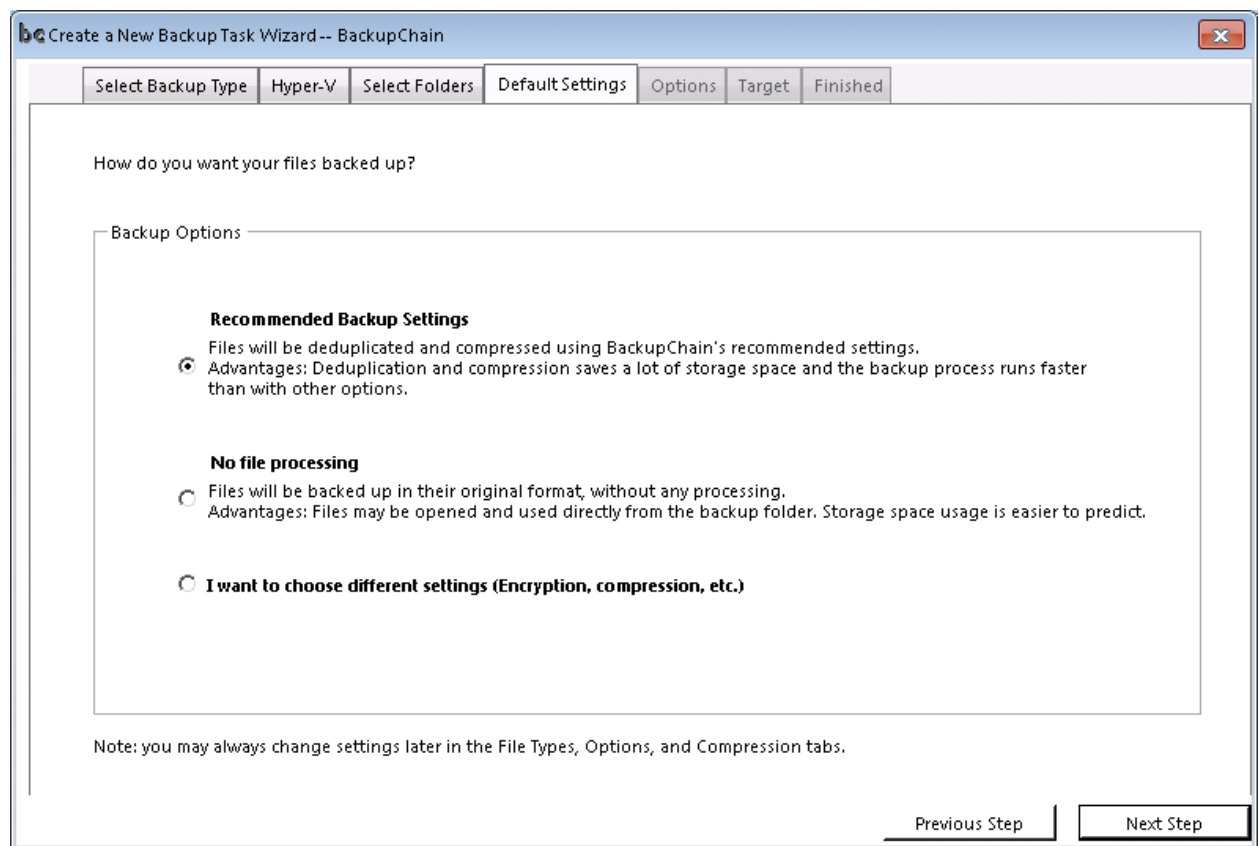
For simpler VM management purposes, as well as for better performance, it's recommended to set a dedicated folder for each VM on a separate drive, ideally a separate physical disk or disk array. The use of checkpoints is not recommended but as long as you include the folder in the BackupChain backup configuration, they will be backed up as well. If your VM is stored in the default folders (the two listed above), the checkpoints will also be stored in there. If you created

a dedicated folder when creating the VM, all VM-related files will be within it and you have all files nicely in one folder.

*It's not required for backup purposes but if you wish to change the VM configuration from default folders to a dedicated folder, please proceed as follows:*

- *Delete any checkpoints that may exist. Check the Hyper-V Manager status for the VM and wait until the VM status is clear, if necessary.*
- *Create a new VM with similar settings as the original*
- *Create the dedicated folder and move the VM's VHDs into it*
- *For each VHD that exists, add a virtual disk to the VM and point it to the VHD in the dedicated folder*
- *Remove the old VM (optional) and boot the new one.*

Next, accept default settings or use custom settings:



Recommended backup settings will turn on deduplication, data compression, and a retention period of 10 file versions (i.e. after the 11<sup>th</sup> backup of a file the oldest backup is deleted).

“No file processing” switches off deduplication and data compression and uses a retention period of 10 file versions.

If you choose custom settings the following screen opens:

**Create a New Backup Task Wizard -- BackupChain**

Select Backup Type | Hyper-V | Select Folders | Default Settings | **Options** | Target | Finished

Please choose among the following options. These are minimum settings to get you started. More advanced settings can be specified later if necessary.

**Deduplication**

☒ On ☐ Off

**Compression Settings**

☐ No Compression (Usually slower)  
☒ Fastest Compression  
☐ Standard Compression  
☐ High Compression (Slower)

**Resource Usage**

☐ Maximum Speed (Uses more resources and RAM)  
☒ Minimal System Impact (Slower)  
☐ Reduce Hard Drive Stress (Slowest)

**Automatic Cleanup**  
 Keep this many backups of each file in the backup store:  
 Enter a number or ALL to keep all file changes.  
 A setting of 10 will keep up to 10 backups of each file

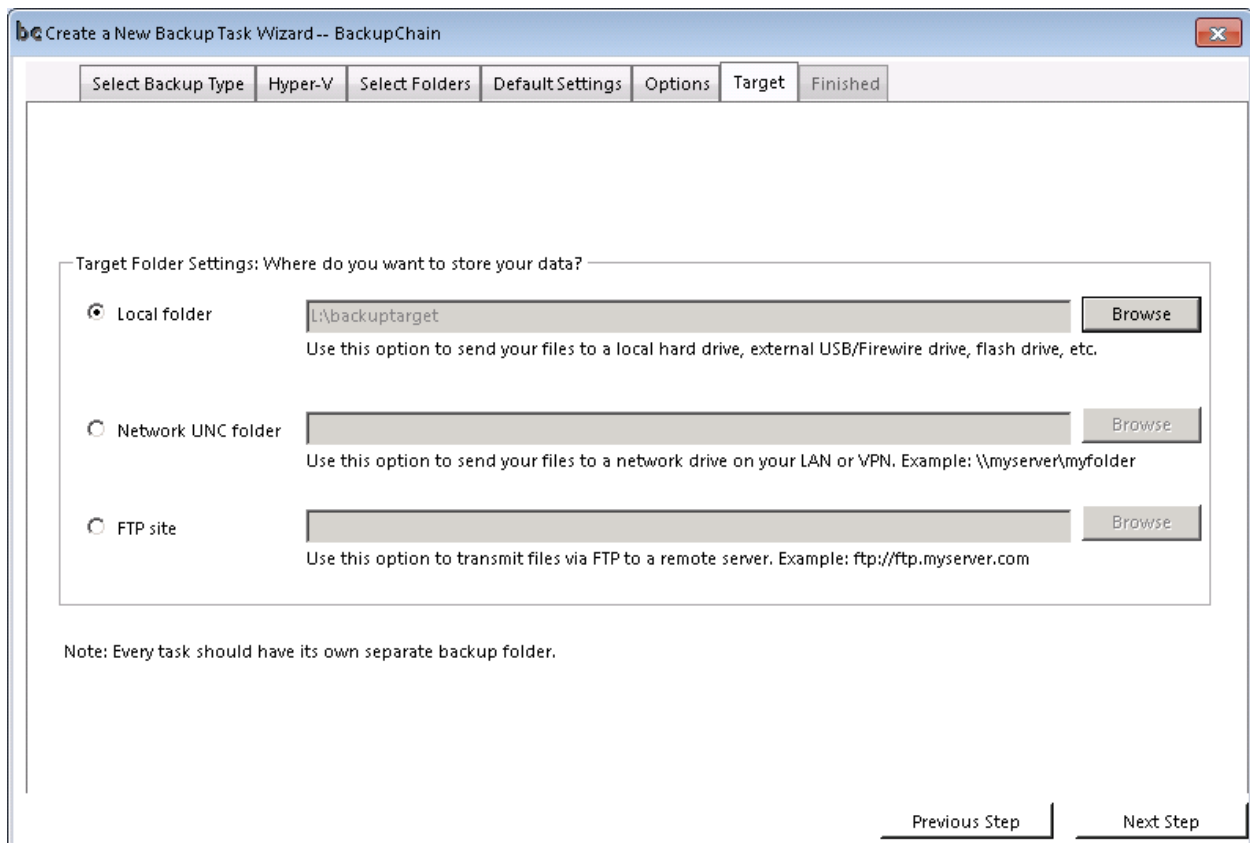
☐ Encrypt files with military strength encryption (AES 256, HIPAA compliant)

Password:  Confirm password:

[Previous Step](#) [Next Step](#)

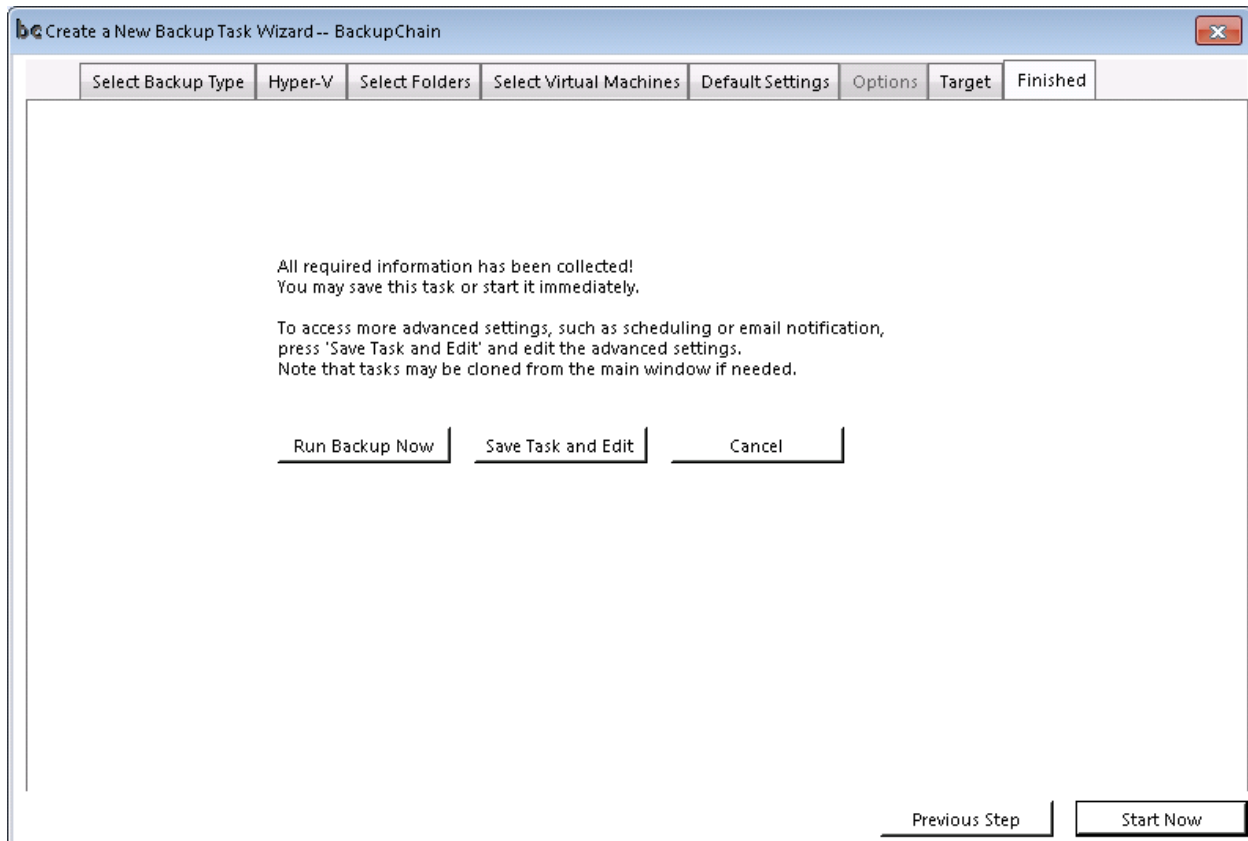
Here you can preset the basic settings of your task in just one screen, such as encryption, deduplication and data compression. All the fine-tuning may be done later in the Main Screen of BackupChain.

Now we are ready to proceed and set the backup target:



In our example above, we use a local drive but you could send your backups to a network device or FTP site instead as well. Note that deduplication does work over standard FTP.

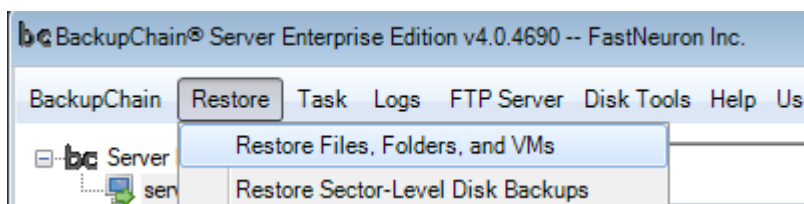
Then click Next Step:



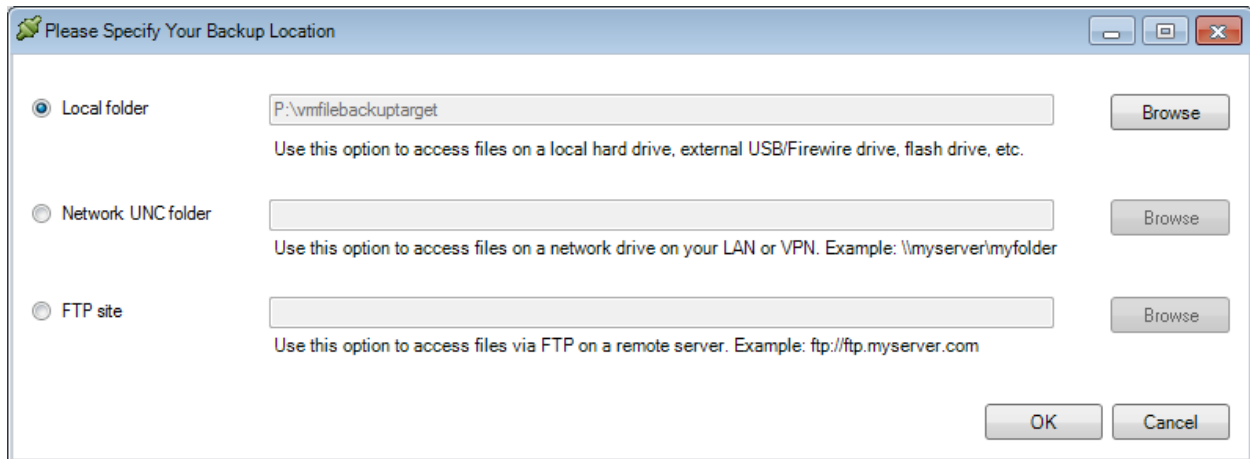
If you want to run the task immediately, click Start Now. Otherwise click Save Task and Edit, to return to the Main Screen where you can add a schedule to the task and change numerous other settings.

### *Restoring Hyper-V VMs running on Windows 10 hosts using the Professional Edition*

To restore a Hyper-V virtual machine *using the standard file restore process*, select the backup task from the Backup Task List (unless restoring on a new machine) and select Restore from the main menu. Proceed with Restore Files and Folders:

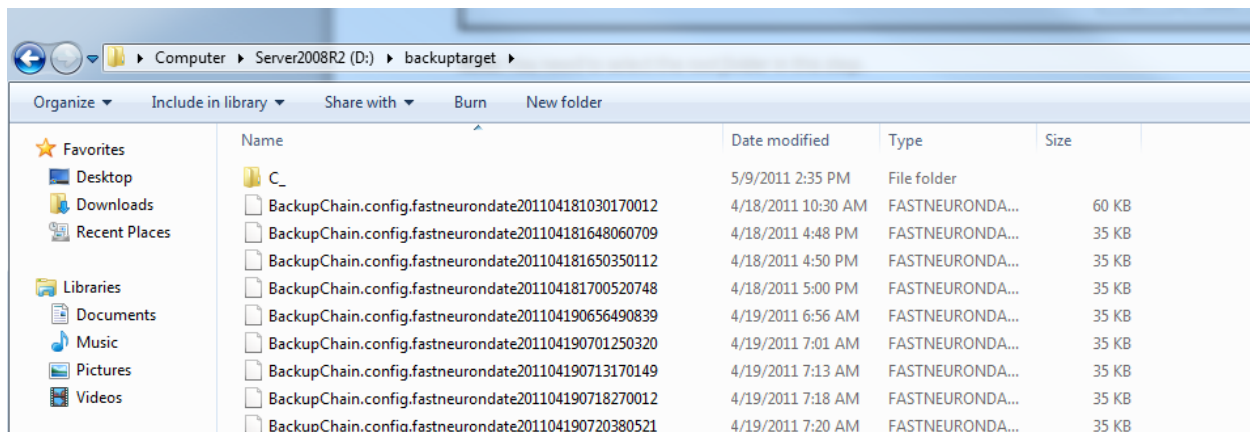


Then you need to fill in the details about the backup location. This information is usually preset with the task settings:



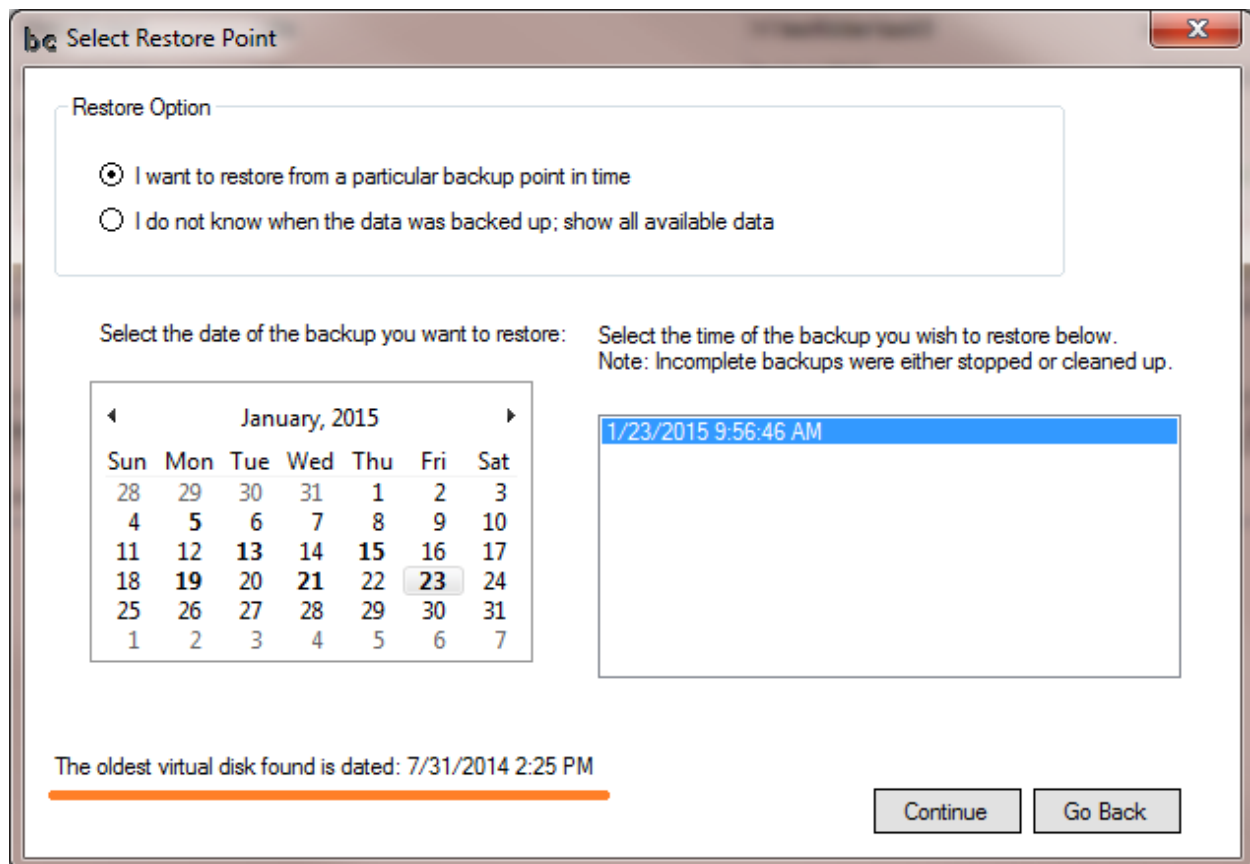
**Note:** You need to select the *root folder* in this step.

If you open the folder in Windows Explorer, the root folder may look like this:



Notice the C\_ folder (for C: drive) and the BackupChain.config files. These files are necessary for restore operations.

