



# CBMR For Windows

## Cristie Bare Machine Recovery

### User Guide

Version 9.6.1 released April 2024

**Copyright © 1998-2024 Cristie Software Ltd.**  
**All rights reserved.**

The software contains proprietary information of Cristie Software Ltd.; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between Cristie Software Ltd. and the client and remains the exclusive property of Cristie Software Ltd. If you find any problems in the documentation, please report them to us in writing. Cristie Software Ltd. does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of Cristie Software Ltd.

- *IBM Tivoli Storage Manager (TSM), AIX and TIVOLI are trademarks of the IBM Corporation.*
- *IBM Spectrum Protect is a trademark of the IBM Corporation.*
- *IBM Virtual I/O Server (VIOS) is a trademark of the IBM Corporation.*
- *NetWorker and Avamar are trademarks of the Dell EMC Corporation.*
- *vSphere, vCenter and vCloud are trademarks of VMware Inc.*
- *Hyper-V is a trademark of Microsoft Corporation.*
- *Azure is a trademark of Microsoft Corporation.*
- *Amazon Web Services (AWS) and Amazon Elastic Compute Cloud (EC2) are trademarks of Amazon.com, Inc.*
- *Cohesity DataProtect is a trademark of Cohesity Inc.*
- *Rubrik is a trademark of Rubrik Inc.*
- *CloneManager® is a registered trademark of Cristie Software Ltd.*
- *SysBack is a registered trademark of Cristie Software Ltd.*

PC-BaX, UBax, Cristie P4VM (Protect for VMs), Cristie Storage Manager (CSM), SDB, ABMR (Bare Machine Recovery for EMC Avamar), NBMR (Bare Machine Recovery for EMC NetWorker), TBMR (Bare Machine Recovery for Spectrum Protect/TSM), CBMR (Cristie Bare Machine Recovery), CoBMR (Bare Machine Recovery for Cohesity DataProtect), RBMR (Bare Machine Recovery for Rubrik) and CRISP (Cristie Recovery ISO Producer) are all trademarks of Cristie Software Ltd..

Cristie Software Ltd  
New Mill  
Chestnut Lane  
Stroud  
GL5 3EW  
UK

**Tel: +44 (0) 1453 847009**  
**Email: [support@cristie.com](mailto:support@cristie.com)**  
**Website: <https://www.cristie.com>**



# Contents

<b>1</b>	<b>Document conventions</b>	<b>4</b>
<b>2</b>	<b>Introduction</b>	<b>5</b>
<b>3</b>	<b>Using CBMR for Disaster Recovery</b>	<b>6</b>
3.1	Preparation .....	6
3.1.1	Create The Bootable Recovery Environment .....	7
3.1.2	IBM Spectrum Protect Client Version .....	7
3.1.3	Creating an IBM Spectrum Protect Node .....	7
3.1.4	IBM Spectrum Protect Servers Requiring SSL/TLS Registration .....	8
3.1.5	Transitional Nodes .....	9
3.2	The Create Configuration Wizard .....	9
3.2.1	Storing Configuration Parameters .....	10
3.3	Creating and Testing DR Backup .....	12
3.4	Restoring Your System .....	17
<b>4</b>	<b>WinPE5, WinPE10 or WinPE11 based CBMR Recovery Environment</b>	<b>19</b>
4.1	CBMR Recovery Environment Main Menu .....	20
4.2	Begin the Restore Process .....	23
4.2.1	Logfile Save Path .....	23
4.2.2	Select Restore Type .....	25
4.2.3	File Restore Type .....	25
4.2.4	IBM Spectrum Protect Restore Type .....	27
4.2.5	FTP Restore Type .....	31
4.2.6	Specify Key Repository .....	32
4.2.7	Storage Pools .....	34
4.2.8	Confirm Volume Layout .....	38
4.2.9	Select Datasets to Restore .....	43
4.2.10	Clone Settings .....	44
4.2.11	Dissimilar Hardware .....	45
4.2.12	Disk Recovery Sequence .....	47
4.2.13	Disk Scaling .....	49



# 1 Document conventions

The following typographical conventions are used throughout this guide:

<code>/etc/passwd</code>	represents command-line commands, options, parameters, directory names and filenames
<a href="#">Next &gt;</a>	used to signify clickable buttons on a GUI dialogue
<b>Note:</b>	describes something of importance related to the current topic



## 2 Introduction

CBMR provides complete data protection, as well as the ability to recover critical servers from scratch within minutes. CBMR can be used as a standalone backup product and provides an ideal solution for server migration.

CBMR backs up the operating system and hard disk configuration of critical servers, enabling rapid recovery of data to an identical state following damage to or failure of the physical hardware, or a corruption of the operating system.

Please refer to the supplied Readme document for a list of supported Windows OS's.

CBMR also provides the ability to clone to a new machine from an existing backup. The cloning option allows the hostname and/or the IP address to be changed during the recovery.

CBMR is available as a single edition suitable for all platform types. You must have one of the supported Windows™ Operating Systems correctly installed prior to proceeding with the installation of CBMR.

To minimise the impact of a system failure, you need to have a restore strategy in place. CBMR allows you to recover Windows Workstations and Servers without first having to re-install the operating system or backup software. This reduces the recovery time significantly. All you need is disaster recovery media from which to boot your computer and a disaster recovery backup of the original Windows system.

Finally, a full backup of the system can be restored using the backup features of CBMR or any other preferred third party Backup/Restore software.

Backups can be performed to a variety of different Backup Locations and media, including IBM Spectrum Protect, tape, ftp, disk, network-attached storage etc.

**IMPORTANT:** Refer to the installed Readme file for any limitations and last minute updates.



## 3 Using CBMR for Disaster Recovery

This section describes the essential elements of CBMR when used for Disaster Recovery (DR).

If you wish to use CBMR in standard backup/recovery mode please refer to section CBMR in More Detail.

CBMR can protect a system against disaster all the time, if set up and configured correctly. The following sections explain this procedure.

*Note: When using a CBMR backup to recover a Windows Domain Controller the recovered system will boot twice.*

### 3.1 Preparation

To use CBMR in a production environment for DR purposes, you must follow the procedure in the order listed below:

1. **Installation** (refer to the [CBMR Installation and Licensing Guide](#))
  - Install the CBMR Backup and Restore software
  - License the Software (using a Trial or Full license)
2. **Prepare the WinPE5, WinPE10 or WinPE11 DR USB flash drive drive or ISO/CD-ROM** (refer to the [Cristie Recovery ISO Producer User Guide](#))
  - Install and run the Cristie Recovery ISO Producer (CRISP) tool on a suitable system to create the CBMR WinPE5, WinPE10 or WinPE11 based DR environment in either USB flash drive or ISO form. The ISO may then be burnt to CD or DVD physical media if required. This only needs to be done once.
3. **Machine Configuration**
  - Save the Machine Configuration parameters. These are saved automatically each time a DR backup is started. No further User action is required.
4. **Backup system (OS) and User data**
  - Perform regular Disaster Recovery backups as required. This can be scheduled daily, monthly, weekends only etc. using the CBMR scheduler interface to the Windows Scheduler.
  - Add any extra standard data backups as required

You will then be ready to Restore the system from the Disaster Recovery Backup in conjunction with the DR media when required.

*Note if using IBM Spectrum Protect, check the IBM Spectrum Protect BA Client version in use on your server. Also refer to [Create a IBM Spectrum Protect Client Node](#).*

**To perform a Bare Machine Recovery you must:**

1. Boot into the DR environment on the machine to be restored from the CBMR WinPE5,



WinPE10 or WinPE11 DR USB flash drive, CD or DVD.

2. Perform a system recovery from the specified backup location. If this is a dissimilar system make sure you have the necessary drivers for the new disk controllers.
3. Perform conventional data recovery from your third party backups if necessary.

### 3.1.1 Create The Bootable Recovery Environment

The supplied CRISP tool is used to create the CBMR recovery environment. This is based upon a customised version of Microsoft's WinPE5, WinPE10 or WinPE11 environment.

CRISP should be run in conjunction with the supplied CRISP WinPE5, WinPE10 or WinPE11 Fileset for CBMR 9.6. The fileset will be installed automatically alongside the CRISP on the same host or technician machine.

A full discussion of how to install and run CRISP is contained in the separate [CRISP User Guide](#). Note that the CRISP does not need to be installed on the system to be backed up; any suitable machine will do.

Output from the CRISP tool is a bootable WinPE5, WinPE10 or WinPE11 USB flash drive or ISO file. The latter can then be burnt to physical media (CD or DVD) or mounted directly in a VM environment.

Once created the recovery environment is booted on the target system which then drives the restore process.

### 3.1.2 IBM Spectrum Protect Client Version

If you intend to use IBM Spectrum Protect as your backup location it is important to check the version of the IBM Spectrum Protect Client installed on your machine. Versions supported by CBMR are summarised in the [Readme](#) document.

**Note:** Please refer to the [Readme](#) document for the latest client support details.

If you are not using IBM Spectrum Protect, please skip this step.

### 3.1.3 Creating an IBM Spectrum Protect Node

This step is only required if IBM Spectrum Protect is used in the recovery procedure. Please ignore this step if IBM Spectrum Protect is not being used.

CBMR will connect to a IBM Spectrum Protect server as a client node. The machine's operating system files and other important files will be stored under a Filespace in the client node. If you need to create a Client node using the [IBM Spectrum Protect Admin Client](#), refer to the IBM Spectrum Protect Administrator Guide for further information.

To use the IBM Spectrum Protect module, you must enable CBMR to backup to the IBM Spectrum Protect by creating a dedicated node via the IBM Spectrum Protect Admin client.

The settings required for the node are:



<b>Archive Delete Allowed</b>	YES
<b>Backup Delete Allowed</b>	YES
<b>Client Compression setting</b>	CLIENT
<b>Force password reset</b>	NO
<b>Node Type</b>	CLIENT

In addition, you must consider your password policy. If you specify a Password Expiration period, you will have to set the password in CBMR every time the password expires.

*Note: automatic password generation for the client nodes is supported in CBMR 5 and later.*

### Additional Configuration to Maintain Multiple Backup Versions

If it is required to hold more than one version of the DR backup in the same filespace, then the node must be setup correctly to support this.

You must have a Management Class (MC), which contains a Backup Copy Group (BCG) and an Archive Copy Group (ACG). Your node needs to be registered to use the MC.