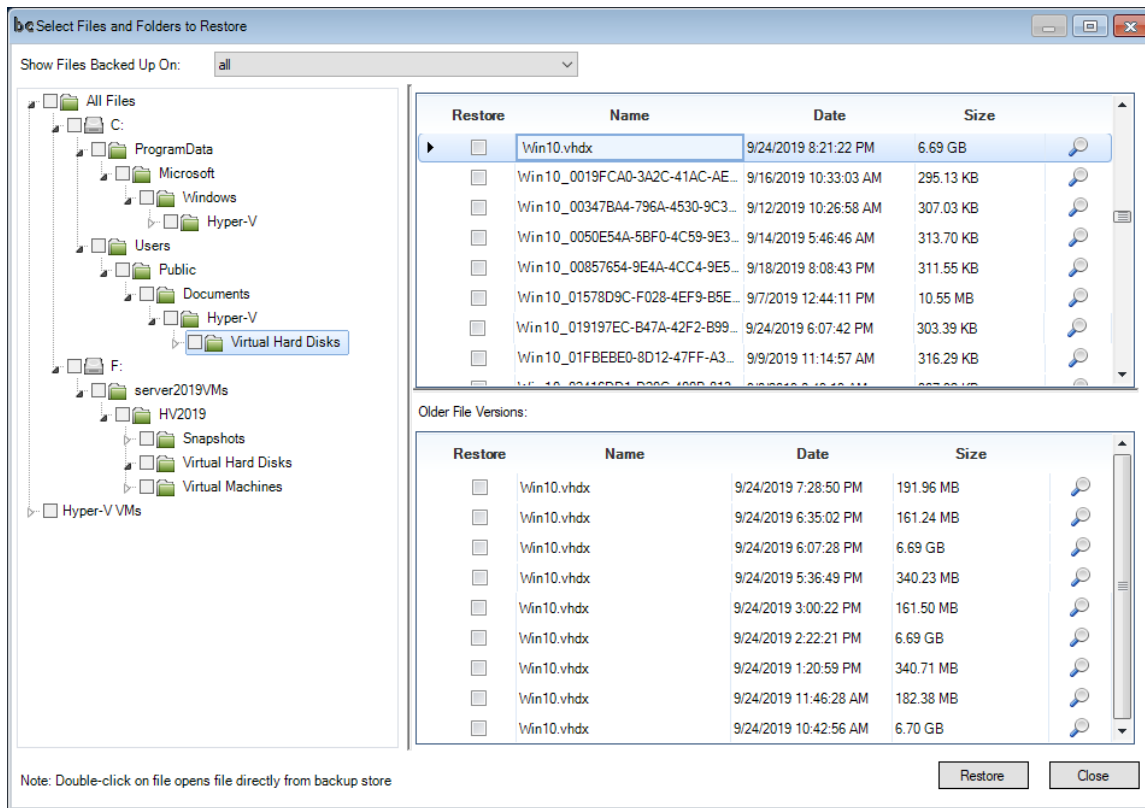
Proceed and the backup set selection opens:



Note that BackupChain will scan in the background all available restore points. It will look for the oldest virtual disk that is available and display the date (see above in orange). Depending on your backup settings, there may be restorable backups from before that, but the date displayed, once the scan is complete, shows the backup date of the oldest virtual disk found, which is the oldest fully restorable backup.

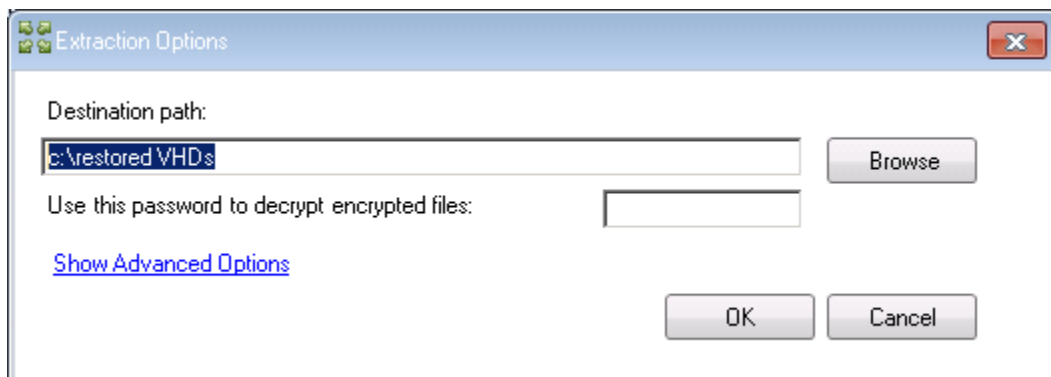
Either select “I do not know when the data was backed up” to obtain the full view of all existing backups, or select a particular day and time.

Proceed and click OK and the Restore Screen opens:



Navigate to the folder containing the virtual machine files and **check the entire folder**. This will restore all files within this folder as well as all subfolders. The restore process will restore the latest version of each file in the folder. The “latest version” is determined by the date filter at the top of the restore screen. Now proceed by clicking Restore.

If the virtual machine contains snapshots, you need to restore all the files to the same folder, such as C:\VHD. WARNING: Even though the default restore setting does not overwrite files without your permission, you still need to be careful not to overwrite files accidentally!



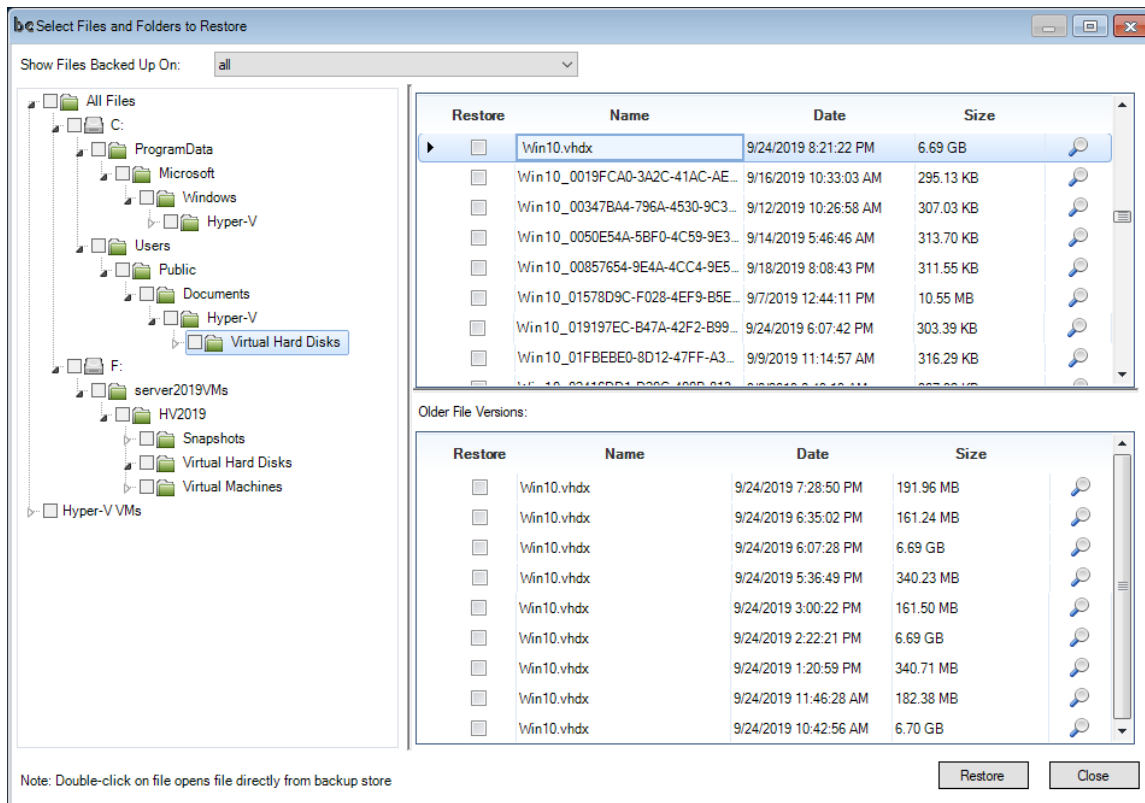
## Replacing the original VM

If you would like to replace the original VM with the one from your backup, there are several options.

First you need to turn off the original VM.

If your VM was neatly stored in a single dedicated folder, the restore process is extremely simple. You can replace the files at their original location via a setting in the 'advanced options' of the Extraction Options screen above. In that case, **do not enter a destination path**.

If your VM is stored in the default folders C:\ProgramData\Microsoft\Windows\Hyper-V and C:\Users\Public\Documents\Hyper-V, you will see that Hyper-V places all VM files in there, for all VMs you have. This isn't exactly neat but still works. When doing a restore you will see those two folders in your Restore Screen. Select the VHD and any AVHD files (checkpoints if any) and click restore. If you want the latest version of your VM, select the VHDs at the top, like Win10.vhdx below:



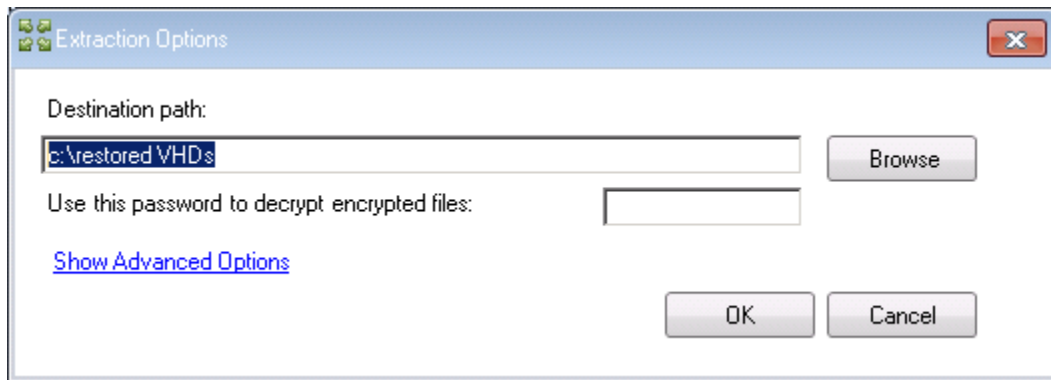
**If you need an older version, do not select line at the top, select from the bottom half, or set the Restore Point at the top of the screen "Show Files backed up on:"**

If your VM doesn't contain checkpoints (recommended practice), then all you need to restore is just the VHD file/s, there's just one for each virtual drive in the VM. If checkpoints are present you need to restore those as well (file extension AVHD and AVHDX).

### *Restoring a VM to a New Hyper-V Host or Side-by-Side with Original VM*

Select the relevant VM files as described in the previous section. For VMs that use checkpoints you must restore those as well (file extension AVHD, AVHDX). If your VM does not use checkpoints (recommended practice) you just need to have the virtual disks for the VM (VHD or VHDX files).

In the Extraction Options screen, enter a destination path and finish the restore process.



You can enter any path you want, including UNC; it will be created if necessary.

If you want the VM restored to its original location, it can't live side-by-side with the original. In that case you will need turn off and delete the original VM first. Note that Hyper-V does not delete the VHDs when you delete the VM in Hyper-V Manager. Then do not enter a path in the screen above and click 'show advanced options'. When the screen expands choose 'restore to original location' and keep the destination path box empty.

Head over to Hyper-V Manager and create a new VM in Hyper-V with similar settings as before (optional).

Now add a new Hyper-V machine via the Server Manager and connect to the existing virtual disk:

The screenshot shows the 'New Virtual Machine Wizard' window with the 'Specify Name and Location' step selected. The left sidebar lists the steps: 'Before You Begin', 'Specify Name and Location' (highlighted), 'Specify Generation', 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area contains instructions and input fields for the virtual machine's name and location.

**New Virtual Machine Wizard**

**Specify Name and Location**

Choose a name and location for this virtual machine.


The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name:

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☐ Store the virtual machine in a different location

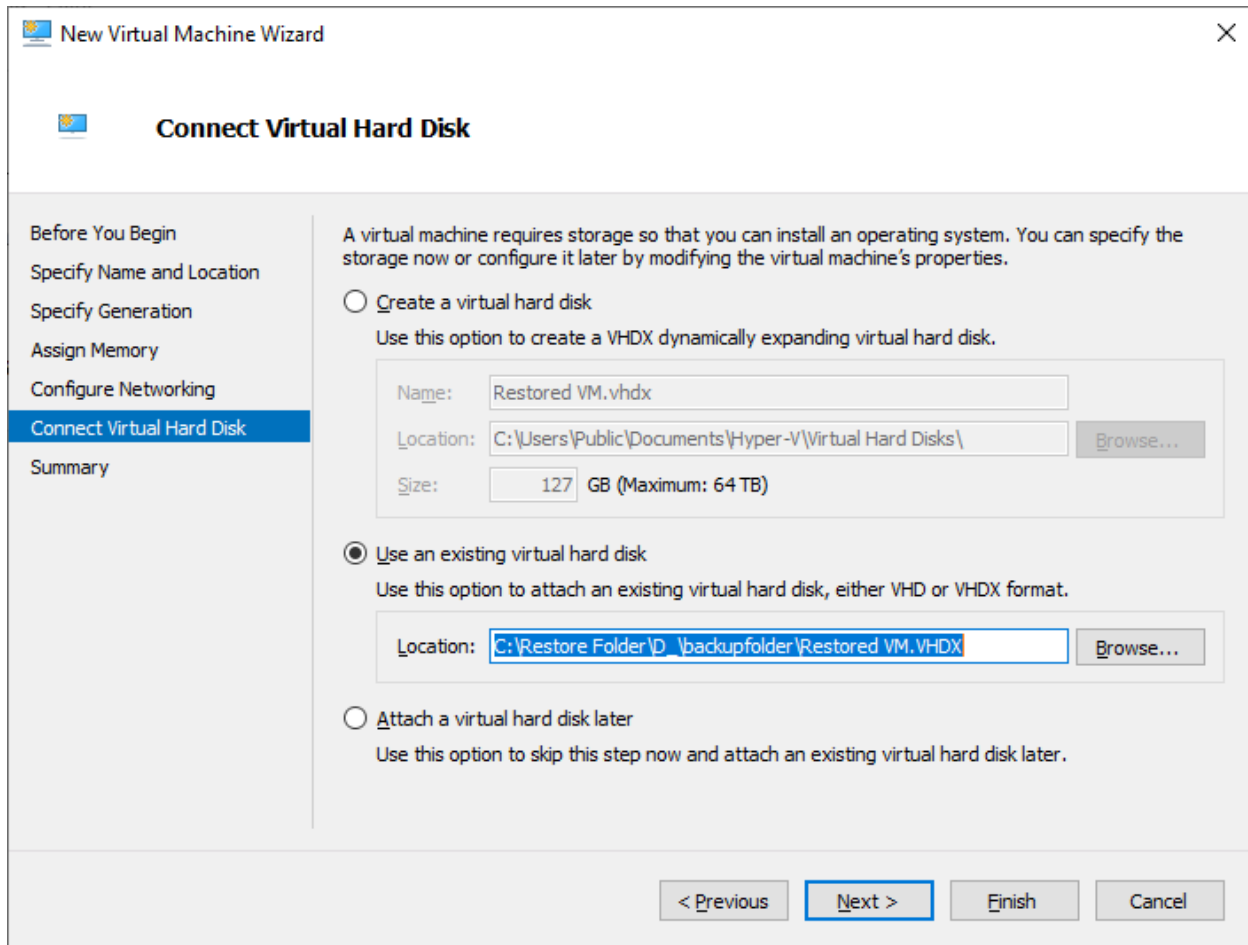
Location:

 If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

< Previous   **Next >**   Finish   Cancel

Try to assign the same or similar settings, such as number of CPUs and RAM, and start the machine.

Instead of creating a new virtual disk, select the one that BackupChain restored:



The VM is now ready to boot. Note that if the VM had checkpoints you need to place them next the VHDX file in the same folder. In the screen above you would select the most recent AVHDX for the VM's main VHDX file, instead of the VHDX file. Checkpoint files always contain the parent's name in their file name so you can track them easily.

### Summary

These steps above summarize the steps required to restore a VM on any Hyper-V host (Windows 8/10 and Windows Server 2008 and later). Note that the Server Editions of BackupChain contain automatic backup and restore features that automate the entire process. When backing up or restoring VMs, you just select the VM from a list and BackupChain does the rest. However, for home, test, and development usage, the Professional edition provides all the features needed for a robust backup system that provides deduplication, compression, encryption, alerts, and many other features. To keep the management effort to a minimum and the backup and restore steps as simple as possible, it's greatly recommended to do two things: place each VM in a dedicated folder (ideally all VMs under a dedicated subfolder, like D:\VMs and then D:\VMs\Windows10VM., etc.) and do not use checkpoints, at least use them only temporarily. That reduces backup to just selecting D:\VMs and restoring to just selecting/replacing D:\VMs for a full restore of all VMs or D:\VMs\Windows10VM for one resting one particular VM. More complex environments can be handled by the Professional edition as well, but

require more management and configuration. It may be best to use the Server or Server Enterprise if your VM configuration is complex and changes frequently.

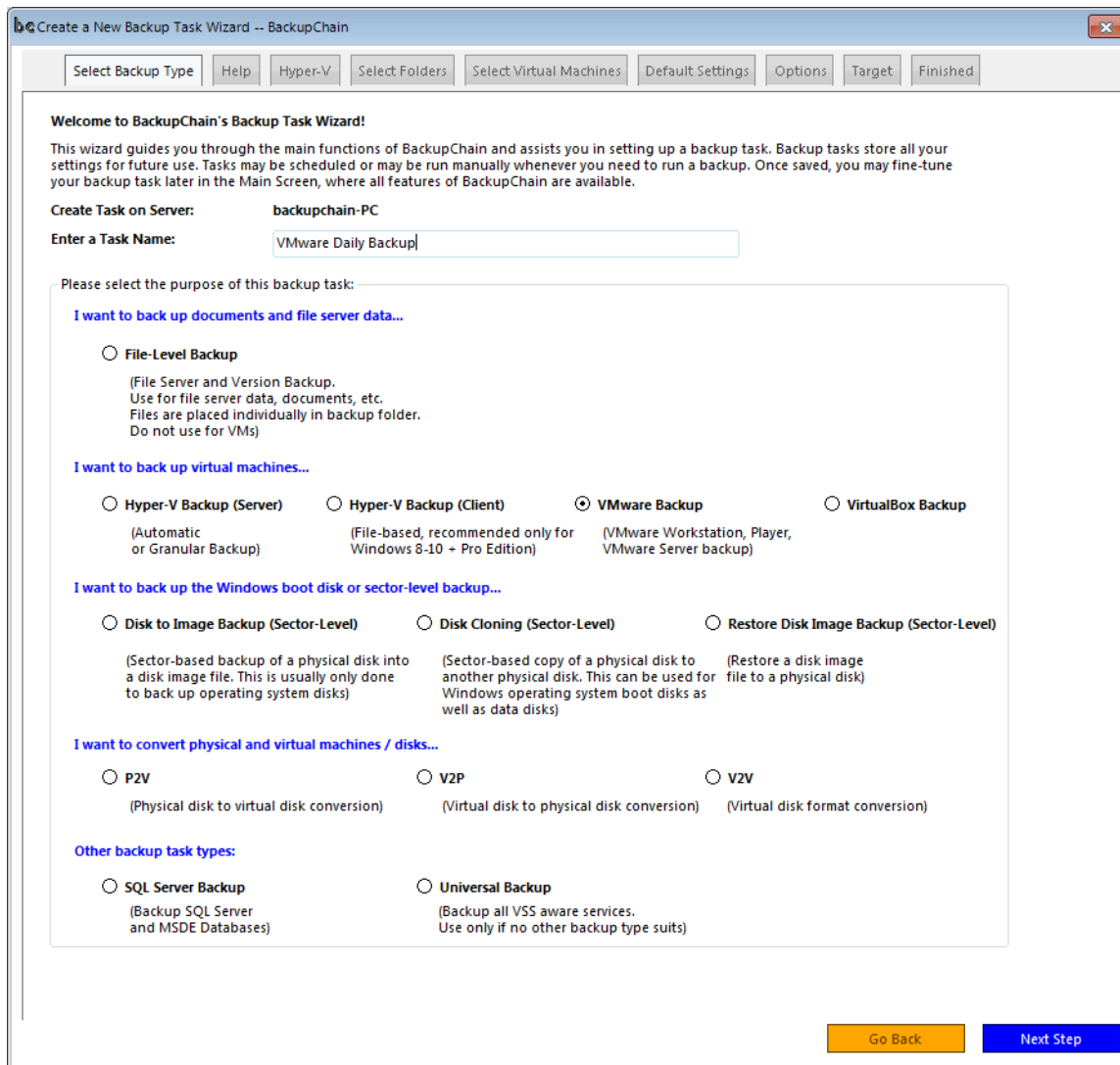
## VMware Virtual Machine Backup

BackupChain performs live virtual machine backups of VMware hosts running on top of Microsoft Windows, such as VMware Server and VMware Workstation. At the moment ESX and ESXi are not supported. You can back up ESX virtual machines from inside the VM using a sector-level disk backup (see respective chapter).

**Important:** In order to generate live virtual machine backups, BackupChain needs to run on the host computer. Another option is to run BackupChain within the virtual machine where you can run file-level backups as well as sector-level full disk backups. The steps below are illustrating backups taken from the host. To take backups inside, check the sections on sector-level disk backup and general file backup.

### Backup

Create a new VMware Backup task by clicking New Task in the main screen. It's recommended to create a VMware Backup task and use it only for VMware-related files:

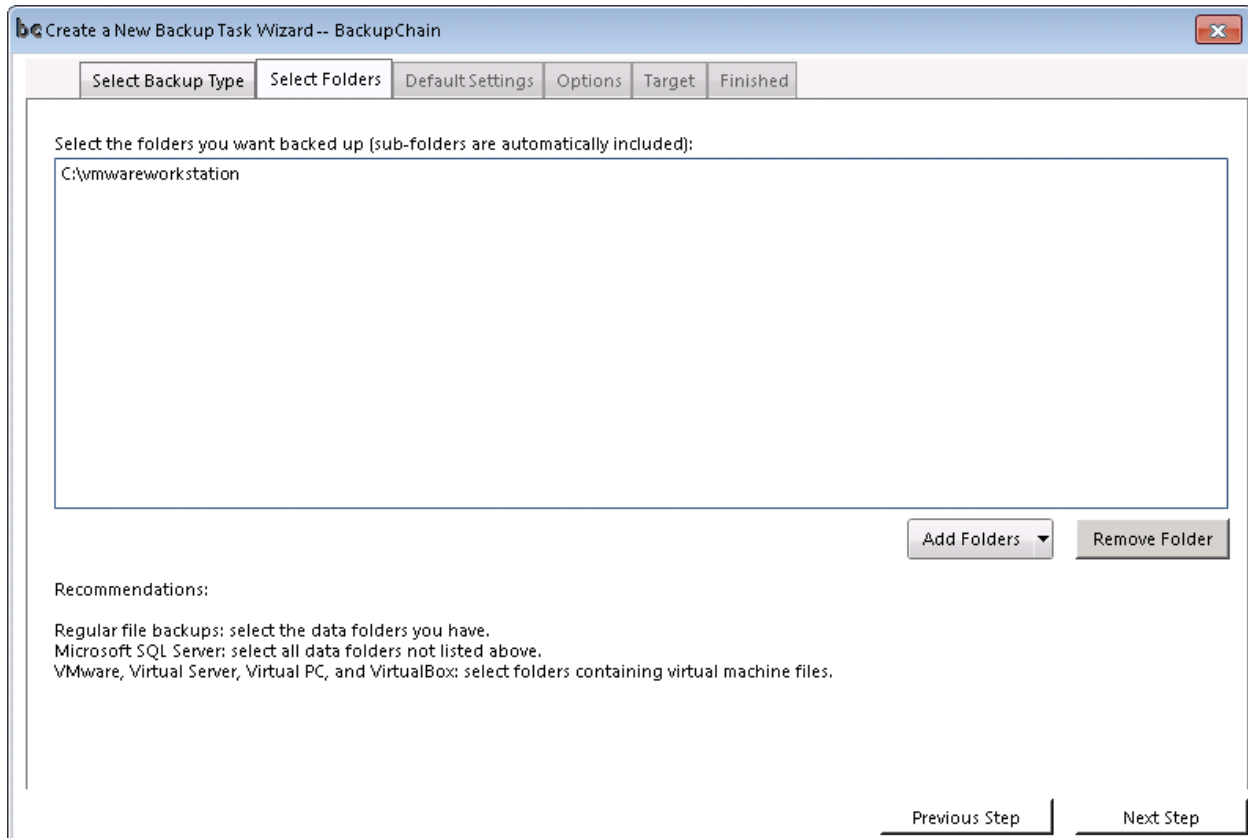


In this example, we back up a Windows Server 2008 R2 virtual machine, located in C:\VmwareWorkstation. The folder has the following sample contents:

Name	Size
vmware-0.log	142 KB
vmware-1.log	627 KB
vmware.log	253 KB
Windows Server 2008 R2 x64.nvram	9 KB
Windows Server 2008 R2 x64.vmdk	6,780,992 KB
Windows Server 2008 R2 x64.vmsd	0 KB
Windows Server 2008 R2 x64.vmx	3 KB
Windows Server 2008 R2 x64.vmxs	1 KB

We select that folder for backup. Note that you can only back up live virtual machines when they are stored locally. Live backups do not work over the network. Offline backups do work over the network, however.