The parameters of the BCG of interest are:

- Versions Data Exists = 2
- Versions Data Deleted = 1
- Retain Extra Versions = 30
- Retain Only Version = 60

In this example, there can be two versions of an object. The Versions Data Deleted attribute specifies the maximum number of different backup versions (1 in this case) retained for files and directories that you erased from your file system. This parameter is ignored as long as the file or directory remains in your file system.

The expiration date for the remaining versions is based on the retain extra versions and retain only version parameters. In the example, if there is more than one version and one is deleted, the deleted one will be kept for 30 days. The only remaining copy of the object will be retained for 60 days (that is AFTER you make it inactive).

*Note: if several versions of a DR backup are maintained in IBM Spectrum Protect, the WinPE5, WinPE10 or WinPE11 recovery environment will allow you to choose a specific version to restore.*

### 3.1.4 IBM Spectrum Protect Servers Requiring SSL/TLS Registration

To enable CBMR to use IBM Spectrum Protect servers configured to use SSL/TLS certificates, the host system must be first registered with the server. This is now the default configuration for servers version 8.1.2 or later.





A suitable certificate can be registered by running these commands:

1. Copy the IBM Spectrum Protect SSL/TLS certificate to a local folder on the host system.
2. Run a command shell on the host system.
3. Change directory to the folder **C:\Program Files\Tivoli\TSM\baclient** (assuming the default install location was used for the IBM Spectrum Protect client).
4. Run the following command:

```
dsmcert.exe -add -server <server_ip_or_name> -file <path to certificate>
```

The command will indicate success or failure of the registration process.

### 3.1.5 Transitional Nodes

If you backup to a node located on an IBM Spectrum Protect Server version 7.1.8 or 8.1.2 and above, using an IBM Spectrum Protect version earlier than 7.1.8 or 8.1.2, you may have to change the node **Session Security** setting to **"Transitional"** after your Disaster Recovery.

This is because the Disaster Recovery environment contains a CBMR client version later 8.1.2 or later that enforces SSL communication. This will prevent older IBM Spectrum Protect clients from accessing the node.

You can set this by updating the node with the command:

```
UPDATE <node_name> SESSIONSECURITY=Transitional
```

## 3.2 The Create Configuration Wizard

Configuration information is stored within the DR backup itself. As part of this process, details relating to hard disks, operating system, storage controller(s), network adapter(s) and network settings are stored. You can override some of these details if you wish.

The next section discusses this in detail.

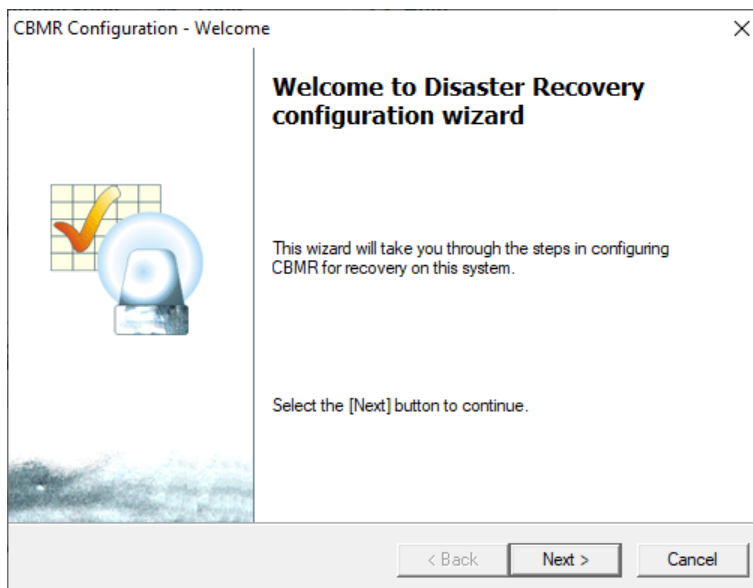


### 3.2.1 Storing Configuration Parameters

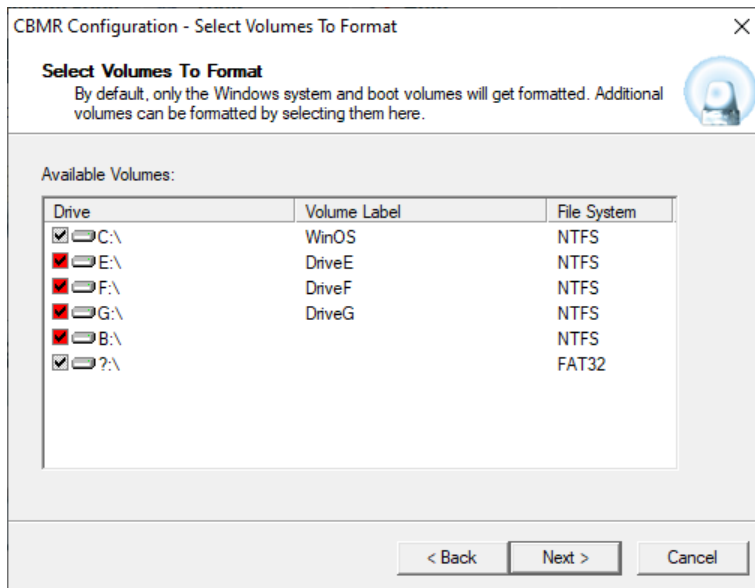
In the CBMR main window, click on **Setup Disaster Recovery Configuration**:



The **CBMR Configuration - Welcome** dialogue will appear.

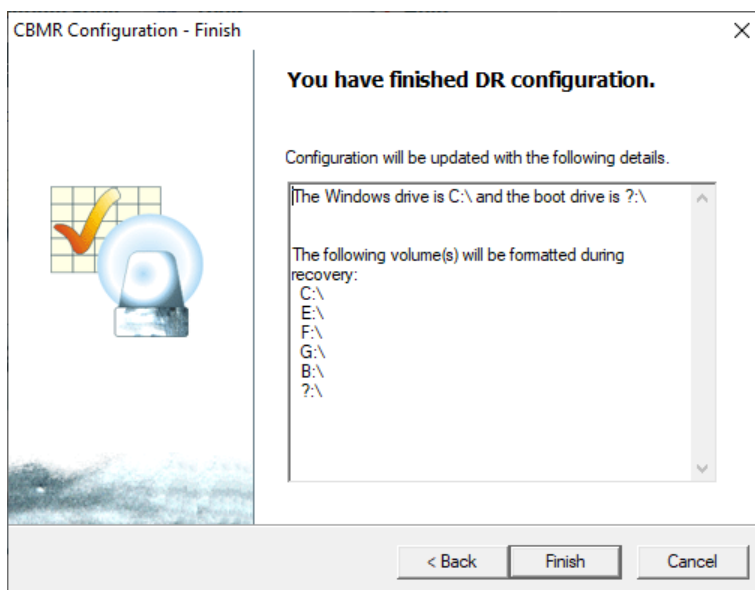


Select **Next>** and the **CBMR Configuration - Select Volumes to Format** dialogue will help you to select the disks and partitions which should be formatted during a recovery:



The Windows boot and system partitions will be selected by default and you cannot exclude them. All other volumes and partitions can be selected or de-selected by clicking on the selection box which toggles the current selection.

Click on [Next>](#) to confirm the disks/partitions for formatting.



Check that all your selections are correct. If you need to modify any of these settings, choose the [Back](#) button and modify your selection.

Finally, click [Finish](#) to save the settings. When a DR backup is run, the configuration information will be stored to a folder **CBMRCFG** on the Windows drive. This folder will be automatically included with the backup. This folder should never be removed manually, nor its attributes or contents changed.



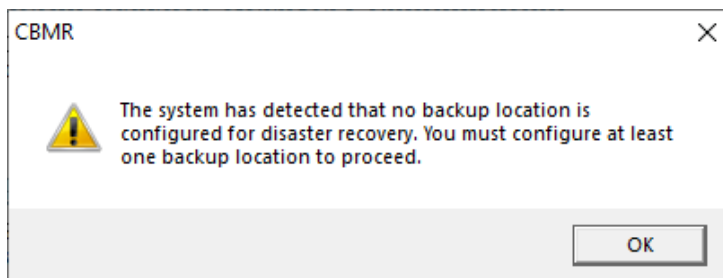
### 3.3 Creating and Testing DR Backup

For locally attached physical Backup Locations (ie tape, library auto-loader or local disk), insert a clean tape in the tape drive or ensure there is enough space on the backup disk.

Click on the **Run** or **Schedule Disaster Recovery Backup** option in the CBMR main window:

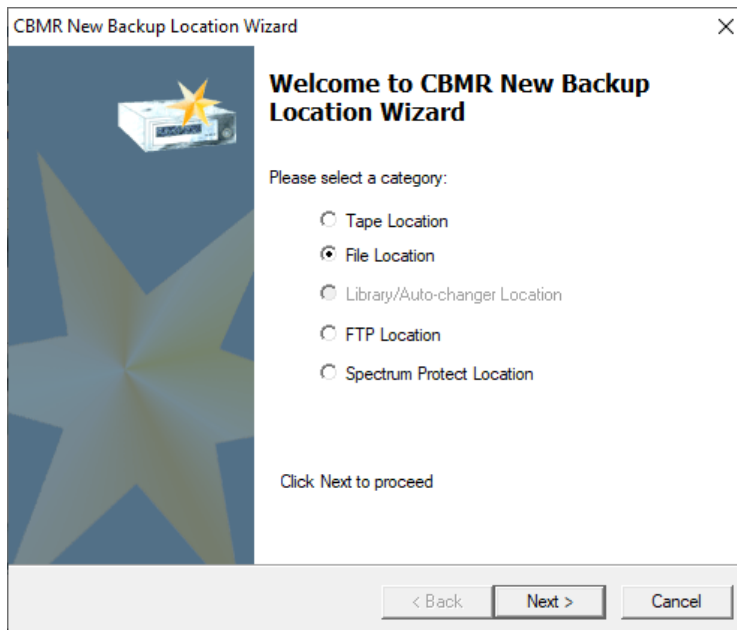


At least one Backup location must exist in order to proceed through the wizard. If none have been previously configured, you will see a message that indicates this.