If you don't know which folders are used by a particular VM, simply check the virtual disk setting for the VM in VMware. There you will find the path to the VMDK file, which is where all other VM-related files are also stored. In our example below, it is c:\VMwareWorkstation, and all our VMs in subfolders, which are included automatically:

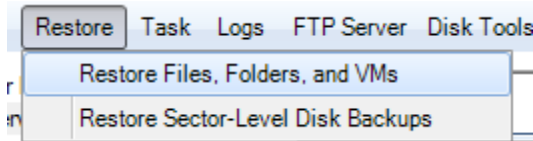


We then accept the default settings in the following screens and select a backup target. See previous chapters for more information on backup options.

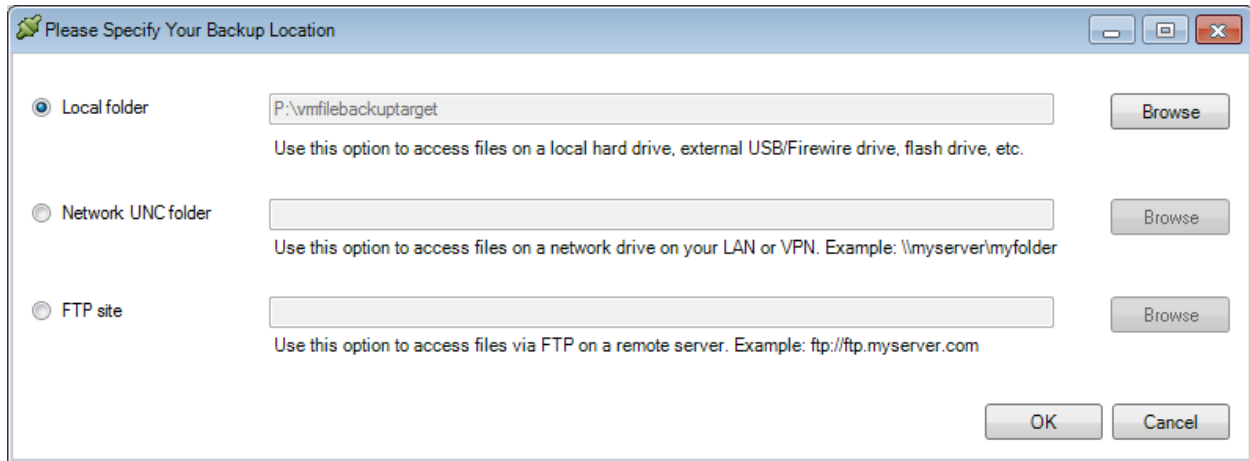
The task is now complete and can be started. You can set the schedule and edit other configurations later once the task is saved.

## Restore

Follow the steps below to restore a VMware virtual machine. Select Restore Files, Folders, and VMs from the main menu:

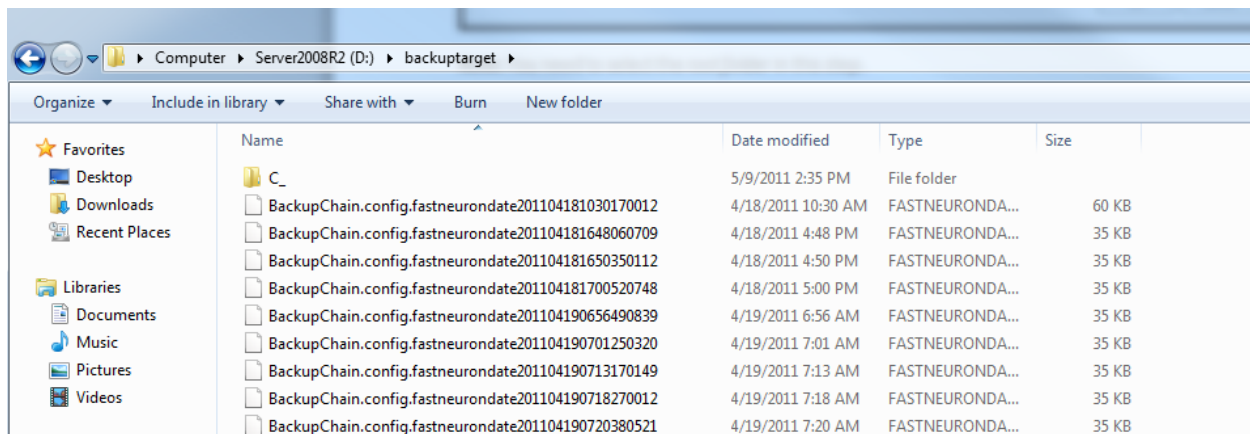


Then you need to fill in the details about the backup location. This information is usually preset with the task settings:



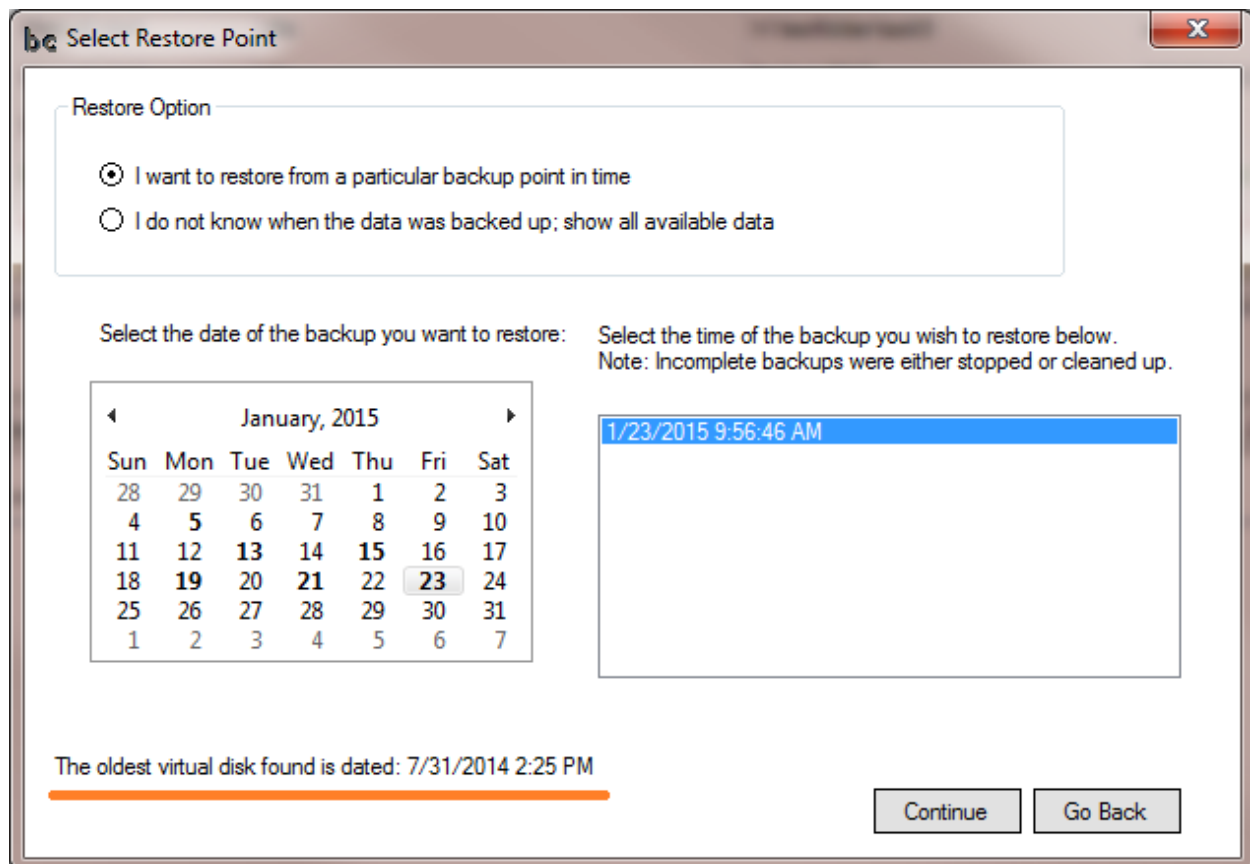
**Note:** You need to select the *root folder* in this step.

If you open the folder in Windows Explorer, the root folder may look like this:



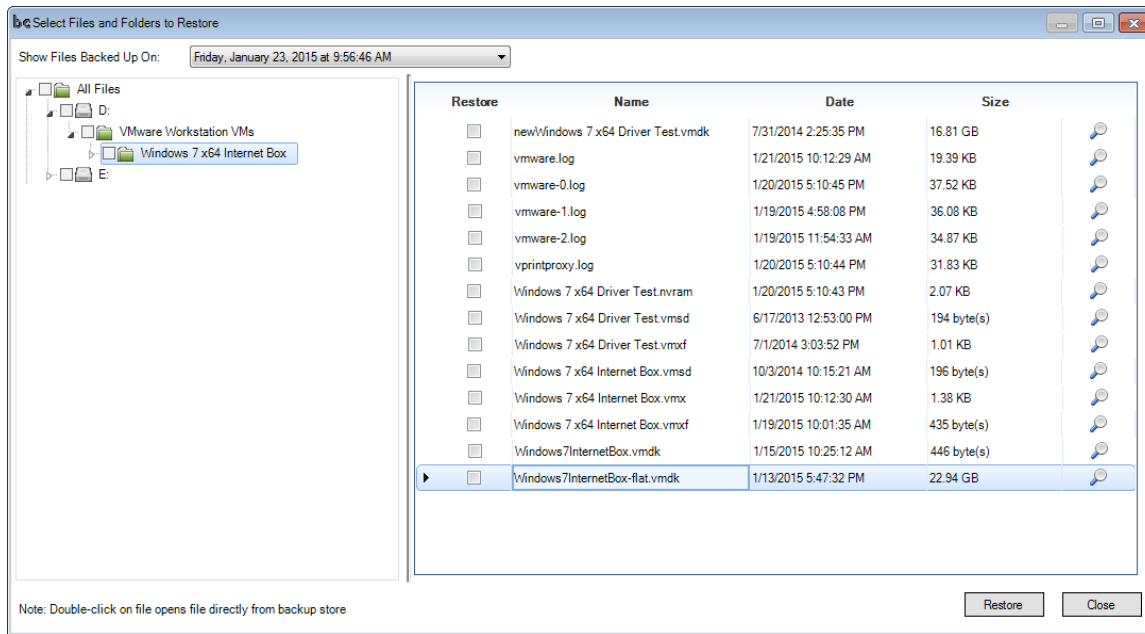
Notice the C\_ folder (for C: drive) and the BackupChain.config files. These files are necessary for restore operations.

Proceed and select a Restore Point. Select a date from the calendar and the list of backups taken on that day will be shown underneath. Select the backup time and click Proceed. Alternatively select "I do not know when the data was backed up" to obtain the 'full' view of all available backups at the same time.



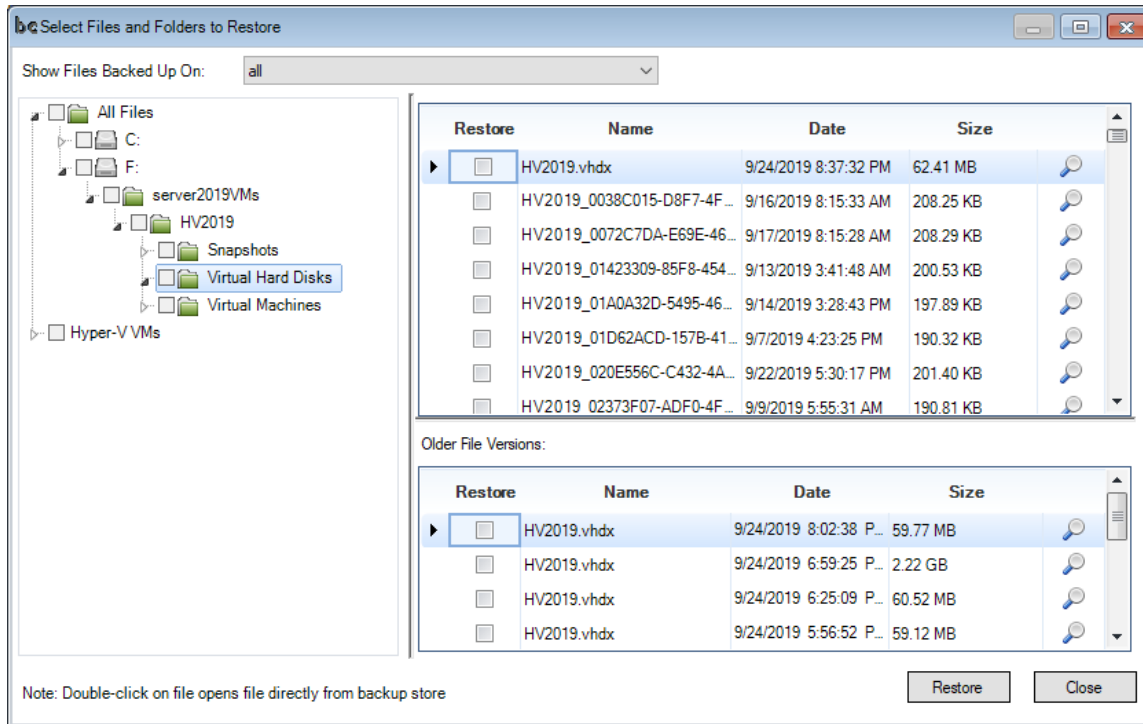
Note that BackupChain will scan in the background all available restore points. It will look for the oldest virtual disk that is available and display the date (see above in orange). Depending on your backup settings, there may be restorable backups from before that, but the date displayed, once the scan is complete, shows the backup date of the oldest virtual disk found, which is the oldest fully restorable backup.

Now the Restore Screen opens:

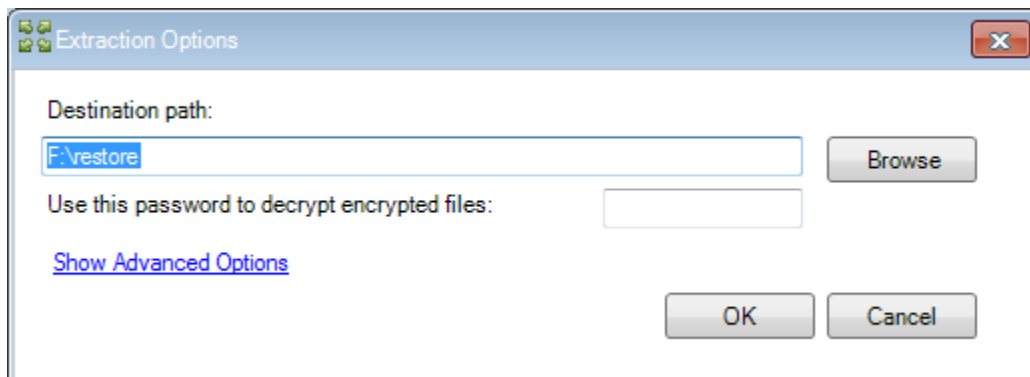


In order to restore all the files related to a virtual machine (their latest version), select the folder in the tree to the left and do not select any files. (“D:\VMware Workstation VMs\Windows 7 x64 Internet Box” in example above).

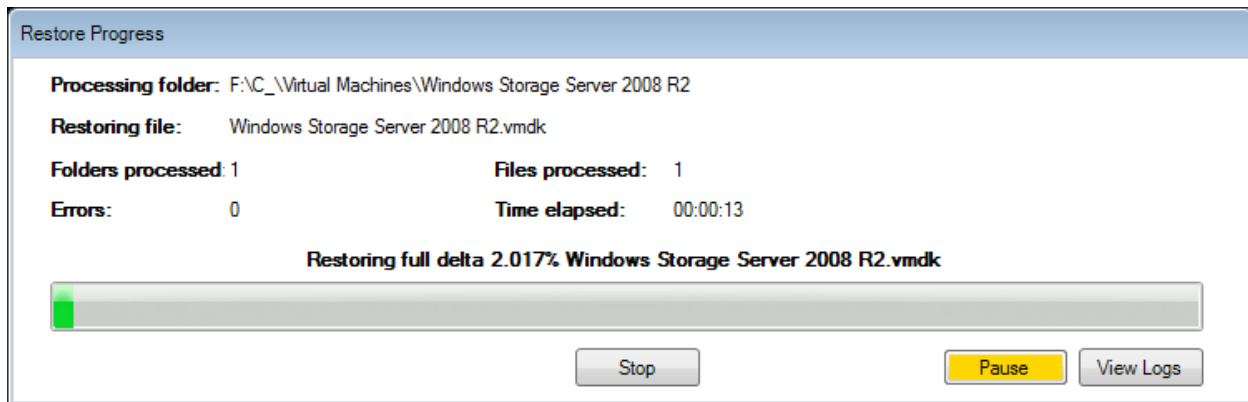
If you want to restore an earlier version of a VMDK file, click on the VMDK file as shown above, and the screen splits in half. The bottom half now shows all old versions of the VMDK file. To restore an old version, do not select the file at the top, select only one file from the bottom list. Then click the Restore button to proceed. If older file versions are present, the screen looks like this, note the file “HV2019.VHDX” is selected at the top and its older file versions appear at the bottom:



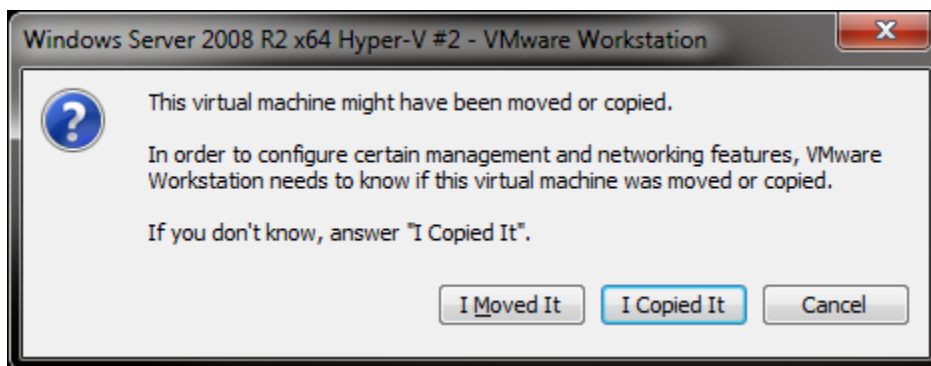
To proceed after clicking “Restore” simply enter a path where you want the restored files to be stored. You can always move them elsewhere from there. Note that a UNC path may also be entered here if necessary.



Proceed with the restore and wait until finished:



Then use Windows Explorer and navigate to the VMX file of the virtual machine you restored. VMware will then ask whether you moved or copied the VM:



By answering “I moved it” you make VMware aware of the VM’s new location. Then power up the VM and your restore is complete! “I copied it” will assign a new hardware ID to the VM. Use the latter only if you are restoring the VM side-by-side for testing along with the original VM.

Note: When powering up a restored VM, if you receive a “Windows has not been shut down correctly” it’s because the “booted” flag hasn’t been cleared from the hard disk image. Be assured that the VM is in good condition.

## Cold VMware Backups

Cold VMware backups are also possible. You can shut down the virtual machine before backup and then restart it. Some users prefer this method or create some backups cold and some live. You could set up several backup tasks to automate the process.

VMware provides the utility “vmrun.exe”, refer to VMware’s documentation for more information.

You could invoke VMware's vmrun.exe as External Utility in BackupChain's Options tab.

Run this command when the backup starts:

```
C:\path-to-vmware\vmrun.exe stop "C:\path-to-vm\myvm.vmx"
```

Run this command when the backup ends:

```
C:\path-to-vmware\vmrun.exe start "C:\path-to-vm\myvm.vmx"
```

In both cases you would want to use the option to wait until the program finishes.

## Microsoft SQL Server Database Backup

There are two ways to back up SQL Server database. One way to use a VSS-powered hot copy of the database files (MDF, LDF, etc.). Alternatively, you can use SQL Server's BACKUP DATABASE command and then have BackupChain deduplicate the backup file.

### Backup MDF and LDF Files

Create a new SQL Server backup task:

**Create a New Backup Task Wizard -- BackupChain**

Select Backup Type | Help | Hyper-V | Select Folders | Select Virtual Machines | Default Settings | Options | Target | Finished

**Welcome to BackupChain's Backup Task Wizard!**

This wizard guides you through the main functions of BackupChain and assists you in setting up a backup task. Backup tasks store all your settings for future use. Tasks may be scheduled or may be run manually whenever you need to run a backup. Once saved, you may fine-tune your backup task later in the Main Screen, where all features of BackupChain are available.