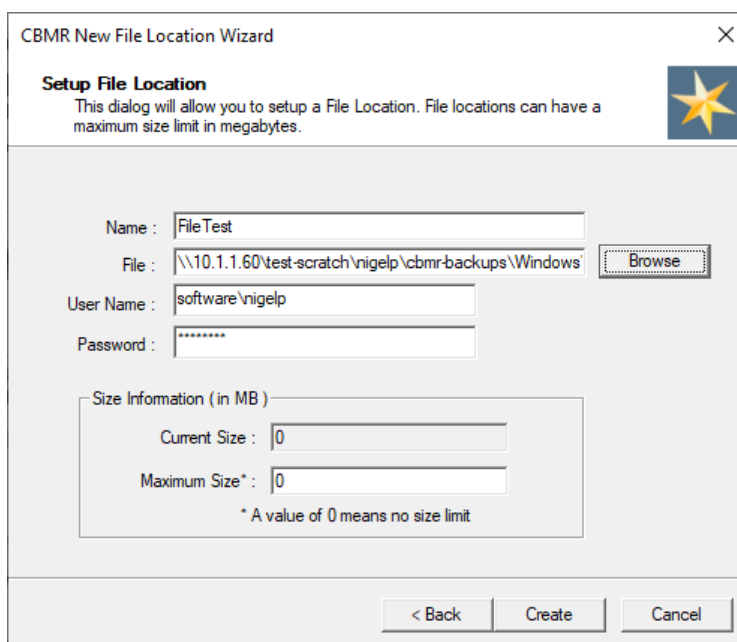
Click **OK** to accept the message.

This will open the **CBMR - New Backup Location Wizard** welcome dialogue.

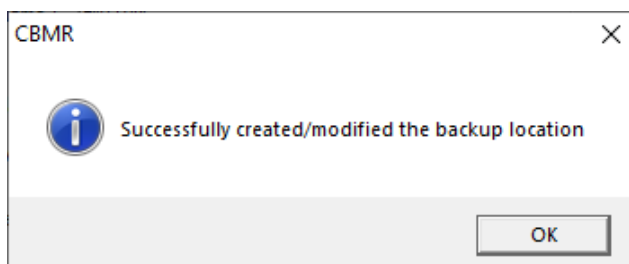


Select the Category of Backup required, for example, **File**.

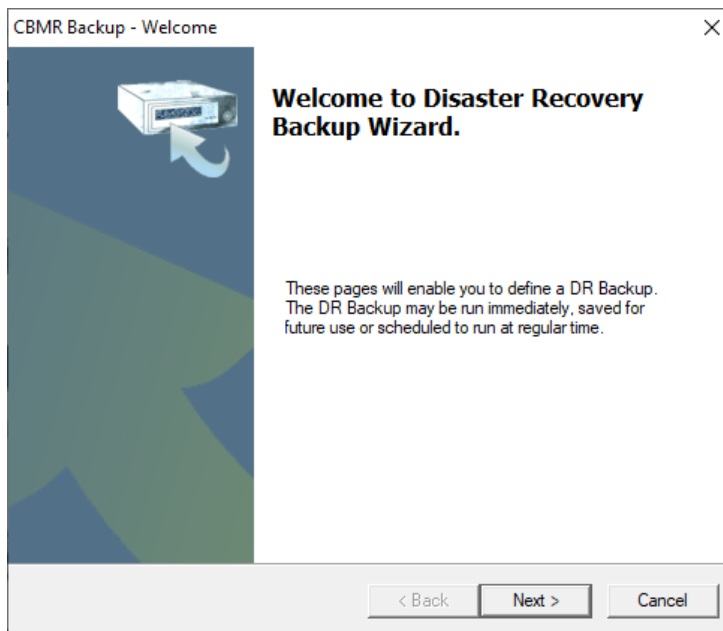
Select **Next>** to continue and the **CBMR - New File Location** Wizard is displayed:



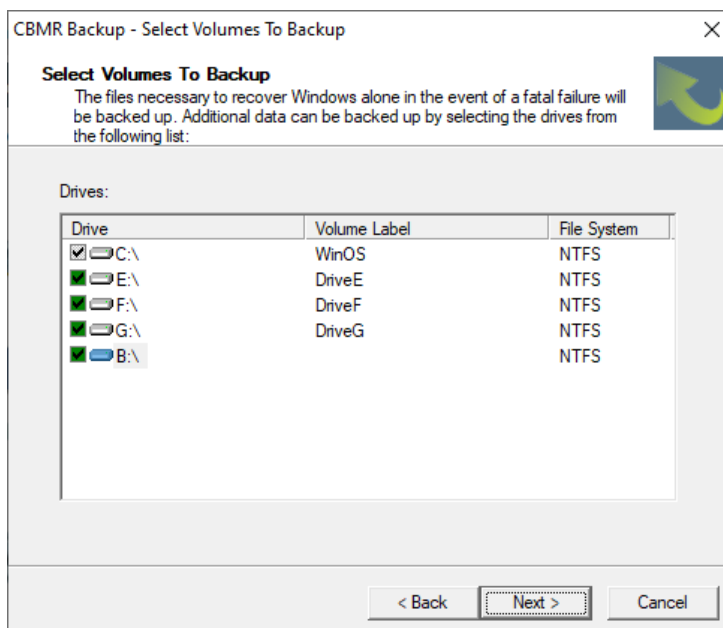
Click **Create** to create the specified File Location. This is confirmed thus:



Click **OK** to continue and the following dialogue is displayed:

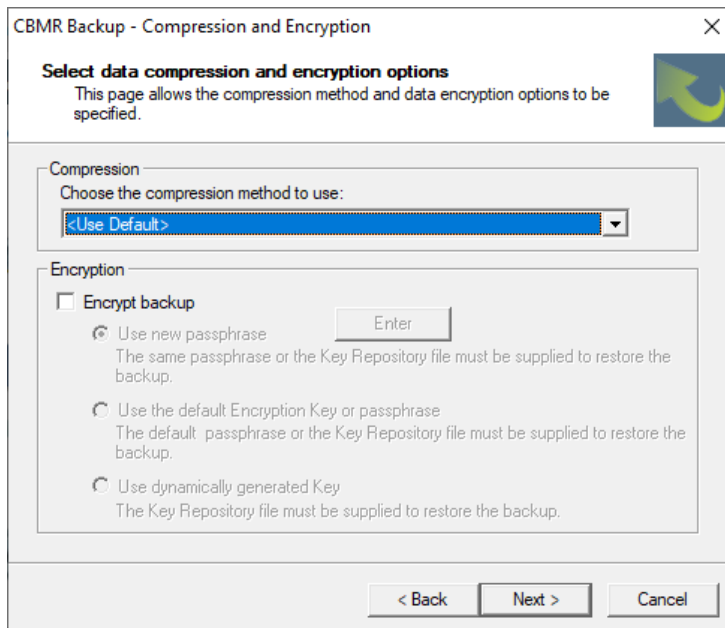


Click **Next>** and the **CBMR Backup - Select Volumes To Backup** dialogue is displayed:



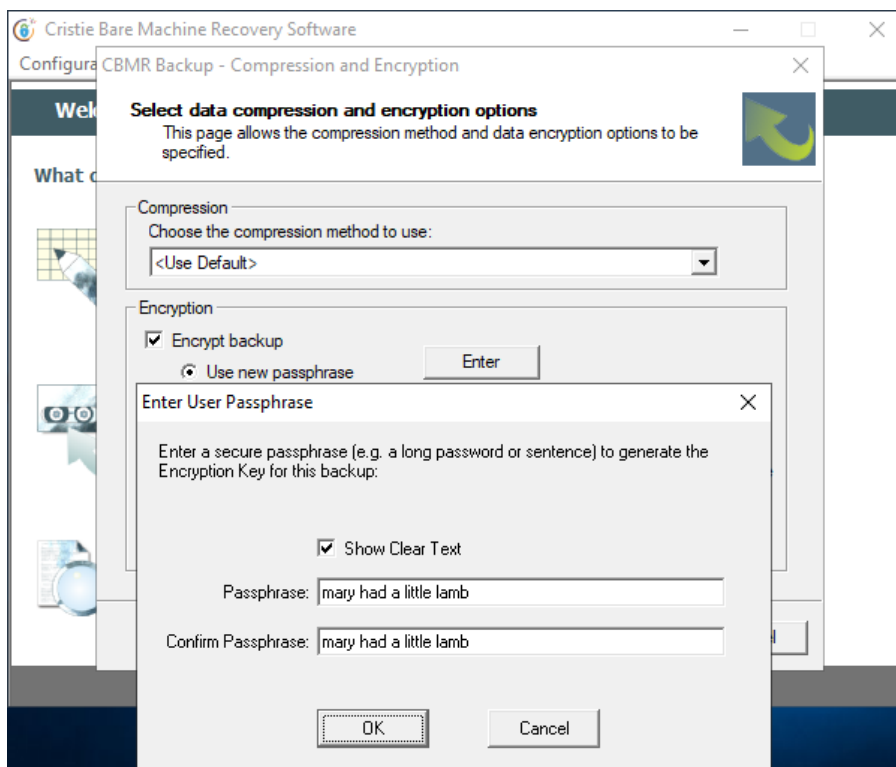
The dialogue shows all the available hard disk drives (including any partitions mounted on folders). You can select all or a sub-set as required. Whatever you choose, the Windows folder, the IBM Spectrum Protect installation folder (if installed), the Registry, "Documents and Settings" folder and CBMR folder will always get backed up.

Select **Next>** to open the **CBMR Backup - Compression and Encryption Options** dialogue:



Select **<Use Default>** to accept the default compression method. Alternatives are available via the drop-down menu.

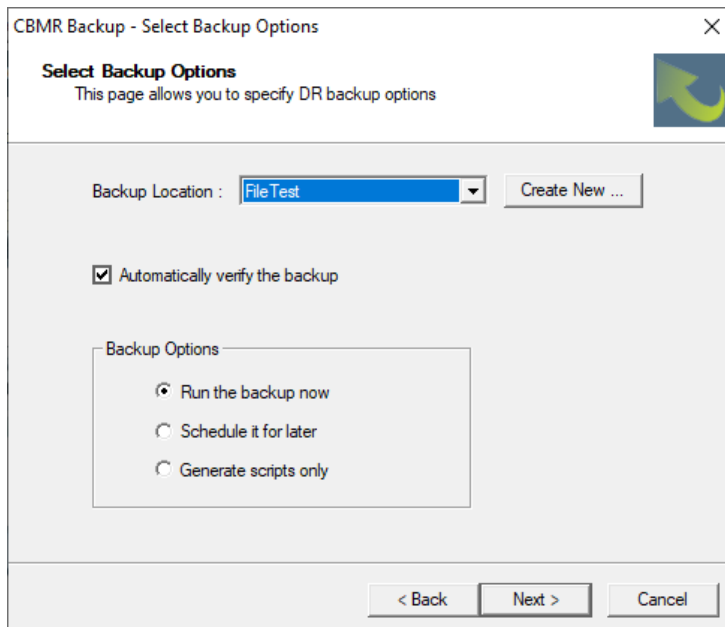
If you wish to encrypt the DR backup, select the **Encrypt backup** tick-box.