Create Task on Server: backupchain-PC

Enter a Task Name: Daily SQL Database Backup

Please select the purpose of this backup task:

**I want to back up documents and file server data...**

☐ **File-Level Backup**  
(File Server and Version Backup. Use for file server data, documents, etc. Files are placed individually in backup folder. Do not use for VMs)

**I want to back up virtual machines...**

☐ **Hyper-V Backup (Server)** (Automatic or Granular Backup) ☐ **Hyper-V Backup (Client)** (File-based, recommended only for Windows 8-10 + Pro Edition) ☐ **VMware Backup** (VMware Workstation, Player, VMware Server backup) ☐ **VirtualBox Backup**

**I want to back up the Windows boot disk or sector-level backup...**

☐ **Disk to Image Backup (Sector-Level)** (Sector-based backup of a physical disk into a disk image file. This is usually only done to back up operating system disks) ☐ **Disk Cloning (Sector-Level)** (Sector-based copy of a physical disk to another physical disk. This can be used for Windows operating system boot disks as well as data disks) ☐ **Restore Disk Image Backup (Sector-Level)** (Restore a disk image file to a physical disk)

**I want to convert physical and virtual machines / disks...**

☐ **P2V** (Physical disk to virtual disk conversion) ☐ **V2P** (Virtual disk to physical disk conversion) ☐ **V2V** (Virtual disk format conversion)

**Other backup task types:**

☒ **SQL Server Backup** (Backup SQL Server and MSDE Databases) ☐ **Universal Backup** (Backup all VSS aware services. Use only if no other backup type suits)

Go Back Next Step

Select the Microsoft SQL Server database folders for backup. The default location of database files is under C:\Program Files\Microsoft SQL Server

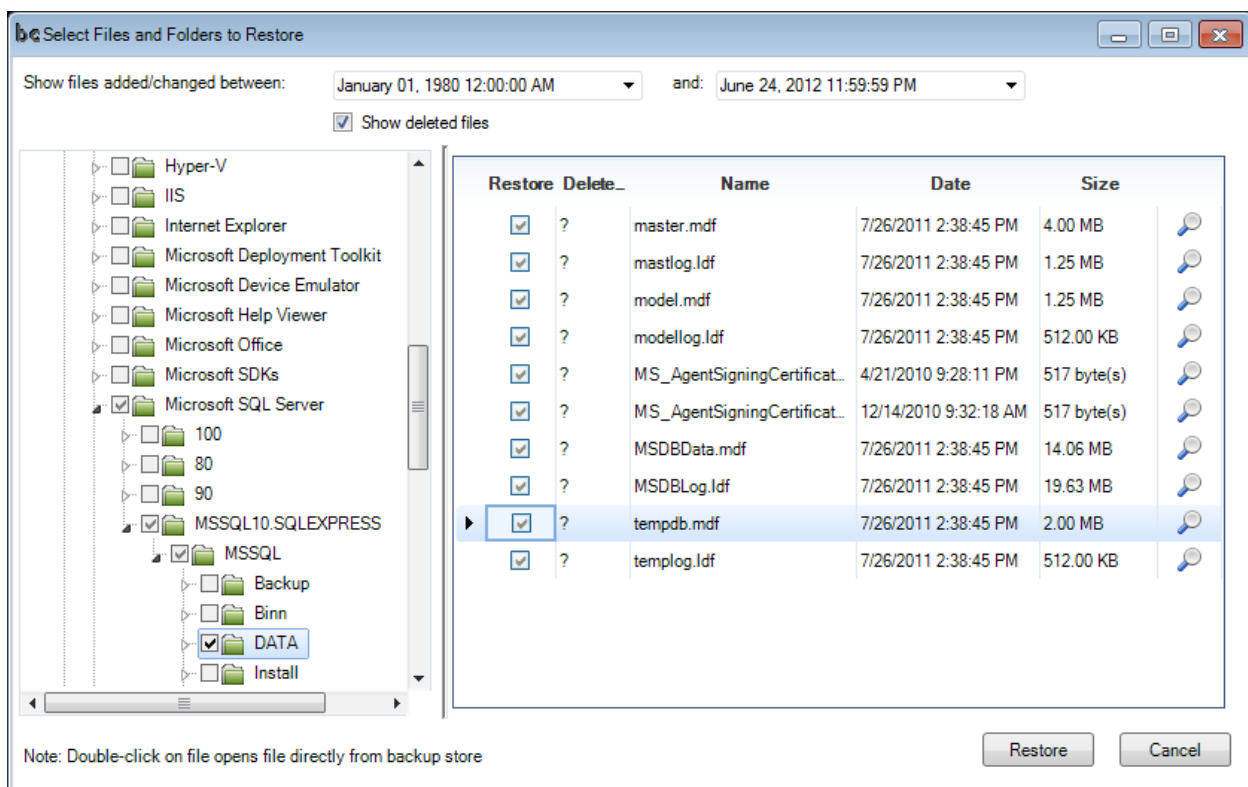
Ensure the service “SQL Server VSS Writer” is activated and enabled. Ideally it should be set to start at boot time automatically. To check it’s working, open a command prompt window as administrator and issue the command: vssadmin list writers. The command should list a VSS writer for SQL Server.

Follow the guidelines introduced in previous chapters to complete the backup (select relevant folders, set a target folder, save task, then set schedule and other settings in the main window).

## Restore

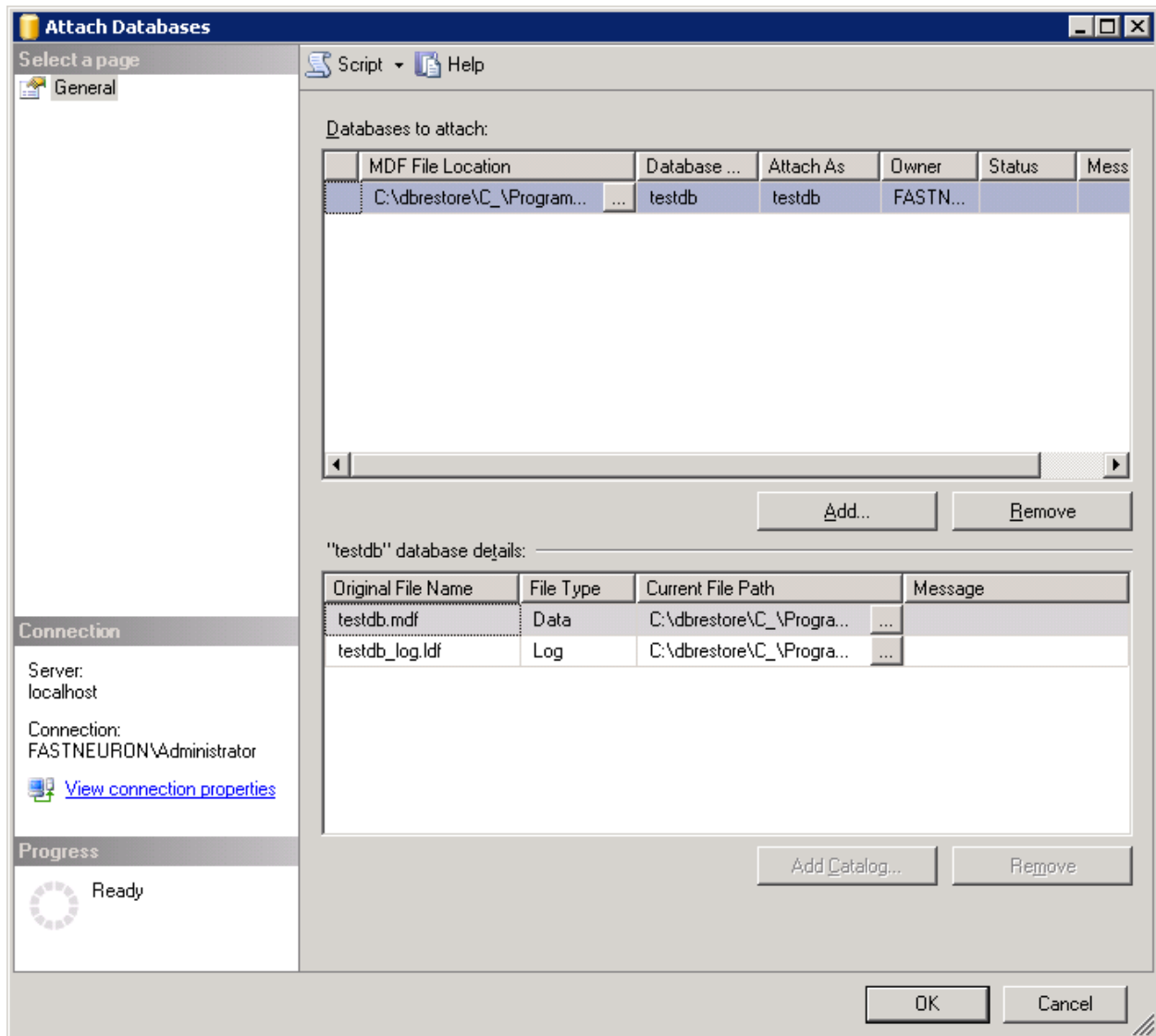
Follow the general restore steps outlined in previous sections. (Select Restore from main menu and select backup folder).

Then navigate to the database files (MDF and LDF file types). In our example below these are located in C:\Program Files\Microsoft SQL Server\MSSQL10\_50.MSSQLSERVER\MSSQL\DATA



We select the latest MDF and LDF files and hit restore. Note: you need to select matching LDF and MDF pairs (matching date / time) when restoring an older version. You may use the date filter at the top of the restore screen, or select one of the older file versions at the bottom half of the screen.

After restoring to a temp folder, open SQL Server Management Studio’s option to attach databases:



Select the MDF file you just restored. In the example above, the database is called testdb.mdf.

Then, refresh the Databases node of SQL Server Management Studio and the new database will show up as a child node.

## Backup Via SQL Server Script and then Deduplicate Using BackupChain

Some people prefer to use SQL Server's backup function to create a backup file.

Run the following script to create a BAK file from SQL Server:

```
BACKUP DATABASE mydatabase TO DISK='C:\tmp\db.bak' WITH FORMAT
```

Alternatively, create a SQL Server Backup task in BackupChain and use this command as external utility. Run the utility before the backup starts:

```
"C:\Program Files\Microsoft SQL Server\90\Tools\Binn\osql.exe" -E -Q "BACKUP DATABASE mydatabase TO DISK='C:\tmp\db.bak' WITH FORMAT"
```

See example below:

The screenshot shows the 'External Utilities' configuration window in BackupChain. The window has a tabbed interface at the top with 'Folders', 'Files', 'Exclusions', 'Backup Target', 'File Versioning / Cleanup', 'Deduplication', 'Schedule', 'Options', and 'Compression'. The 'Options' tab is currently selected. Inside the 'Options' tab, there is a section titled 'External Utilities'. It contains five rows of configuration options, each with a checkbox for when to run the program, a checkbox for 'Wait for program to finish', a text field for the program command, and a checkbox for 'Check exit code' with a corresponding input field. The first row is selected, and its command field contains the SQL Server backup command: "C:\Program Files\Microsoft SQL Server\90\Tools\Binn\osql.exe" -E -Q "BACKUP DATABASE mydatabase TO DISK='C:\tmp\db.bak' WITH FORMAT".

Run program when this backup task:	Wait for program to finish	Program Command	Check exit code
<input checked="" type="checkbox"/> Run program when this backup task starts:	<input checked="" type="checkbox"/>	"C:\Program Files\Microsoft SQL Server\90\Tools\Binn\osql.exe" -E -Q "BACKUP DATABASE mydatabase TO DISK='C:\tmp\db.bak' WITH FORMAT"	<input type="checkbox"/> 0
<input type="checkbox"/> Run program when this backup task succeeds:	<input type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/> Run program when this backup task ends:	<input type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/> Run program when this backup task fails:	<input type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/> Run program after drive snapshot completed:	<input type="checkbox"/>		<input type="checkbox"/>

Then, in BackupChain's Folders tab, add the folder C:\tmp to back up the BAK file using deduplication.

In addition, you will want to turn on compression for BAK files in the File Types tab (use Add button if entry does not exist):

Folders	Files	Exclusions	Backup Target	File Types	Deduplication	Schedule	Options	Compression	Speed	Log	Log Options	Progress
---------	-------	------------	---------------	------------	---------------	----------	---------	-------------	-------	-----	-------------	----------

File types to back up:

Extension	Number of Backups	Compression	Min. File Age	Deduplication	Delayed Deletion Period	Retention Period
*.bak	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever
*.*	10	<input checked="" type="checkbox"/>	0 secs	<input type="checkbox"/>	Never delete	Forever
*.trc	10	<input checked="" type="checkbox"/>	2 minutes	<input checked="" type="checkbox"/>	Never delete	Forever
*.ldf	10	<input checked="" type="checkbox"/>	2 minutes	<input checked="" type="checkbox"/>	Never delete	Forever
*.mdf	10	<input checked="" type="checkbox"/>	2 minutes	<input checked="" type="checkbox"/>	Never delete	Forever

Click Add and enter \*.bak. Check “Compress Files of This Type” and check “Apply file deduplication on files of this type”:

**Add New File Extension**

New Extension: \*.bak Examples: \*.docx, \*.bt, \*.vhd, \*.\*  
☒ Compress files of this type  
☒ Apply file deduplication on files of this type

Number of backups to keep: 10 Set 'number of backups to keep' to zero to exclude certain types of files. Set it to ALL to keep all file versions of this file type. You may also enter new values.

Minimum file age: 0 sec After a file has been changed, this is the waiting period before a file is backed up. Examples: "0 sec" backs up files immediately "1 h" backs up files that have been created or altered >= 1 hour ago

OK Cancel

Your backup configuration is now complete.

## Restore using BAK files

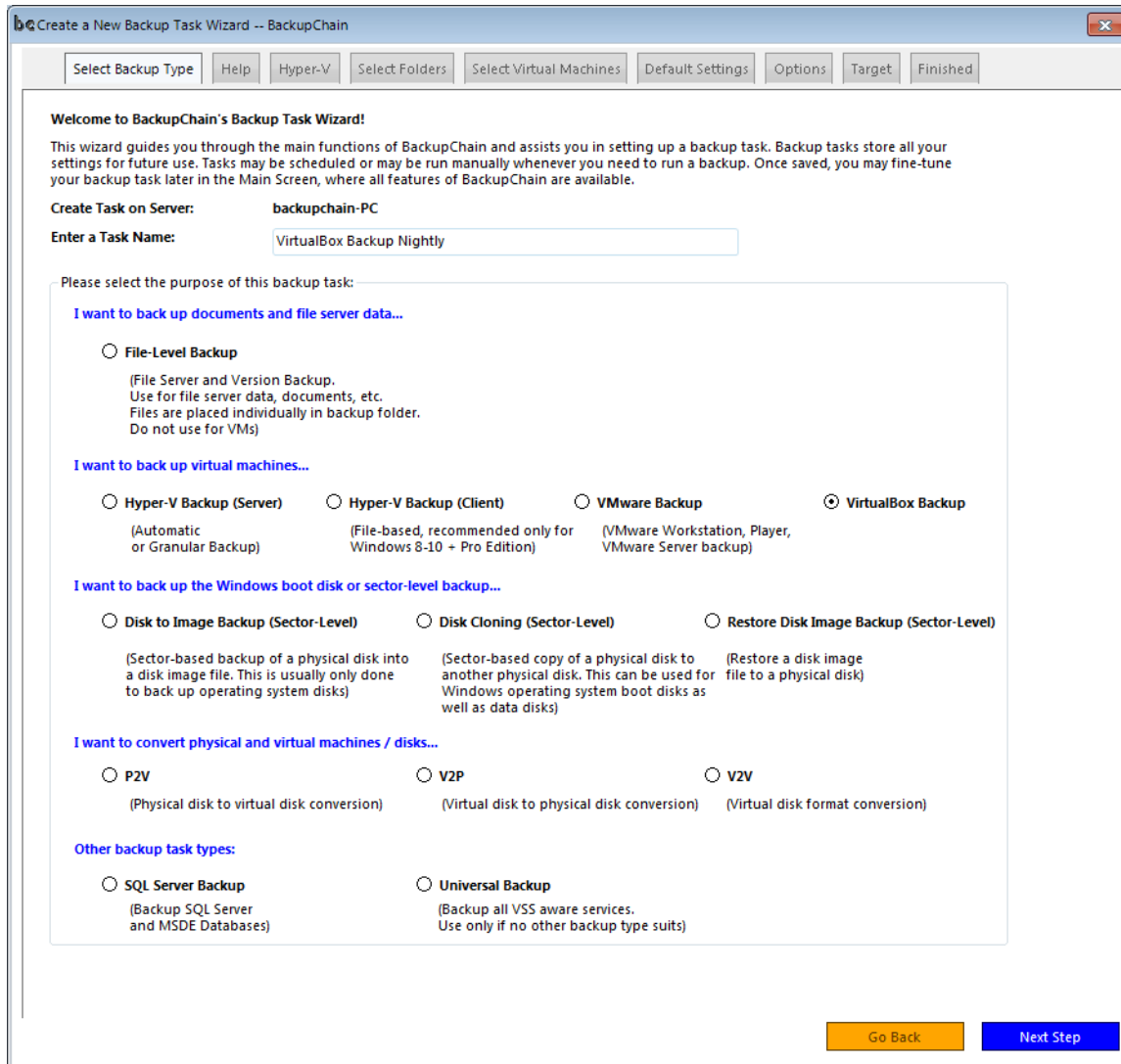
Follow the general restore guidelines discussed in earlier sections to restore the BAK file. Then, follow Microsoft’s SQL Server documentation on how to use the RESTORE DATABASE command to restore the database (<http://msdn.microsoft.com/en-us/library/aa238405%28SQL.80%29.aspx>).

## VirtualBox Backup and Restore

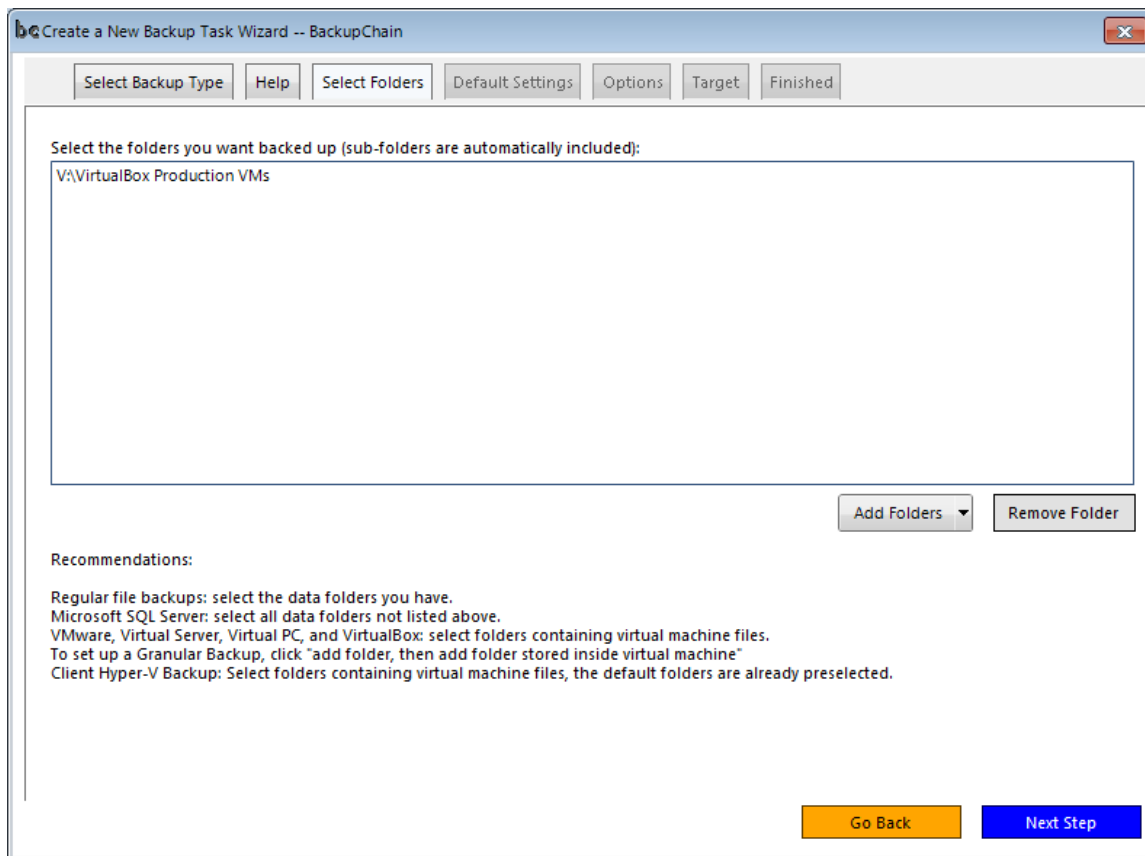
The steps outlined here are similar to the VMware backup and restore steps above.

### Backup

1. Create a VirtualBox Backup task using the New Task button.



2. Select the folder containing all virtual machine files (VHD, VHDX, VMDK, VDI).



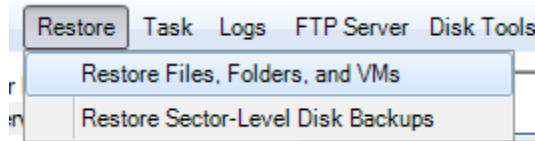
If you are not aware of the exact location of your VM's files, open VirtualBox and open the VM's settings. Navigate to the virtual disk configuration and take note of the path to the VDI or VHD file. That's usually the folder where all VM-related files are stored and the folder you need to include above.

3. Set a target folder and either save the backup task or run the backup.

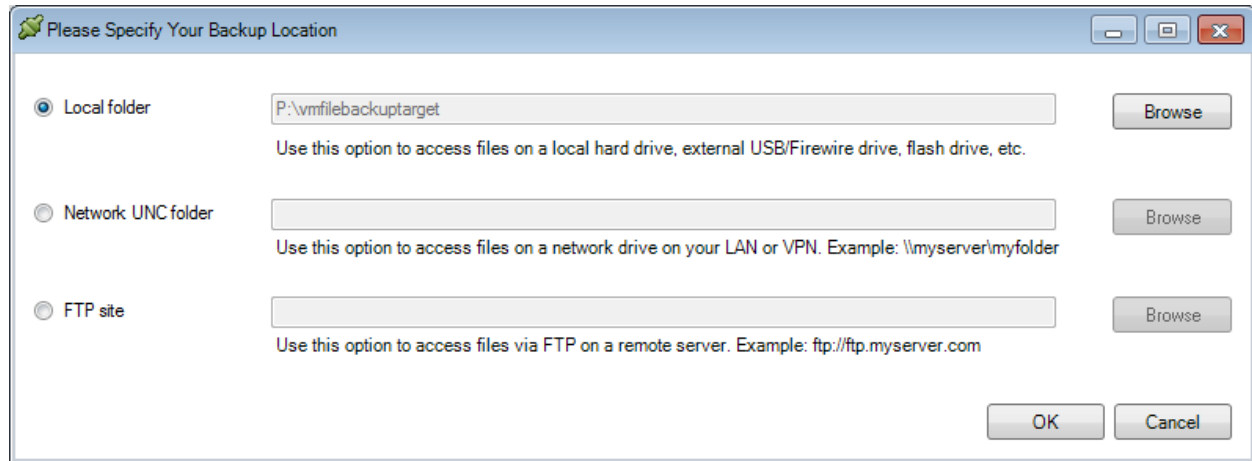
## Restore

1. Restore the virtual machine folder to a new location.
2. Restore the VM's folder, navigate to the VM's VBOX file and double on it to start the restored VM.
  - a. Or, attach the restored virtual disk file (VDI) to a newly created VM.
3. Start the machine.

The detailed steps are shown below. Select Restore Files, Folders, and VMs from the main menu:

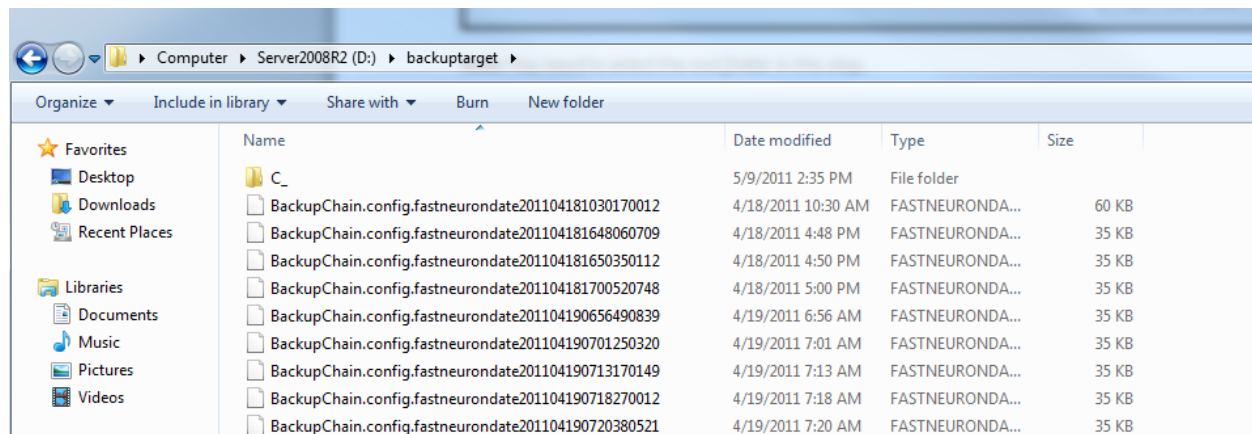


Then you need to fill in the details about the backup location. This information is usually preset with the task settings:



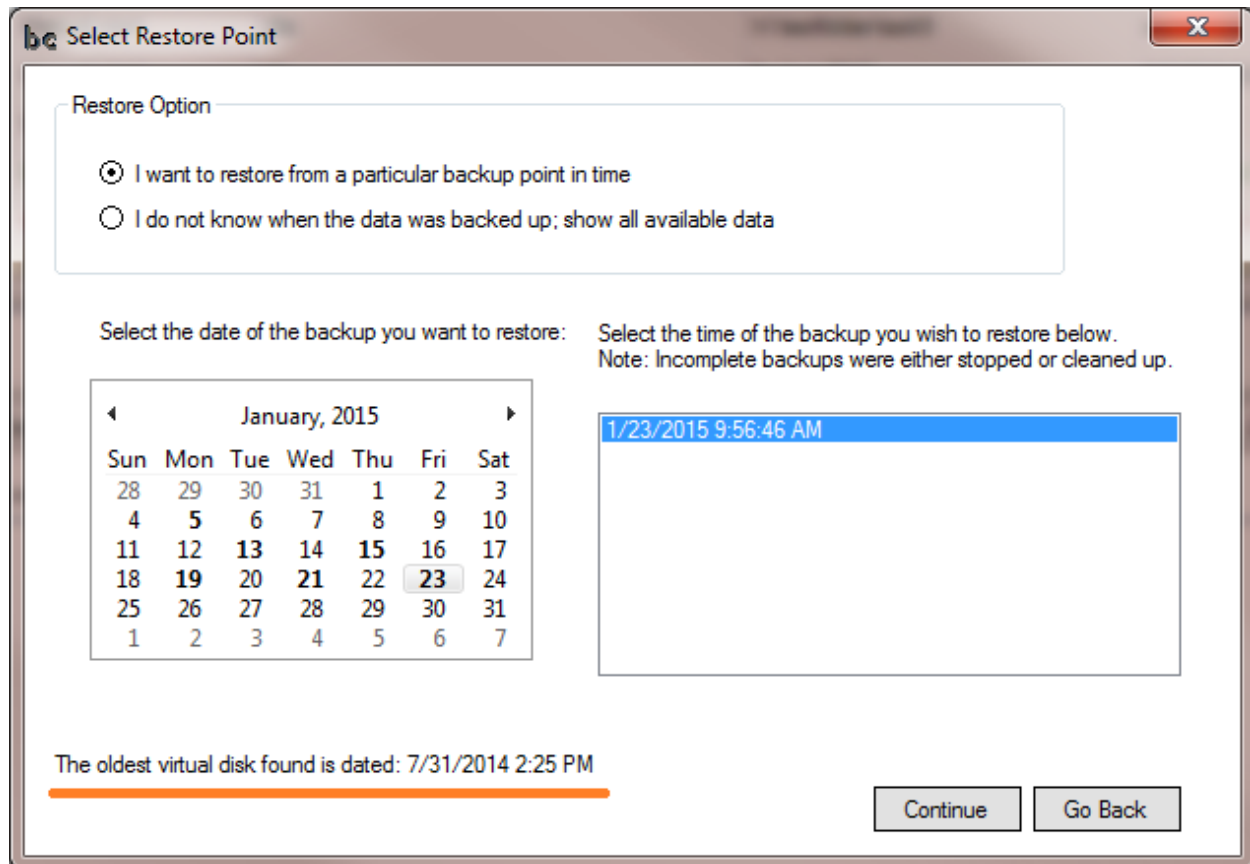
**Note:** You need to select the *root folder* in this step.

If you open the folder in Windows Explorer, the root folder may look like this:



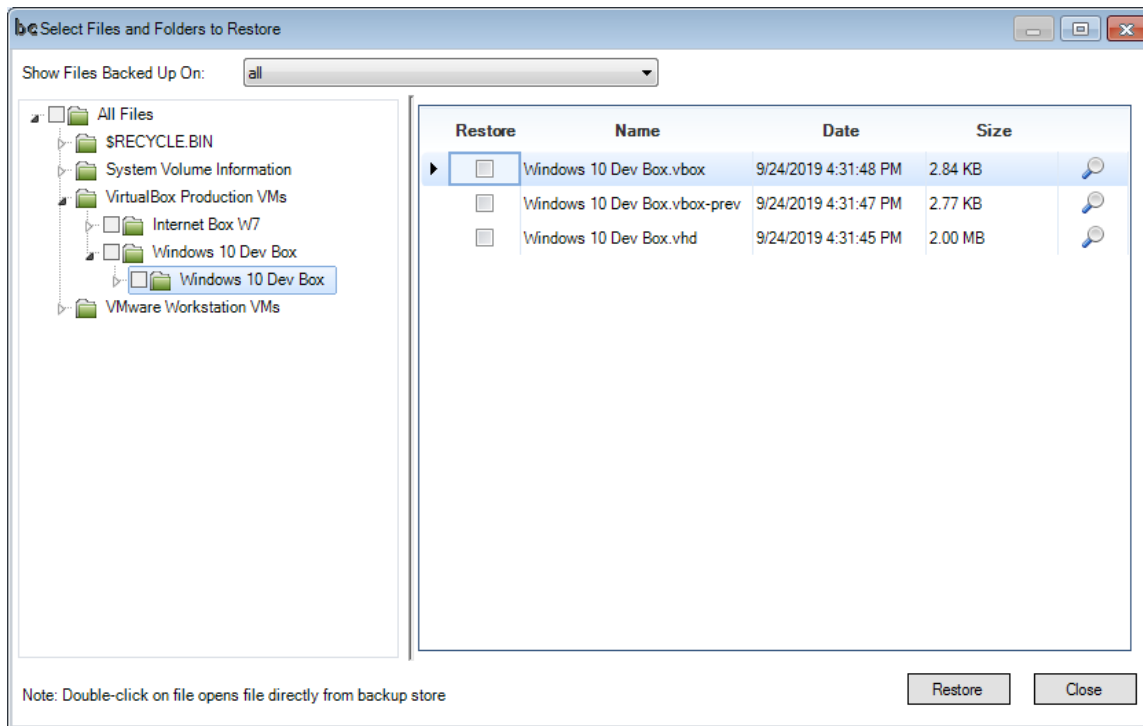
Notice the C\_ folder (for C: drive) and the BackupChain.config files. These files are necessary for restore operations.

Proceed and select a Restore Point. Select a date from the calendar and the list of backups taken on that day will be shown underneath. Select the backup time and click Proceed. Alternatively select "I do not know when the data was backed up" to obtain the 'full' view of all available backups at the same time.



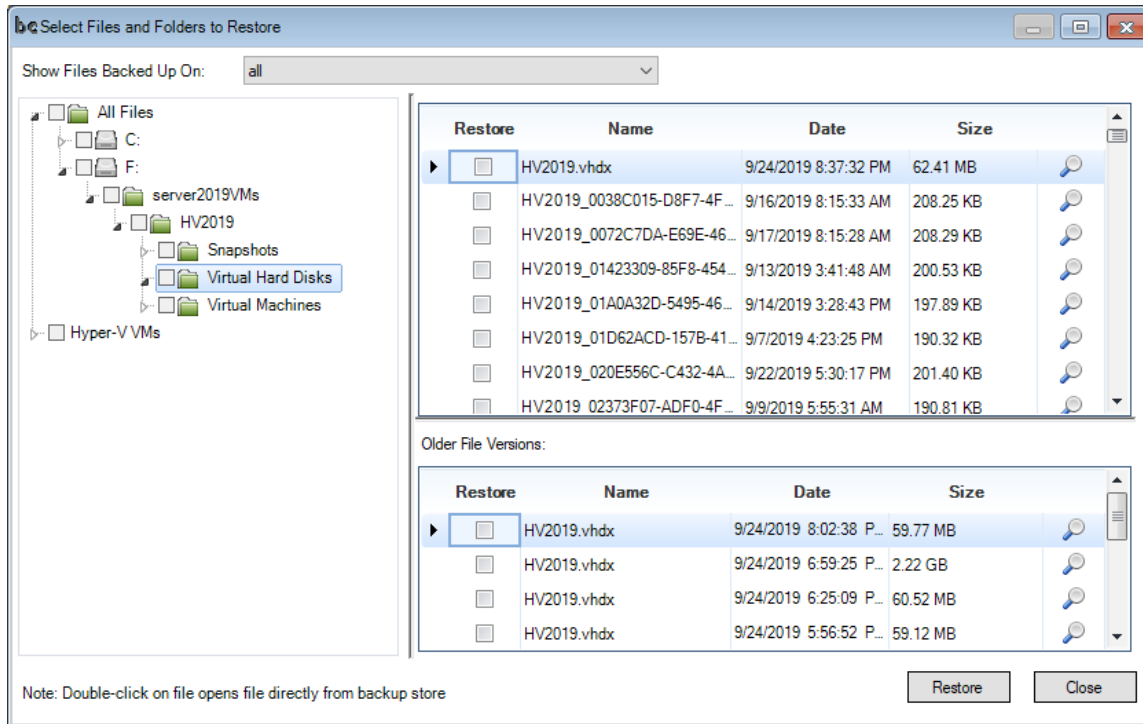
Note that BackupChain will scan in the background all available restore points. It will look for the oldest virtual disk that is available and display the date (see above in orange). Depending on your backup settings, there may be restorable backups from before that, but the date displayed, once the scan is complete, shows the backup date of the oldest virtual disk found, which is the oldest fully restorable backup.

Now the Restore Screen opens:



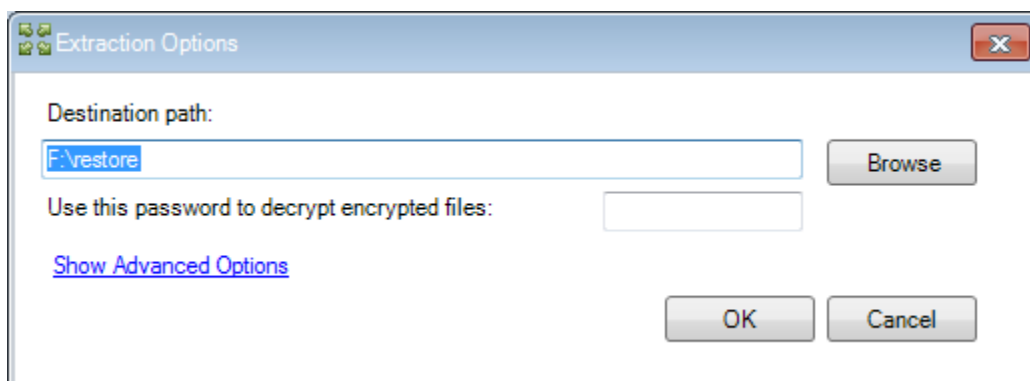
In order to restore all the files related to a virtual machine (their latest version), select the folder in the tree to the left and do not select any files. In our example above we would select “Windows 10 Dev Box” in the tree and click “Restore”.

If you want to restore an earlier version of a VDI file, click once on the VDI file in the above screen, and the screen splits in half if older versions exist. The bottom half now shows all old versions of the VDI file, if any exist. To restore an old version, do not select the file at the top, select only *one* file from the bottom list. Then click the Restore button to proceed. If older file versions are present, the screen looks like this, note the file “HV2019.VHDX” is selected at the top and its older file versions appear at the bottom:

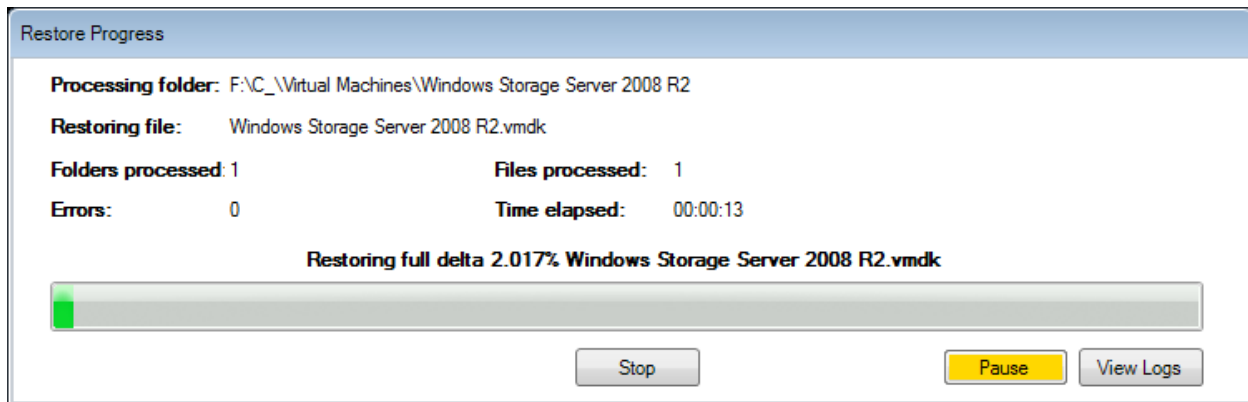


In the above example, it would be possible to restore HV2019.vhdx, which is the VM's main disk, from the bottom half of the screen, which contains older versions.

To proceed after clicking "Restore" simply enter a path where you want the restored files to be stored. You can always move them elsewhere from there once the restore process has finished. Note that a UNC path may also be entered here if necessary.



Proceed with the restore and wait until finished:



Then use Windows Explorer and navigate to and double-click on the VBOX file of the virtual machine you restored and the restored VM will boot automatically.

Note: When powering up a restored VM, if you receive a “Windows has not been shut down correctly” it’s because the “booted” flag hasn’t been cleared from the hard disk image. Be assured that the VM is in good condition.

## How to Set up the Built-in FTP/FTPS Server

BackupChain includes a server-grade, yet simple to use, FTP and FTPS server. With this component you can set up your own *secure* remote storage server.

Unlike many FTP servers on the market, BackupChain's FTP server supports secure and encrypted transfers, file name path lengths of up to 32,767 Unicode characters, and has virtually no file size limitation. This ensures that all file names are preserved and that all kinds of files on a Windows file server can be backed up correctly over the wire without issues.

### Server-side scanning database

BackupChain's FTP server offers more than just FTP. When you are dealing with very large file server backups, the files will be likely distributed over thousands if not millions of folders. When scanning folders, FTP is very inefficient because a separate request is necessary to obtain the list of files in each folder. BackupChain FTP Server, **only in the Server Editions of BackupChain**, contains a server-side scanning feature that compiles an up-to-date list of all files and folders on the server and transfers that to the client in compressed form. The client can then detect file changes on its own. This method eliminates 100% of all folder lookup requests and reduces transmission to just new and changed files and the initial server scan request. The benefit is especially dramatic when dealing with very large file server backups, where time savings can exceed 90%.

For VM-related or small scale backups, the server-side scanning feature is not necessary, as the number of files and folders is small, even if the files themselves are rather large. You can switch off the use of server-side scanning in the Speed tab of your backup task ("Enable folder cache" setting).

### Incremental and Differential Deduplication

BackupChain supports incremental, file-level deduplication over plain FTP. This allows efficient backups of large virtual machines and databases over the wire via the traditional incremental backup scheme: a full, compressed backup is followed by N increments or differentials, forming a backup chain.

### Security Features

BackupChain's FTP Server will ban an IP address for three minutes if the user name / password combination is incorrect. If you accidentally misspell the password or user name when connecting to the server, you need to wait three minutes before retrying. This helps counteract brute force attacks. Also the password has to be at least eight characters long.

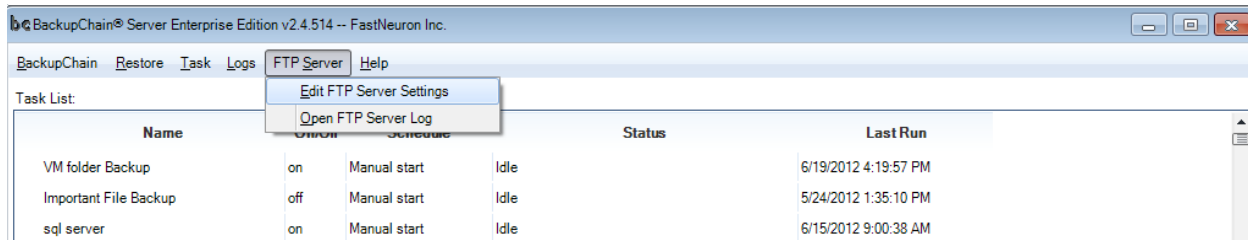
The FTP server can be configured with permitted IP ranges per user, so that you can minimize the probability for an attack. By only allowing a particular IP or specific IP ranges to access a user's data, you can be certain that no outsider can try to break into the account from other locations.

### Reliability Features

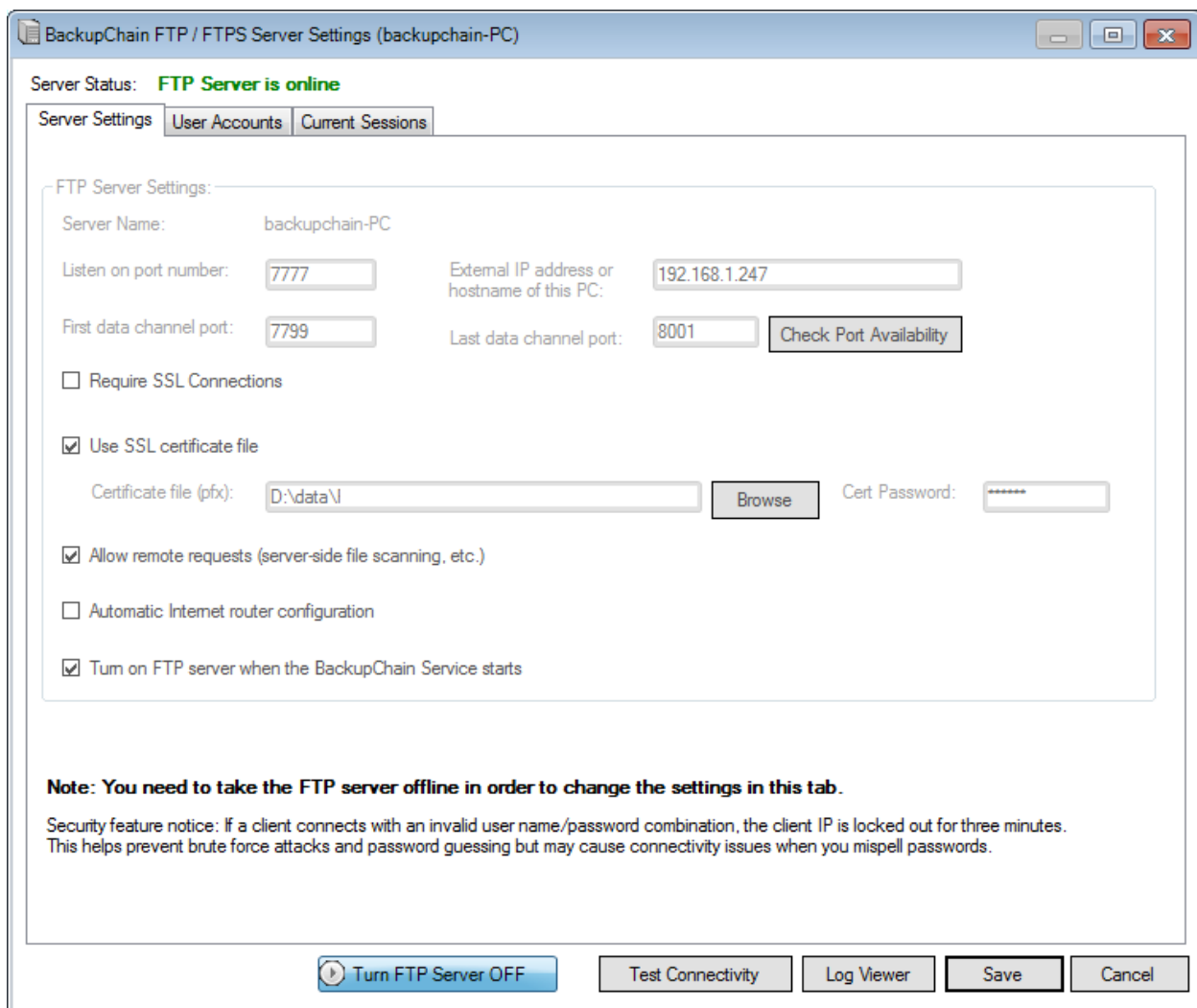
BackupChain's FTP connections are automatically reconnected and resumed when a link breaks. If the link fails for extended periods, the file is skipped and an error is logged.