Use either the system default key or enter a new passphrase or key. Click **OK**.

Select **Next>** to display the **CBMR Backup - Select Backup Options** dialogue:





CBMR Backup - Select Backup Options

**Select Backup Options**  
This page allows you to specify DR backup options

Backup Location : **File Test** Create New ...

☒ Automatically verify the backup

Backup Options

- ☒ Run the backup now
- ☐ Schedule it for later
- ☐ Generate scripts only

< Back Next > Cancel

The **Automatically verify the backup** check box will be checked by default, which will force an integrity check of the backup after completion. This is independent of the program default settings.

*Note: this can be turned off to reduce the overall backup time by clearing the check box. However, this is not recommended.*

Select **Run the backup now** if you wish to run the DR backup immediately on pressing the **Next>** button.

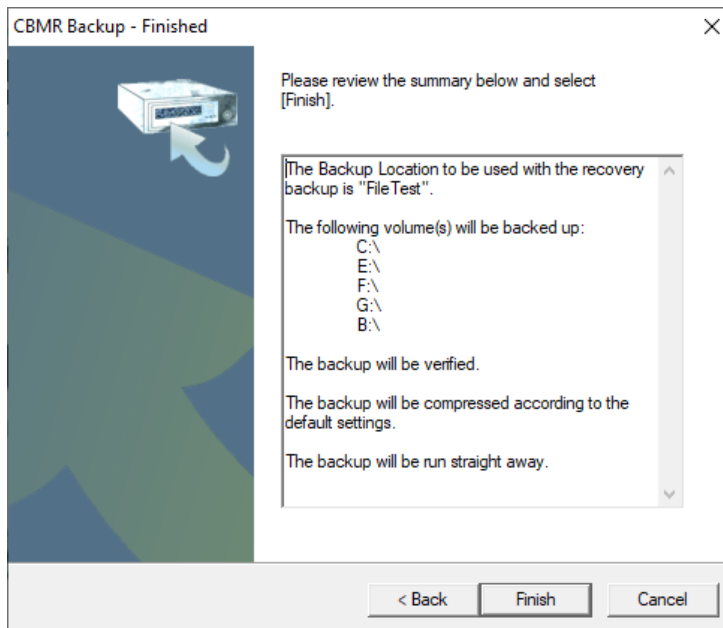
Select **Schedule it for later** if you wish to schedule it either using the CBMR or Windows Scheduler, depending on the default settings.

Select **Generate scripts only** if you wish to prepare a script (disrec.scp) for scheduling the DR backup. No actual backup will be performed in this case.

Press **Next>** to continue to the last page of the Wizard.







Select [Finish](#) to start the backup process.

*Note: it is not possible to run a DR backup until the DR configuration has been setup and saved at least once.*

## Testing the Backup Location Using WinPE5, WinPE10 or WinPE11 Mode Recovery

Insert the WinPE5, WinPE10 or WinPE11 Disaster Recovery USB flash drive or DVD/CD in your DVD/CD-ROM drive and reboot your computer from that device. Follow the on-screen instructions and boot the [Windows PE Recovery Console](#).

*Note: before storing your Disaster Recovery Disk (and the DR Backup tape if used), it is important to check that the Disaster Recovery works and the Backup Location is accessible. You only need to test that you can connect to the backup data. The description below is a summary of the process which is described in more detail in the section Restoring Your System.*

## 3.4 Restoring Your System

This section discusses the steps required to run a recover sequence using the CBMR Recovery Environment. The console is booted from the media created by CRISP in conjunction with the CRISP WinPE5, WinPE10 or WinPE11 Fileset for CBMR 9.6 (see [Create the bootable cloning environment](#) for further details).

The WinPE5, WinPE10 or WinPE11 based recovery environment is booted on the **target** system. This could be the original or a dissimilar system.

A typical CBMR recovery sequence consists of the following steps.

1. Install and run the Cristie Recovery ISO Producer (CRISP) tool on a suitable host system to create the CBMR WinPE5, WinPE10 or WinPE11 based recovery environment (USB disk or CD/DVD). This only needs to be done once.



2. Boot the CBMR WinPE5, WinPE10 or WinPE11 recovery environment on the **target** system.
3. Run a restore sequence from the recovery environment on the **target** system using the CBMR backup.
4. When the restore operation is complete and, before booting the system, you may change the hostname and IP address as required. If the target system uses different hardware from the source system inject additional drivers into the system using the hardware wizard tool. This tool will detect any new devices in the target system and prompt for the drivers.
5. Boot the recovered system.



## 4 WinPE5, WinPE10 or WinPE11 based CBMR Recovery Environment

When the **WinPE5, WinPE10 or WinPE11 CBMR Console** is booted, a Windows installation-like boot procedure is started.

During the boot process, WinPE5, WinPE10 or WinPE11 drivers for your Plug and Play devices will be loaded - in particular the **Mass Storage** devices and **Network Adapters**. When the WinPE5, WinPE10 or WinPE11 system has booted, it is possible to remove the physical USB flash drive or CD/DVD (if used) if you wish.