## Setting up the FTP Server

Select “FTP Server” and “Edit FTP Server Settings” from the main menu:



The FTP Server Settings screen opens up:



Note: In order to change the base FTP server’s settings, such as port numbers, you need to take the server offline (left-most button at the bottom “Turn FTP Server OFF”) if the server is currently running. The other settings found in the User Accounts tab may be edited while the FTP server is running.

First you need to select a primary port and PASV port number. It's recommended to use numbers above 5000 and the numbers shouldn't conflict with other services installed on the computer.

You can check the local availability of the port numbers you entered by clicking "Check Port Availability" or by using the command-line utility "netstat" with -a switch: "netstat -a" to see all occupied ports on a system.

If you have a DSL or wireless home router with UPnP capabilities, you can check the option "Automatic Internet Router Configuration" and then click "Check Port Availability" to have BackupChain automatically open up the ports with your Internet router. The Windows Service "SSDP Discovery" Service needs to be enabled and running for this feature to work and your Internet router must support UPnP configuration.

For FTP transfers, you either need a static IP address on the Internet or a dynamic DNS service, such as no-ip.com or dyndns.org. Basically you need to provide a host name for external computers to access your FTP server. The example above uses the internal IP address "192.168.1.247" but you could also enter a static public IP address instead if you have one, or a domain name, like "myserver.mydomain.com".

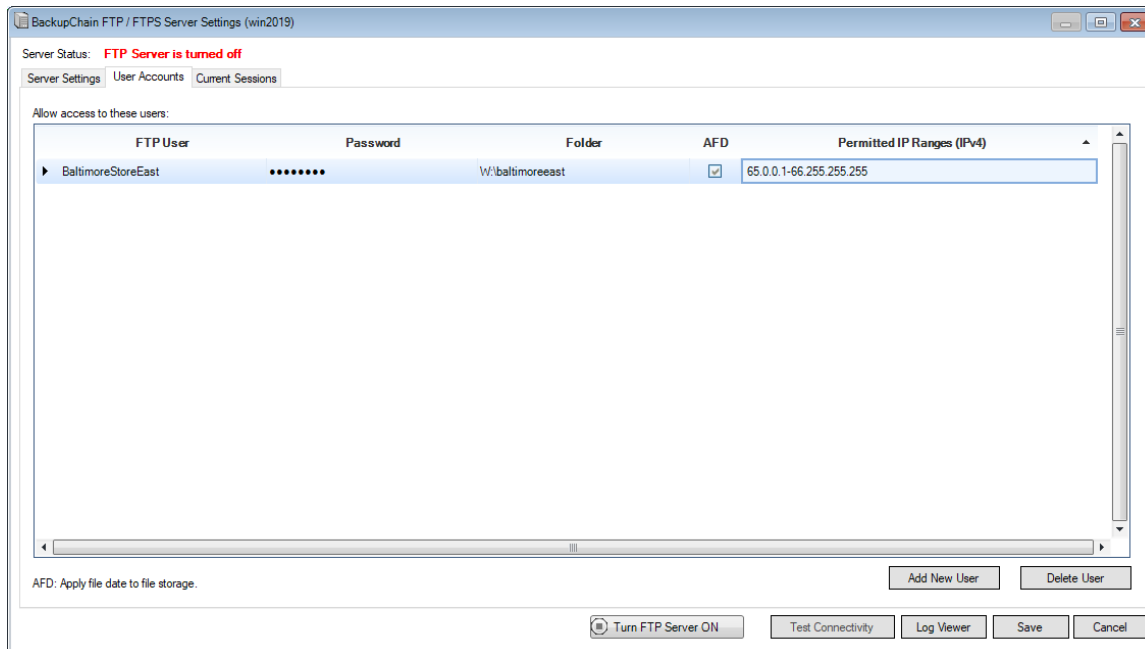
In order to use FTPS (FTP over TLS / SSL), which is an encrypted and secure form of FTP that doesn't expose user name and passwords or data to other parties that may be eavesdropping the link, you need to either use a self-signed server certificate, or if you bought an SSL certificate you can provide the full path to the pfx file name and the password you used when you created the certificate with the certificate authority.

"Require SSL connections" will cause BackupChain to drop client links that do not 'upgrade' to a secure link when connecting; i.e., only secure links will be accepted to proceed with user authentication and data transfers.

"Use Certificate File" allows you to select your SSL certificate in pfx file format. If you don't select one, the server will generate a self-signed certificate automatically and you can still use encrypted links via FTPS.

### **Adding FTP Users**

Switch to the User accounts tab and click "add new user":



You need to have at least one FTP user set up and have assigned that user to a folder on your computer. That folder will be used to store the incoming backups of that user. In our example above, user name “BaltimoreStoreEast” with password “12345678” is assigned to the folder W:\baltimoreeast.

You can create as many users as you like and assign them to different folders. Each FTP user is confined to their private folder and cannot enter other folders on your computer.

**Note:** Passwords need to be at least eight characters long.

**AFD:** Means “apply file date to file storage”. If enabled, this feature requires that you use “BackupChain FTP Server” type at the client side where you send the backups to the server. The AFD stores the file date of a file into the file system of the server. Otherwise, the file information is kept as a suffix in the file name. This preserves the file date with high accuracy on systems where this can’t be done otherwise. For example, the file with name abc.txt will end up being “abc.txt.fastneurondate201804061919520637UT” without the AFD feature. Note that when you restore files through BackupChain, the original file name is restored as well. The suffix containing the date information is removed during restore. The AFD feature is useful for those settings where you want to be able to access the file as-is directly from the FTP folder and wish to keep the original file name.

**Permitted IP ranges.** Here you can specify certain IPs and IP ranges that are allowed to access the account. This is a very useful tool and allows you to minimize the attack surface of the server. It’s not unusual for hackers to use port scanners and dictionary based brute force attacks to try to break into servers. By only permitting certain IPs and/or IP ranges, you can protect your server from such attacks. Also note the server will ban a client’s IP for three minutes when the user/password combination is invalid. If you are setting up a server and misspell the password, you will need to wait for three minutes before retrying.

Multiple IPs and ranges can be entered with a comma separator. Enter a range using the '-' minus symbol. Example entries: 1.2.4.5, 2.3.4.5-2.3.4.255, 10.20.30.40

## Starting the FTP Server

After saving all your settings, click FTP Server is Offline and after a pause it should switch to "Online" and indicate that your FTP server has been started.

## Testing FTP Server Connectivity

The Test Connectivity button uses the first user on your list to connect to the server internally. This only works if the first user is configured properly and if the server can handle internal connections. If your FTP server is configured with the external IP address and you run the test from inside your LAN, the router must be capable of rerouting the request within the LAN. Some routers can't and an error will be reported. In those settings you can use the server only from external networks or you need to specify a local IP and use the server only within the LAN.

In order to test external access to your FTP server, and to be sure your firewall and Internet router settings are correct, you need to use another computer outside of your office or home network and connect to the external address you set up with the FTP server.

For example we would open an FTP client or a browser and enter this address:

ftp://backup.fastneuron.com:7777

Then, when the browser asks for a user name and password, we enter "BaltimoreStoreEast" and "12345678", as configured earlier.

Note that Internet Explorer does not support FTPS; hence, you will have to use an explicit FTPS capable client for testing, such as the test button in BackupChain's FTP backup target settings.

## Current Sessions

In the Current Sessions tab you can see all sessions that are currently connected to the server with speed, IP and user information:

BackupChain FTP / FTPS Server Settings									
Server Status: <b>FTP Server is online</b>									
<div> <div>Server Settings</div> <div>User Accounts</div> <div>Current Sessions</div> </div>									
User	IP	Start Time	Comm...	Command	Start Time	Bytes Sent	Bytes Received	Send Speed	Receive Speed
▶ [REDACTED]	[REDACTED]	9/25/2019 7:23:29 AM	STOR		9/25/2019 8:10:02 AM	58 MB (60355884)		3 MB / sec	[REDACTED]

The server also produces a log that you access via the Log Viewer button.

### Helpful Hints

If you have not configured internet servers before, feel free to reach out to our technical support team.

Below are some hints to help you set up the network so you can provide access from the public internet to your FTP server:

1. BackupChain's FTP server needs to be set up as described above before anything else
2. A firewall exception to the Windows Firewall is added automatically. If you use a 3<sup>rd</sup> party firewall system, you must allow incoming TCP traffic on the port numbers chosen in the BackupChain's FTP server configuration screen.
3. Make sure the port numbers you chose are actually available and not in use. Use `netstat -a` to see if another service is listening on the desired port number.
4. Use non-standard ports for better security, above 5000.
5. Use static IP addresses inside your LAN on the computer running the FTP server
6. Use a static IP address for your internet router so it can be accessed reliably from the internet. If that's not possible, sign up for a dynamic DNS service that will map a custom domain name to your current IP address and update the mapping automatically.
7. Use port forwarding for the ports configured. If the main port forwards correctly but the data ports don't, you will see download/upload errors. If only some data ports are affected you will see sporadic connectivity issues in the logs for some files.
8. You need to be aware of the fact that some ISPs block certain ports on either the sender's or the receiver's side. If you define a wide range of data ports, one of them could be potentially blocked. It's best to use high port numbers to avoid this and test the connection from outside to be certain that sender and receiver have a clear path.
9. Some ISP break TCP links after a while on purpose (based on use, duration, port number, and other unknown factors). This will cause connectivity issues. However, BackupChain can recover from most by retrying the operation.
10. Firewalls may be prohibiting outbound traffic (the Windows Defender Firewall generally does not but can be configured that way). Outbound traffic is not needed for the FTP server side.
11. Some smarter router and firewalls try to 'listen' into the protocol and may mistake the communication as a malware threat. Use FTPS (explicit FTP over TLS/SSL), which is encrypted, to avoid these issues.
12. Always use FTPS unless there is a good reason not to. Plain FTP exposes the connection password in clear text to eavesdroppers on the network. If FTP is used over a trusted VPN, performance is better without FTPS.

## How to Back up to a Remote FTP Server

Whether you use BackupChain's FTP server or a different FTP host, all you need to do to send your backup to an FTP server is to change the Backup Target to FTP and hit browse:

The screenshot shows the 'Target Folder Settings' dialog box with the following tabs: Folders, Files, Exclusions, Backup Target, File Types, Deduplication, Schedule, Options, Compression, Speed, Log, Log Options, and Progress. The 'Backup Target' tab is selected. It contains three radio button options: 'Local folder', 'Network UNC folder', and 'FTP site'. The 'FTP site' option is selected. Below the radio buttons are three text input fields, each with a 'Browse' button. The first field is empty. The second field contains '\\myserver\myfolder'. The third field contains 'ftp://mac.sfservers.com'. Below the third field is a note: 'Use this option to transmit files via FTP to a remote server. Example: ftp://ftp.myserver.com'.

Now enter the connection details necessary to access your FTP server:

The screenshot shows the 'Add New FTP Server Connection Details' dialog box with two tabs: 'General Settings' and 'Advanced'. The 'General Settings' tab is selected. It contains the following fields and controls:
 

- 'Server host name and folder: (Example: ftp.myftpsrvr.com/myfolder)' with a text input field containing 'ftp://myremote.office.com'.
- 'Port number:' with a text input field containing '7777'.
- 'User Name:' with a text input field containing 'hany'.
- 'Password:' with a text input field containing 10 dots.
- A checked checkbox labeled 'Use explicit FTP over TLS (FTPS, encrypted link)'.
- 'Server type:' with a dropdown menu. The dropdown is open, showing a list of options: 'BackupChain FTP Server v4 or later' (selected), 'Microsoft IIS 7 or later', 'BackupChain FTP Server v4 or later', 'Linux-based server or NAS', and 'Custom Settings'.

 At the bottom are three buttons: 'Test', 'OK', and 'Cancel'.

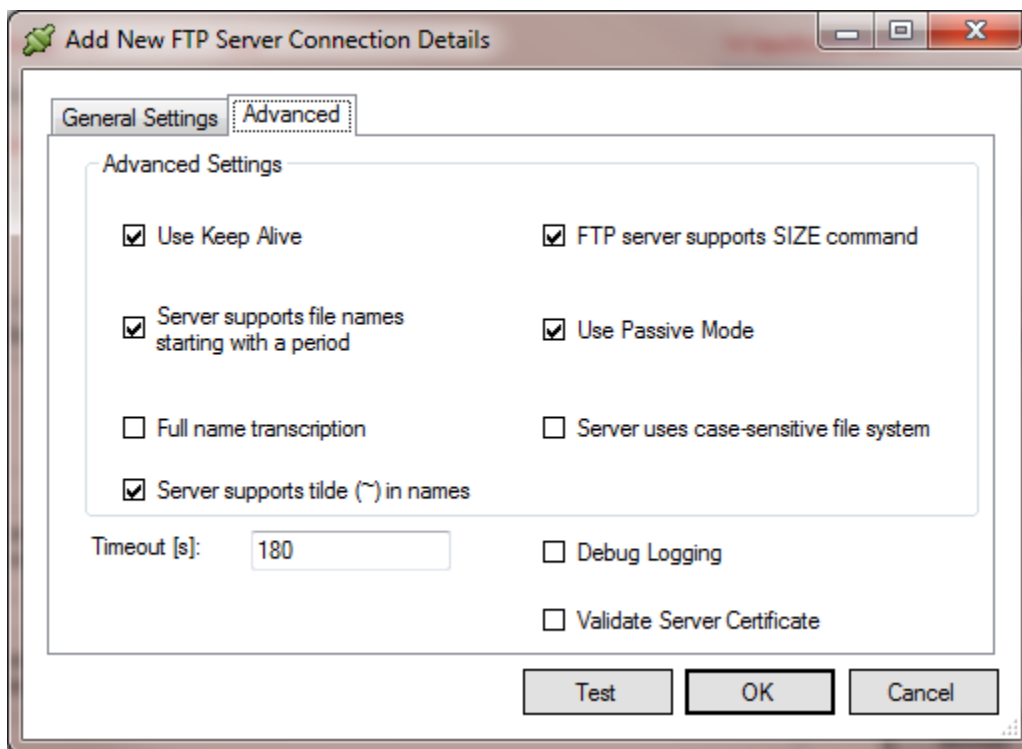
Don't enter the ftp:// prefix, simply enter the IP address or host name as shown above.

The port number is entered separately below. Port 21 is the standard port used for most FTP servers.

You need to enter a user name and password, use anonymous for anonymous access, if your server supports it and you don't have your own user name.

The option "Use explicit FTP over TLS" switches on encrypted FTPS which protects your session from wiretapping.

The server type choice is very important. If you use a BackupChain FTP server backed, choose 'BackupChain FTP Server v4 or later'. For IIS 7 and later, and fully compatible FTP implementations based on NTFS file systems, use 'Microsoft IIS 7 or later'. If you have a NAS server that is based on Linux or not on a Windows operating system, use "Linux-based server or NAS". For all other scenarios, use 'custom settings', which you can edit in the 'advanced' tab:



The above screen in 'custom' mode allows you to change the presets.

"Use Keep Alive" enables a function that attempts to keep the connection active (prevent line drop) during long transfers.

"FTP server supports SIZE command" should be kept on. It is provided to cope with non-standard FTP servers that don't support SIZE commands.

"Use Passive Mode" is the recommended way to access FTP. If you need to use FTP active mode, switch it off but ensure you firewall is configured properly.

“Full name transcription” causes BackupChain to transliterate characters into codes, because on various systems, certain characters are not supported which are valid on Windows. Some systems don’t allow spaces or special characters, such as @ or dots. Those will appear in their ASCII code for example like this !2e.

Some versions of IIS don’t support file names starting with a tilde ~, for those serves that do not fully support ~ you need to uncheck ‘server supports ~ in names’.

On Linux/Unix systems, files and folders are case-sensitive, which can lead to backup errors because Windows is not case-sensitive. Check the option ‘server uses case-sensitive file system’ to force all names to uppercase.

“Validate Server Certificate” forces BackupChain to check the SSL certificate of the server before proceeding. Keep this turned off if you use a self-signed certificate.

### FTP Backup Characteristics

When you send your backups to a BackupChain FTP server, there is no need for further configuration. With other FTP servers, however, you may need to change the FTP server type in order to get all files to back up properly. For IIS targets and Linux-based targets you will need to choose the respective FTP server type in the FTP target folder settings of your backup task.

Always use an empty FTP backup (sub)folder when you start using BackupChain’s FTP function. If your FTP server requires file name transcription and has this feature turned on, after the backup is completed you will find the backup altered the file names of your remote files with special characters, such as “!20”. In addition, BackupChain extends each file with file date information.

This can also occur if you are using a BackupChain FTP Server with the “AFD” (apply file date) option switched off. If you are connecting to a BackupChain FTP server, set the server type as “BackupChain FTP Server” and on the server side, check the AFD option.

The need for file name transcription has arisen from the fact that many FTP servers (especially some NAS devices) do not follow the full standard and

1. Do not support file date manipulation, and
2. Cannot handle special characters in file names, such as spaces or international characters.

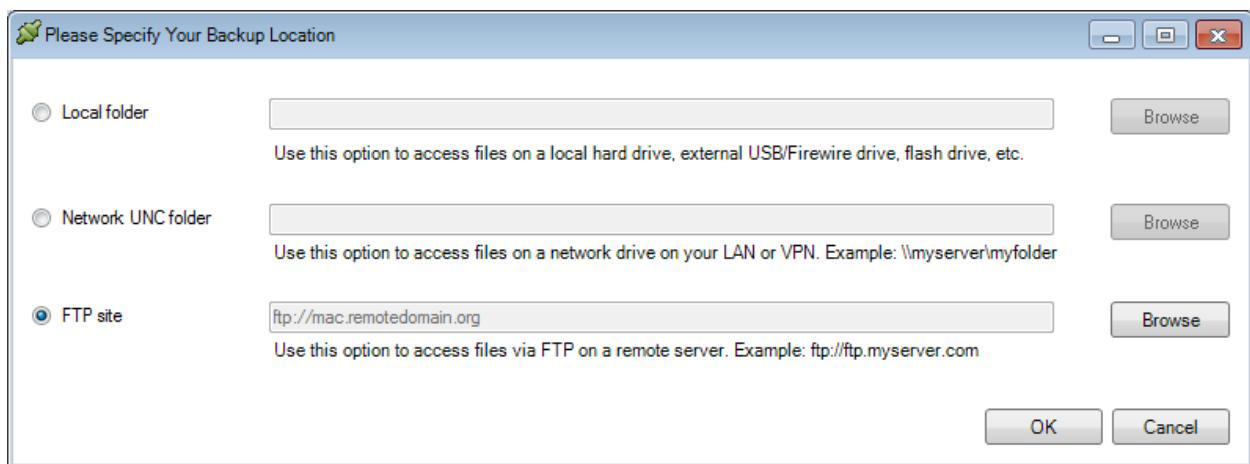
However, when restoring files through the BackupChain Restore Screen, the files are always restored with their correct original names and file date.

Note that some FTP servers do not allow long file names (longer than 240 characters) or international characters. If you have problems with Unix-based FTP servers, check that your FTP account has rename permissions enabled and try to limit path length and the use of special characters. BackupChain v4 and later provide some additional character transliteration settings to get files with certain special characters to back up properly on those systems.

BackupChain's FTP server is capable of handling paths up to 32,767 Unicode characters long. If used on top of a NTFS volume, there is virtually no file size limit.

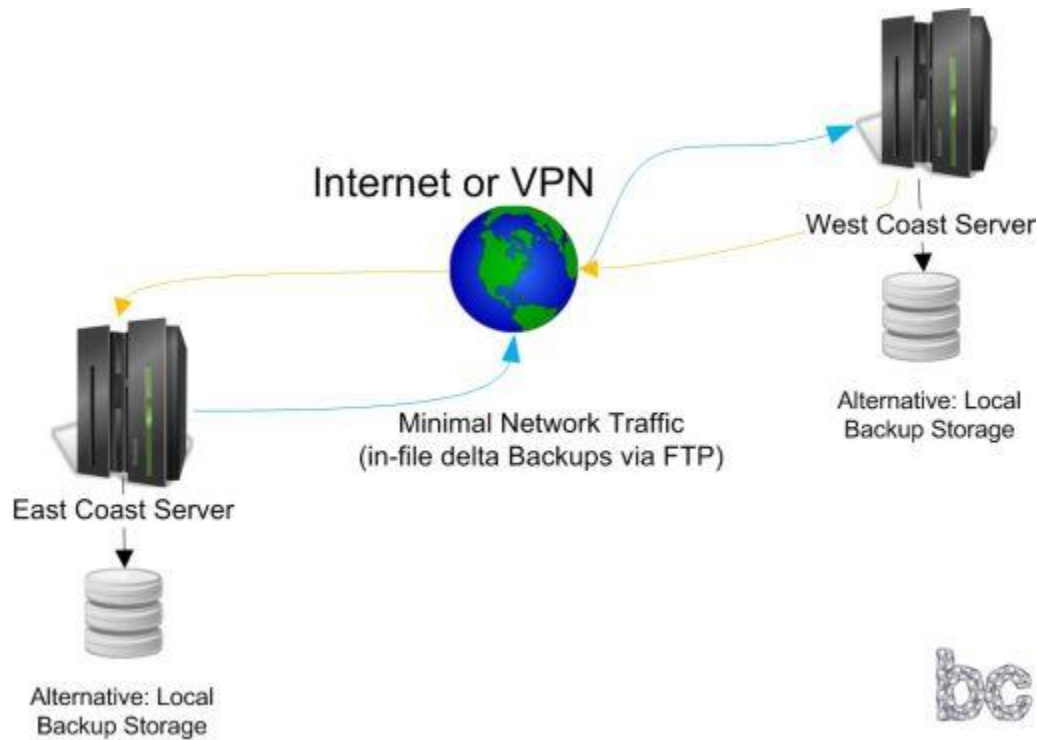
## How to Restore Files Stored on a Remote FTP Server

Restoring files stored on a FTP server works exactly as with local backup stores. After selecting "Restore Files and Folders" from the main menu, select FTP site and Browse, so you can enter the FTP server connection details. If you want to restore from a pre-existing FTP backup task your settings are already pre-entered and you are ready to proceed:



## How to Set Up Your Own Online Remote Backup System

Using the information provided in the previous sections, set up the FTP server at one site and set up BackupChain to send the files to the FTP server:



The above example uses two BackupChain installations, east and west coast.

To set this up, install BackupChain on each server and set up the FTP server on each server as well.

You need to have static IP addresses for both or a dynamic DNS service as discussed in the previous section (How to Set up the Built-in FTP Server).

Then, set the Backup Target of each server to point to the other server's FTP address. For example, if the west coast FTP server is located at `ftp://westcoast.mycompany.com`, then the east coast server should back up to that address. The west coast server would consequently back up to `ftp://eastcoast.mycompany.com`.

## How to Install BackupChain on Windows Server 2008 Core or Hyper-V Server 2008 R2

Also see <http://backupchain.com/i/how-to-install-net-framework-2-0-on-windows-server-platforms>

From the command line execute the following commands to install the .Net Framework 2.0:

```
start /w ocsetup NetFx2-ServerCore
```

```
start /w ocsetup NetFx2-ServerCore-WOW64
```

If the above lines do not work, try these:

```
DISM.exe /online /enable-feature /featurename:NetFx2-ServerCore
```

```
DISM.exe /online /enable-feature /featurename:NetFx2-ServerCore-WOW64
```

Then change directory to the folder containing BackupChainSetup.exe (available from our download page) and run it as administrator.

Then run: C:\Program Files\FastNeuron Inc\BackupChain\BackupChain.exe to open the BackupChain Monitor application.

## How to Install BackupChain on Windows Server 2016 / 2012 Core or Hyper-V Server 2016 / 2012

A .net framework installation is not required because the .net framework v4 is already preinstalled in Hyper-V and core servers.

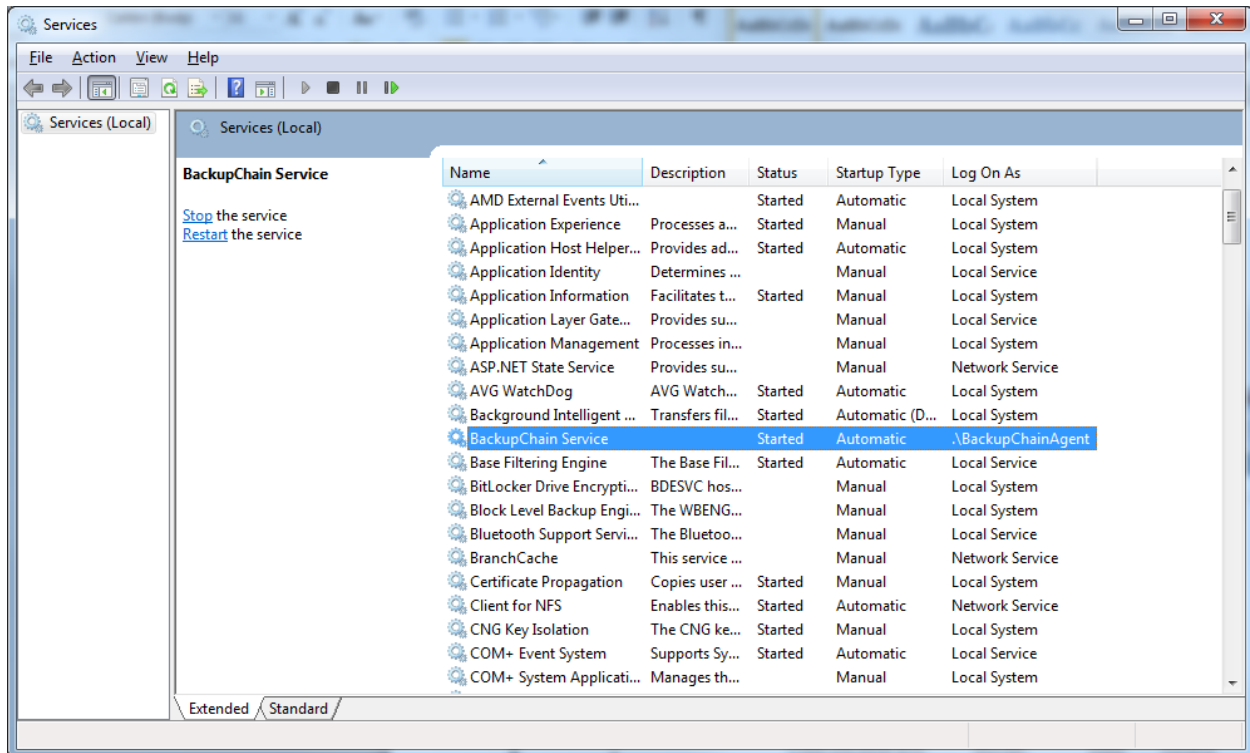
Then change directory to the folder containing BackupChainSetup.exe (available from our download page) and run it as administrator.

Then run: C:\Program Files\FastNeuron Inc\BackupChain\BackupChain.exe to open the BackupChain Monitor application.

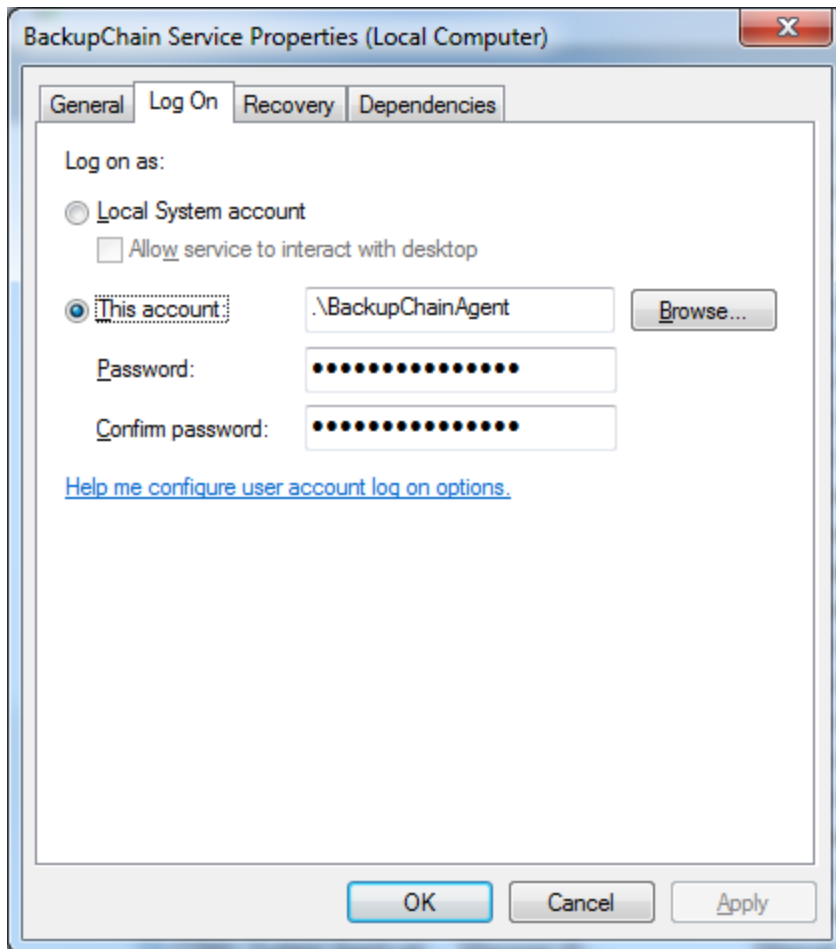
## How to Change the BackupChain Service User

Open the Windows Control Panel and search for Services or Service Manager.

The service name is “**BackupChain Service**”.



Open the properties and navigate to the Log On tab:



BackupChain uses the localsystem user by default. Change the Log On setting above only if there are network access restrictions that cannot be remedied otherwise.

In the above screen you can specify a new account for BackupChain's service if necessary. Please restart the service after changing the user account.

## How to Set up Centralized Remote Management

In order to manage many servers from a single screen without having to log on to each server individually, you need to use the Server Enterprise edition as the “master” and connect to it all other instances of BackupChain you have running on other computers. All instances of BackupChain can be remotely managed, except the Server Edition, which cannot be managed by a master.

### Two Possible Connection Scenarios Combined

Essentially the master console is just another computer running BackupChain Server Enterprise edition or later but has the additional capability of connecting to other servers as well. Connections are handled via TCP and can be *inbound or outbound*.

Note that the way servers are connected for the purpose of remote management does not affect their backups and how their backups are run or stored. The connection scheme is entirely and exclusively limited to the remote management of these servers.

### Inbound Connections

Inbound TCP connections are connections from a slave to the master. The slave is the server being managed by the master.

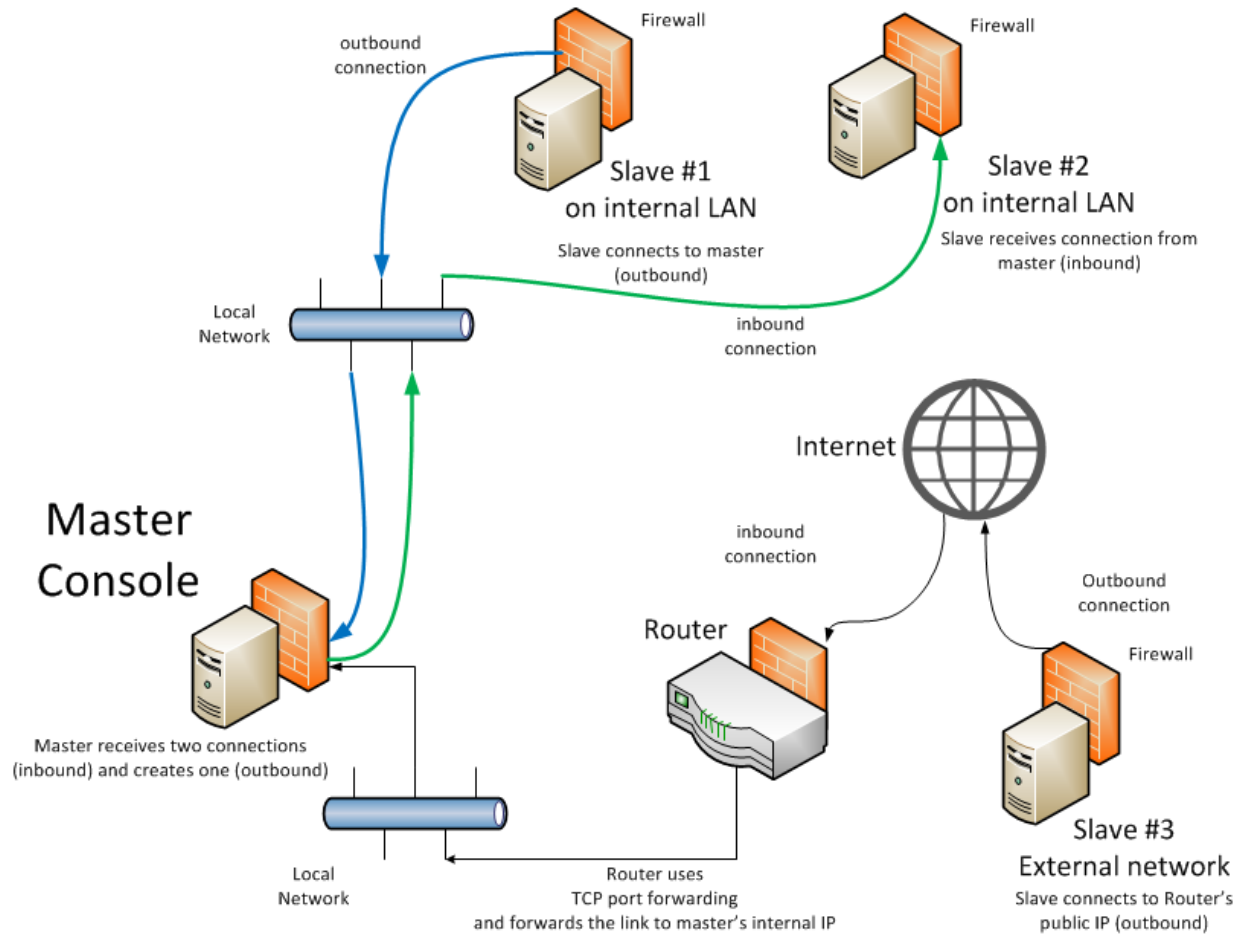
### Outbound Connections

An Outbound connection is a connection made by the master *to* the slave.

Once the connection is established, it doesn't matter whether it was done via an inbound or outbound connection. It does matter, however, for the setup and authentication phase of the connection.

### Example diagram showing a mixed-mode setup

The diagram below shows a mixture of both methods, and also illustrates how the same console can receive connections from slaves on the LAN as well as connections coming from the internet, and at the same time it can also make connections to slaves:



The above diagram shows a master console that is connected to three different slaves, i.e. it can remotely control three other servers. Two of those are on the same LAN and one is external and is accessed over the internet.

For slaves on the internal network, you can use outbound as well as inbound connections and you can always use both methods in combination, but not to connect to the same slave twice from the same master.

## When to use inbound and when outbound?

The reason why BackupChain offers both methods is to offer flexibility and security.

When the master receives the connections from the slaves, it doesn't have to know where the slave is. It just needs to know the slave's name and management password in order to establish trust when the connection comes in. The master also has to be configured to listen for incoming connections in order for this to work.

By using inbound connections, from the master's perspective, the connection has to be configured at the slave side and all devices along the path need to be configured accordingly. For example, slave #1 in the diagram needs to be configured to connect to the master server, and the master server has to be

configured to accept incoming connections. In addition, as with all slaves, you need to add the server in the master's server tree, then indicate that the connection is *inbound*, and set the password required to manage slave #1. Then, when slave #1's connection comes in, the server will recognize the slave by its network name and they will be able to communicate as long as the password is correct.

Outbound connections are typically used in the case of slave #3 above. Because firewalls generally allow outbound traffic, slave #3, which could be a server at a customer site, does not require any additional configuration than what is mentioned above. Slave #3 will be configured to connect to the master console and at the master console you need to add the server, enter the inbound slave name, and enter its password.

In order for slave #3 to reach the master server, however, the connection needs to go through its local router and firewalls, the public internet, then the enter company's firewall and router at the receiving office, the local LAN, and finally arrive at the master console.

Slave #3 will use the router's public IP address or a domain name mapped to it in order to access it. It also has to know the port number. For example, slave #3 could be configured to connect to the master at address: 83.45.23.55:16888, or billsitservice.com:16888, where billsitservice.com maps to the static IP address 83.45.23.55, which is the public IP address of Bill's internet router.

Bill needs to *allow incoming TCP traffic* in the router's firewall (or in a separate firewall if a third device is used) on TCP port 16888 (this is just an example port, you can use any available port number).

Furthermore, the router now has to use TCP port forwarding in order to forward the TCP link to the master console. Let's say the master server's internal static IP address is 10.0.0.3. The router needs to forward the incoming external TCP port 16888 traffic to 10.0.0.3 also on port 16888. BackupChain will need to be configured to accept incoming connections on port 16888 in this case. Once the link arrives at the master server, whether from the internal LAN or from the internet, it will be processed the same and its origin doesn't matter.

Note that BackupChain adds itself into the standard Windows Firewall as exception; hence, you don't have to configure it for inbound or outbound TCP connections. However, if your organization uses a 3<sup>rd</sup> party firewall software or separate device or non-standard firewall settings, you will need to configure each firewall to allow inbound and/or outbound TCP traffic on the port of your choosing, in our example TCP port 16888.

Outbound connections from the master to the slave have their use and benefits, too. However, as you can see from the diagram, if you wanted the master to connect to slave #3, the entire configuration process (router port forwarding and firewall) would have to be done at the site where slave #3 is located. If Bill is an IT service provider with hundreds of customers, his crew would have to configure each customer's router and firewall to let the remote management traffic come in. In addition, customers may feel concerned that a port has to be opened. Naturally, the solution that requires less work and is more secure is the one pictured above. Bill would not have to configure anything, assuming no 3<sup>rd</sup>-party firewall other than the standard Windows firewall is being used, because the standard Windows firewall by default permits outbound traffic, and so do most internet routers. Note that

corporate networks naturally will have additional routers that may need to be configured for outbound traffic as well.

Our example company “Bill’s IT service” will make the choice to use outbound (slave to master) connections at each site. Bill would only have to configure his own router and firewall at the office, *and only once*. Once this is configured, the master console will receive automatically all connections from all customer sites without further configuration. The servers will have to be added individually to the console, however, because for each site you must have the management password in order to connect.

### Typical use for outbound connections (master to slave)

Within a LAN, you may want to have multiple laptops connect to the same group of slave servers and manage them. In that case you don’t have to worry about routers and firewalls, since the standard Windows firewall is configured by BackupChain to allow incoming traffic to BackupChain’s service.

In this scenario you would configure each server to accept incoming connections, say on port 16888. Then on each device you want to use as a master, enable remote management and add each server individually. Configure it to be an *outbound* connection, enter the slave’s static IP address and port number, say 10.0.0.4:16888, and the slave’s password. This can be done to a number of master devices connecting to the same slave computers.

The same slave computer can also be configured to connect to multiple masters and also accept incoming connections from other masters. As you can see the system allows for a secure and flexible interconnection with various network patterns.

### General Recommendations for Setting up Remote Management

- Use static IP addresses everywhere, for your servers on the LAN as well as for your public internet router if the traffic is to go through the internet. The latter is not a must but a better solution because when the ISP changes the IP address of your router, the communication links will break.
- If any “smart/intelligent/sophisticated” firewall has to be crossed, turn on SSL encryption. This is because firewalls listen into the protocol and may mistake the data transfer as a security threat.
- You must turn on SSL encryption on all slaves if you plan to use it anywhere. It’s more secure but adds a small resource overhead per link. The same SSL setting (either on or off) has to be used on all connected devices.
- Make sure you choose a port number that is not being used by the software packages you normally deploy. In the case of Bill’s computer service example above, it only affects the receiving server. In the case where the link will be coming to a router through the internet, the port number has to be available for forwarding in the router as well.
- Stick to the same port number on all servers for simplicity
- Use high port numbers above 5000; those are generally not being filtered by ISPs or used by other services

- Use netstat -a to see which ports are being listened to on a particular server and help you choose a free port number.

### Troubleshooting Remote Management Connectivity

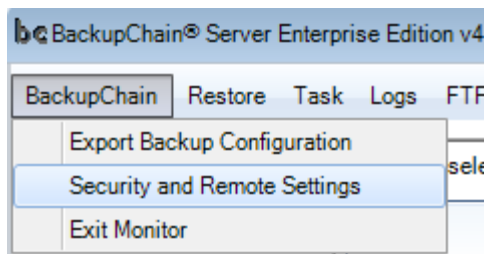
- Use netstat -a to see which ports are being listened to on a particular server and help you choose a free port number.
- Check the Remote Management Log, the log may be opened from the main menu
- Make sure the password and addresses are not misspelled
- All addresses should be static. Check with ping command that domain names resolve to the correct address
- Set up a local LAN test first before trying the connection from an external network. I.e. set up the master and connect another device to be the test slave connecting to the master. When the connection is confirmed to be working, try the connection from the external network or internet. This method eliminates the possibility of a local issue before you move on to the router and public firewall configuration.
- Some ISPs block certain port numbers on certain sites. It can happen that from your FL office you can connect fine but from a different office with a different ISP you can't. By the way, with most routers you can define several port numbers to be forwarded to the same internal address and port. This will allow you to connect to your home office site using different ports, such as billsitservice.com:16888, billsitservice.com:50000, etc. and all connections can be forwarded to the same internal server at 10.0.0.3:16888
- Turn off firewalls for a test if you suspect the connection is not coming through

### Step By Step Instructions for Centralized Management

In order to set up remote management you need to decide which topology you want to use. You can have slaves connect to the master console or the master connects to the slave, or combination of both methods.

#### Setting up the Master Console

From the main menu, open Security and Remote Settings:



In the screen that opens next you must set a password:

**Security and Remote Management Settings**

With this feature you can set up a password to protect your backup settings.

If you require a password, users cannot open the BackupChain user interface without it; hence, settings cannot be changed and backups cannot be stopped without authorization. Note that backups will continue to run inside BackupChain Service, which is an independent, separate process.

**The local network name of this server is: win2019**

☒ Require password to open BackupChain's Monitor Application  
Note: A password is required to enable remote management features.

Password:

Confirm password:

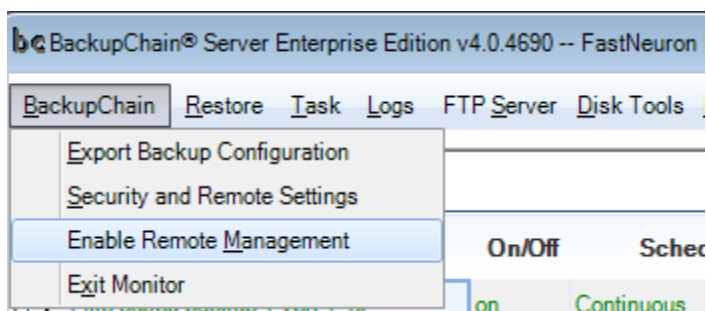
☐ Allow incoming remote management connections  
Port Number:

☐ Connect to remote master consoles  
Enter address or IP with port number. Example: 10.0.0.4:7700

☐ Use SSL links for enhanced security  
Note: all servers you connect together must use the SSL same setting. Use this option if intelligent firewalls need to be crossed.

OK Cancel

Once you set up a password (at the very least) you can click OK and then go back and Enable Remote Management:

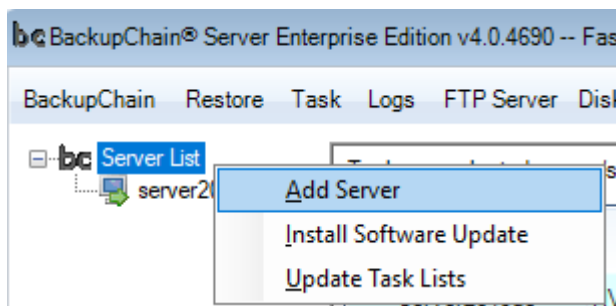


In order **to allow slaves to connect to the master server**, you need to open the Security and Remote Settings screen and check “Allow incoming remote management connections” **on the master computer**. You also have to specify a TCP port number. In our example above it’s 7700.

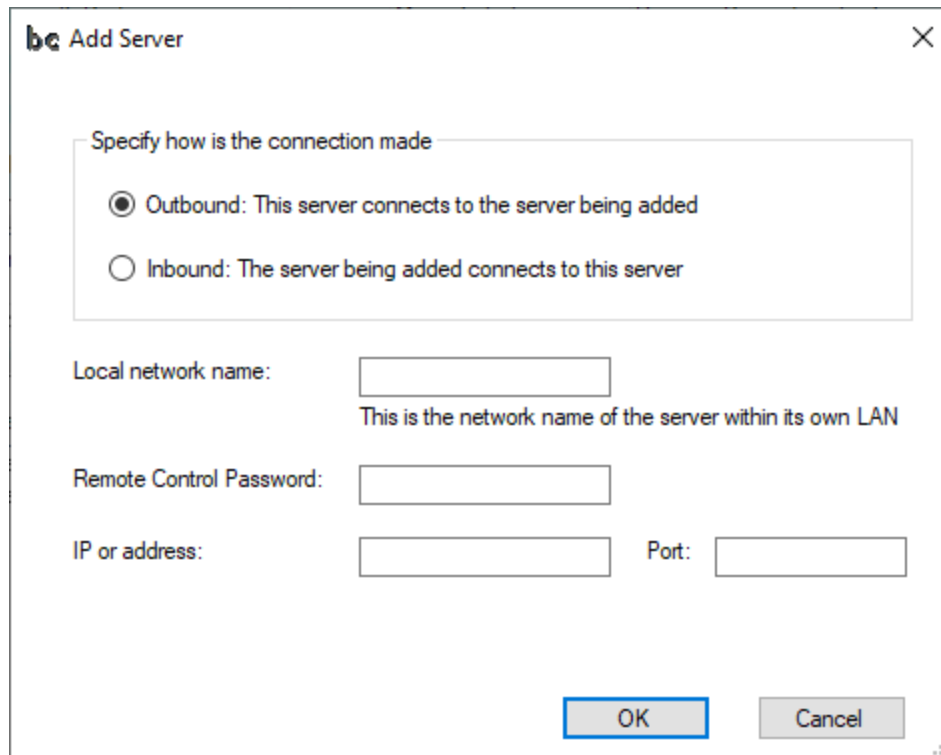
The SSL option should be checked if any remote management link will go through an intelligent firewall system or the internet or other public networks. Otherwise, firewalls might misinterpret the traffic as malicious and abruptly break the connection. The standard Windows Firewall, however, will work fine without the SSL option and requires no further configuration.

### Adding a Slave Server

Once you have enabled remote management by clicking on the option in the main menu (after having set up a password as described above), the main screen will split vertically. You will see a server tree on the left with the local host being already added below. Then right-click on top entry “Server List” and select “Add Server”:



On the screen that follows you can enter the slave’s details:



**bc Add Server** [X]

Specify how is the connection made

☒ Outbound: This server connects to the server being added

☐ Inbound: The server being added connects to this server

Local network name:   
This is the network name of the server within its own LAN

Remote Control Password:

IP or address:  Port:

OK Cancel

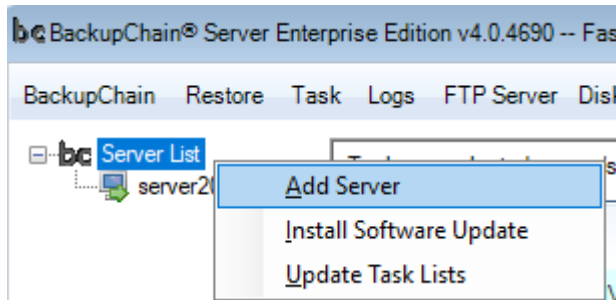
Here you need to specify if the slave will connect to this master server (**inbound**), or whether the master is supposed to connect to the slave (**outbound**).

For the inbound scenario where the slave connects to the master, you must provide the local network name and the remote control password. **The password you enter here is the one you defined in the slave's "Security and Remote Management" configuration screen.** Hence, the master can only control the slave if the master knows the slave's password as well as its network name; this is how trust is being established.

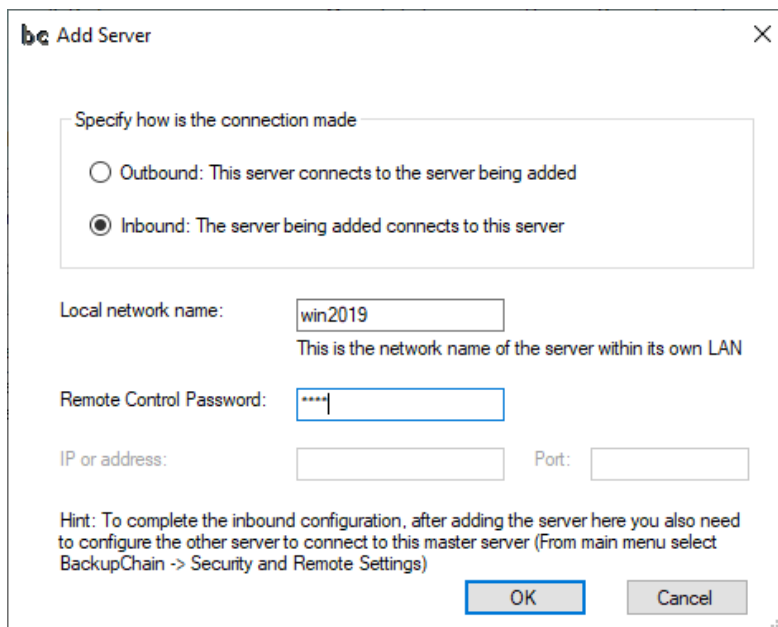
### Setting up Inbound Connections (Master Receives Link from Slave)

When you add the server in the master screen by right-clicking on “Add Server”, enter the network name and password exactly as it appears in the Security and Remote Management Settings **of the slave**.

Click Add Server:



And on the master side you enter:



Based on the slave's settings shown below (note the screen displays the network name “win2019”):

Security and Remote Management Settings

With this feature you can set up a password to protect your backup settings.

If you require a password, users cannot open the BackupChain user interface without it; hence, settings cannot be changed and backups cannot be stopped without authorization. Note that backups will continue to run inside BackupChain Service, which is an independent, separate process.

**The local network name of this server is: win2019**

☒ Require password to open BackupChain's Monitor Application  
Note: A password is required to enable remote management features.

Password:

Confirm password:

☐ Allow incoming remote management connections

Port Number:

☒ Connect to remote master consoles

Enter address or IP with port number. Example: 10.0.0.4:7700

mastersaddress.com:7700  
10.0.0.3:7700

☐ Use SSL links for enhanced security

Note: all servers you connect together must use the SSL same setting. Use this option if intelligent firewalls need to be crossed.

OK Cancel

Also note, the slave has a password defined and the option “Connect to remote master consoles” checked. In our example, this slave connects to two masters. One master is at mastersaddress.com:7700 and the other is a local master at 10.0.0.3:7700. The port number is 7700 and appears after the semicolon.

In the master’s Add Server screen we need to enter the network name “Win2019” so that the incoming connection can be matched to the password of that particular slave, which also has to be entered in the same screen. Only then the two can talk together.

## Setting up Outbound Connections (Master Connects to Slave)

In this example, we set up the same slave to be receiving the master's connection instead. From the master's perspective it's an *outbound* connection. For the slave it's therefore an *inbound* connection. Hence, we need to "allow incoming management connections" and we choose port 7700 as shown below:

Security and Remote Management Settings

With this feature you can set up a password to protect your backup settings.

If you require a password, users cannot open the BackupChain user interface without it; hence, settings cannot be changed and backups cannot be stopped without authorization. Note that backups will continue to run inside BackupChain Service, which is an independent, separate process.

The local network name of this server is: **win2019**

☒ Require password to open BackupChain's Monitor Application  
Note: A password is required to enable remote management features.

Password:

Confirm password:

☒ Allow incoming remote management connections

Port Number:

☐ Connect to remote master consoles

Enter address or IP with port number. Example: 10.0.0.4:7700

☐ Use SSL links for enhanced security

Note: all servers you connect together must use the SSL same setting. Use this option if intelligent firewalls need to be crossed.

OK Cancel

All we need to do at the slave side is to set the password and allow incoming remote management connections.

On the master we need to configure the slave and **tell the master to connect to the slave**, which is an outbound connection:

**bc Add Server** [X]

Specify how is the connection made

☒ Outbound: This server connects to the server being added

☐ Inbound: The server being added connects to this server

Local network name:   
This is the network name of the server within its own LAN

Remote Control Password:

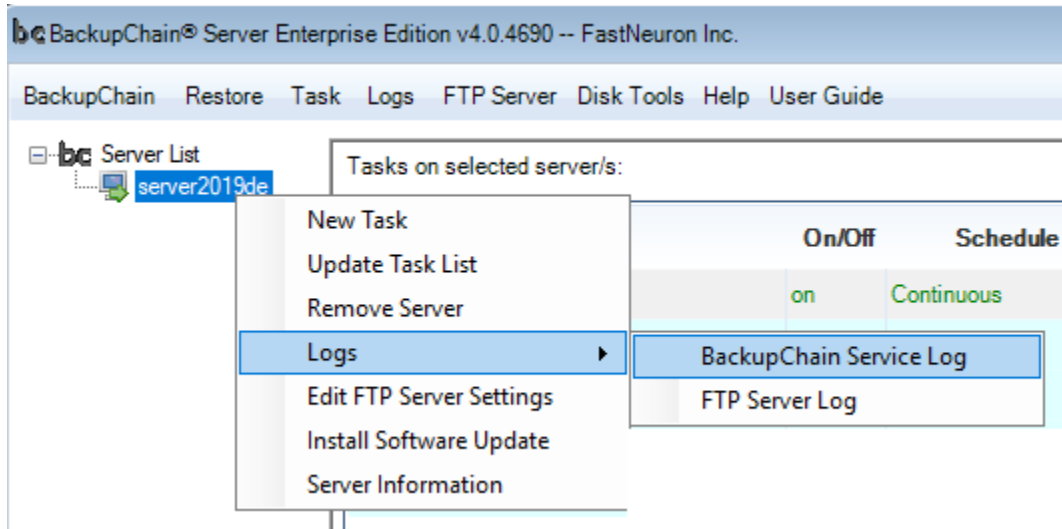
IP or address:  Port:

Note that here **we must provide the local network name** for identification purposes, the remote management password entered in the previous screen on Win2019, and the address or IP address of Win2019 and port number, which in our example are 10.0.0.99 and 7700, respectively.

These settings tell the master where the slave is, what the password is (to establish trust), and that we want the master to connect the slave (outbound); hence, we have to provide the address of the slave (10.0.0.99 or network name on LAN) and the port number.

## Managing Remote Servers

Once the remote server is added, you can see all tasks of all servers listed one underneath the other by selecting the top entry “Server List”. By right-clicking on a particular server, you see additional actions available for each server:



“New Task” creates a new task on the selected server.

“Update Task List” requests an up-to-date task list from the server. The master already periodically makes such requests automatically; however, with this function you can force it to occur immediately.

“Remote Server” removes the server entry from the tree.

“Logs” allows you to load on of the remote server’s main service logs.

“Edit FTP Server Settings” opens the FTP settings at the remote server site.

“Install Software Update” opens the Software Installation Screen where you can remotely update the software of all or selected connected servers.

“Server Information” displays additional server details of the connected server.

## Restoring Files on Remote Servers

In order to start a restore process, you need to log on to the server where the restore process is supposed to run. Note, however, that in LAN environments you can use UNC paths as targets, with document based backups; i.e. you can run the restore process on any server via UNC and pull backup files from another server, and also write the restored data over UNC to any other server. While all kinds of backup tasks can be restored **from** UNC, restoring **to** UNC paths may only be done for documents and offline virtual disks. Note that VMs cannot be integrated automatically into Hyper-V Manager over the

network. For VMs to be added back into the Hyper-V Manager, you need to run the restore locally on the server that is to receive the restored VM.

### **Managing Backups on Remote Servers**

You can manage backups on remote servers from the master server as if you are connected locally. Folder, file, and physical disk selection is passed through as if it were local.

The time in the log view is displayed in the local time zone of the viewer. If your remote servers are in a different time zone, the time shown in the time column is adjusted automatically.

Note that the refresh of remote server backup progress will be slower than that of the local server. Also there may be a delay when you request certain operations, due to the packet roundtrip time to and from the destination. It may take a few seconds before the remote server reacts to a particular command, depending on link conditions and distance.

## Troubleshooting

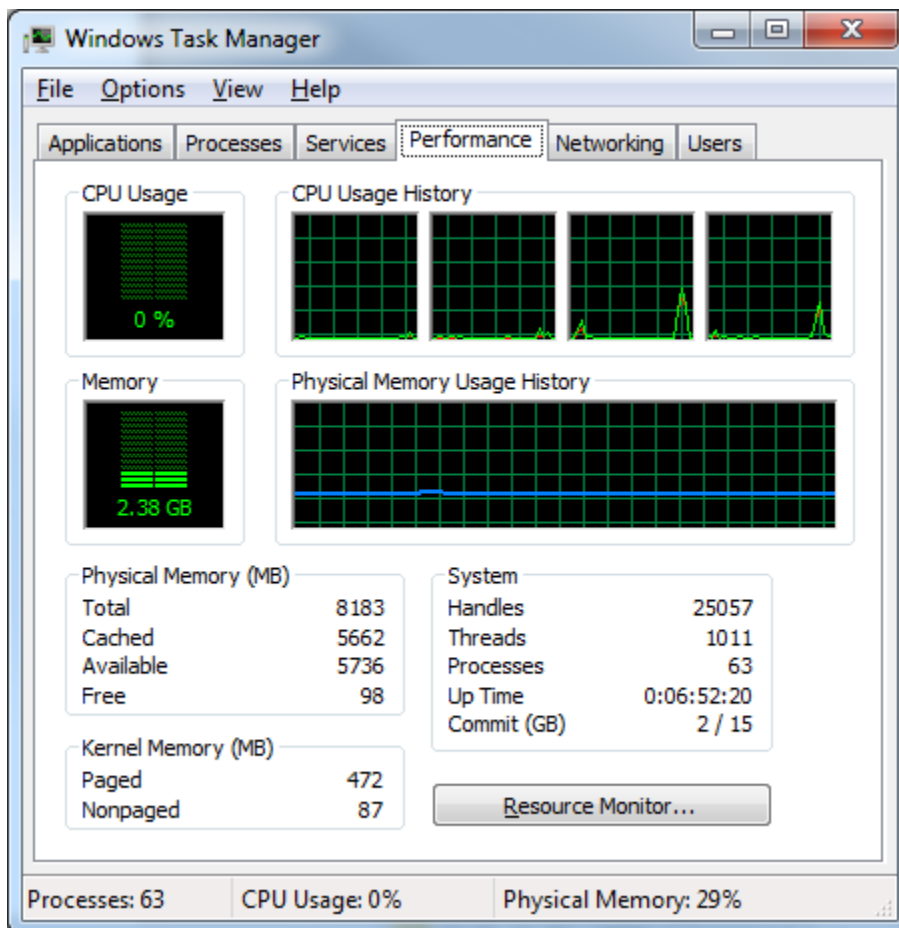
Please visit our website <http://backupchain.com> for up-to-date information.

## General Recommendations

This section discusses various recommended practices when working with BackupChain.

### RAM

Please ensure you have at least 512 MB free or available at all times, as reported by the task manager:



Note, BackupChain will log warnings if available RAM or system drive free disk space are too low during backups.

## System Settings

It is recommended to use a Windows managed page file on drive different than the boot drive for better performance.

In addition, if your server is rather busy during backup, check the amount of space limit assigned to each drive's shadow storage, using this command:

```
vssadmin list shadowstorage
```

Try to assign as much space as feasible for shadow storage, especially on drives that are involved in heavy disk I/O during backup. Fortunately, you can also use a different drive for this type of storage:

```
vssadmin Resize ShadowStorage /For=C: /On=C: /MaxSize=1024MB
```

```
vssadmin Resize ShadowStorage /For=C: /On=D: /MaxSize=UNBOUNDED
```

Note that this space won't be allocated until it's necessary; hence, it's more like an upper limit cap.

## Windows System Restore and Other Backup Tools

Ideally BackupChain backups should not overlap with other backups or the Windows System Restore feature. You can check the Task Scheduler in the Windows Control Panel to edit the System Restore task.

## Simultaneous Backups

Simultaneous backups are possible if you schedule backups to run overlapped. It's not recommended, however, to run too many concurrent backups due to the system stress it causes.

## Hyper-V Backups

Microsoft does not recommend using snapshots/checkpoints in production environments. The use of snapshots dramatically reduces performance and also increases complexity. In addition, snapshotted VMs may only restore on similar hardware because they contain processor dependent and other hardware dependent information.

Many Hyper-V users apply snapshots to create “backups”; however, snapshots aren’t backups as they are stored on the same disk as the original. If you want to keep older versions of your virtual machines, simply back them up with BackupChain manually or in scheduled intervals. This is far more efficient and does not involve a run-time performance penalty.

## Speed Settings

At least initially most users like the idea of a super-fast backup, the reality is that it puts a strain on your hardware and may impact the server’s responsiveness. For that reason, and especially in a cluster shared volume setting, we recommend limiting the backup to one CPU core, using the lowest task priority, and limiting the read I/O speed of BackupChain to about 15 to 50,000 Kbyte/second as a starting point.

To fine-tune this number, take into account your RAID speed and the average load on the hard drives, relative to their read and write speeds. Also, consider that burst speeds may be multiples of the actual long-term data access speeds. Modern hard drives may burst at over 150MB/sec but only give you a reliable 60MB/sec when reading sequential data.

Defragment your drives as well as your VMs from within often. Defragmentation on the host is recommended if you are using dynamically expanding virtual disks. If you use SSDs there is specialized defragmentation software available that will reduce the wear on the drive’s cells and thereby prolong its life.

For better speed consider using a RAID stripe array with mirror (optionally).

Schedule backups at a time when user access is limited.

Use a gigabit network target, ideally using a dedicated network access adapter just for backup data and with a dedicated connection to the storage devices.

## General Recommendations

Reboot your VMs regularly to spot problems early on. A boot error may go undetected and your backup history may not be long enough to restore everything to a bootable state.

Take offline backups at regular intervals in addition to live backups. Shutting down and rebooting will also give you an additional assurance that the VM is in a good state (no boot errors or other disk errors during boot).

Some viruses target the boot sectors of VMs and you may not notice the damage until you reboot. Other common sources of boot problems include: Windows Update, Virus Scanner updates, and other software installations or uninstalls.

## Frequently Asked Questions

Also see <http://backupchain.com/faq/> and <http://backupchain.com/v2help/BackupChainV2Help.html> for up-to-date information.

### What is the FastNeuronDelta file extension?

FastNeuronDelta is the proprietary file format for deduplicated file backup chains.

.1.FastNeuronDelta files are full file copies (which may be data compressed as well).

.0.FastNeuronDelta files are increments or differentials of the above.

In order to restore a delta deduplicated file, you must access to have the latest full copy as well.

### What is the FastNeuronDate extension?

It's a placeholder for a file date. It's used for file systems that do not support file date modification, such as standard FTP.

### Will My Backups Run If I Log off?

Yes, BackupChain runs as a Windows Service in a background (see "FastNeuron BackupChain", Control Panel -> Services / Service Manager). You can use the Service Manager to change the default user used by the service (default is BackupChainAgent).

### How can I reduce RAM Usage?

Choose a lower delta block size in Deduplication tab, and limit to one CPU core in the Speed tab.

### Can I Rename a Task?

Yes, in the Options tab.

## Can I Move the Backup Folder?

Yes. Please stop the backup and disable the task first and then ensure all files are moved beginning with the backup's root folder.

You will see subfolders, such as C\_ or <server name>, in the root folder, as well as several BackupChain.config\* files.

Move all these to a new location without modification and then point BackupChain's target to the new folder.

## Can I Restore Several Backups Simultaneously?

Yes, each one opens in its own new window.

## Can I Backup Files in their Native Format?

Simply switch off deduplication in the Deduplication tab. Uncheck the option "Activate Deduplication (Delta Compression)", and switch off data compression in the Compression tab by unchecking "Turn on compression to save space"

## How do I get a Full Backup Every Time the Backup Runs?

Simply switch off deduplication in the Deduplication tab. Uncheck the option "Activate Deduplication (Delta Compression)".

## How can I Get all my Files Compressed using ZIP?

Ensure compression in the Compression tab is enabled ("Turn on compression to save space" is checked) and check the following in the Files Types tab table:

The row \*.\* (all files) should have 'data compression' checked and 'file deduplication' *unchecked*.

This will turn off deduplication but keep data compression on for all files.

Now remove all other rows in the table so there is just one entry left for the \*.\* extension.

For quicker deletion, you can use the DEL key on your keyboard to delete the rows in the table.

## What is the Name of BackupChain's Background Service?

"BackupChain Service". You can change the service settings via the Windows Control Panel, then Services or Service Manager.

## How Can I limit the Number of File Versions Retained in the Backup Folder?

Every time the backup runs it looks for changed files. If a file was changed, BackupChain will create a new file version for it in the backup folder or backup store. The default is to keep the last 10 copies of each file. Note: a new version is only created if the file has actually changed.

To change the settings, open the File Versioning / Cleanup tab and edit the table:

Folders	Files	Exclusions	Backup Target	File Versioning / Cleanup	Deduplication	Schedule	Options	Compression	Verification	Speed	Log	Log Options	Notes	Progress
Define below how you would like files to be backed up, depending on their file type:														
Extension	Min. Number of File Versions	Compression	Min. File Age	Deduplication	Delayed Deletion Period	Archive Period								
*.*	10	<input checked="" type="checkbox"/>	0 secs	<input type="checkbox"/>	Never delete	Forever								
*.pst	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever								
*.msg	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever								
*.ac2	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever								
*.org	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever								
*.accdb	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever								
*.adl	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever								
*.apr	10	<input checked="" type="checkbox"/>	0 secs	<input checked="" type="checkbox"/>	Never delete	Forever								

Note: If \*.\* is defined, it will be used if there is no exact file extension match.  
 Min. Number of File Versions defines the number of file versions you want to keep for each file, before automatic cleanup occurs.

Add Remove

You can set the 'Min. Number of File Versions' parameter to "No Backup" to completely omit a specific file type, or to "ALL" to keep all file versions forever. Otherwise, enter a number and BackupChain will clean up old backups as soon as the number of versions crosses that limit. See previous chapters for in-depth discussion of this feature.

## How Can I Limit Bandwidth Usage?

Open the task's Speed tab and enable speed limits.