*Note: the DR Console will automatically reboot 72 hours after starting. This is an operating limitation of the Microsoft Windows WinPE5, WinPE10 or WinPE11 environment.*

PE10

PE10

**CBMR**

Please wait while your PnP devices are loaded ...

PE10

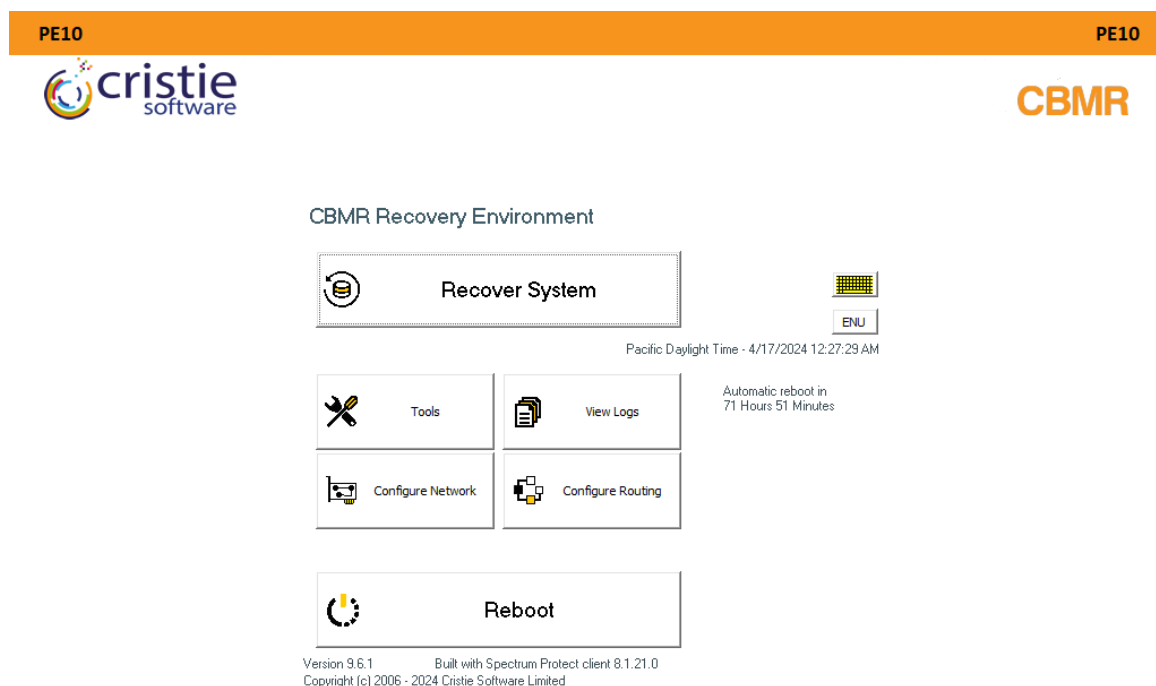
PE10

When this sequence completes, the **CBMR Recovery Environment** will be shown.



## 4.1 CBMR Recovery Environment Main Menu

When you boot the **WinPE5, WinPE10 or WinPE11** DR environment (the WinPE5, WinPE10 and WinPE11 versions are very similar), you will see the **CBMR Recovery Environment** Main Menu as below:



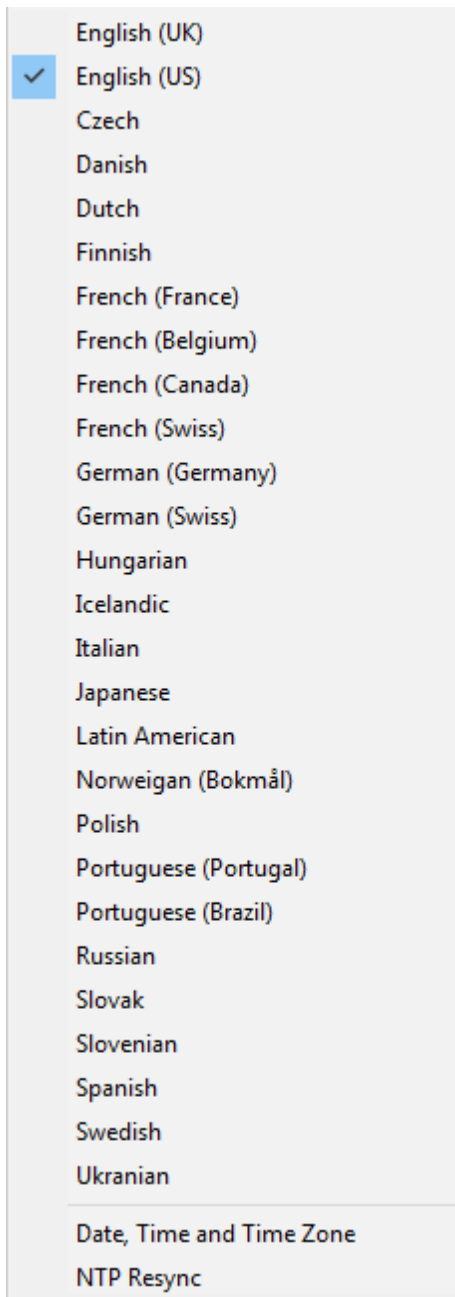
Prior to beginning the restore operation you may configure the network and/or the network routing as necessary. Click the



icons to do this.

A reboot countdown clock is shown **Automatic reboot in 68 Hours 14 Minutes**. This indicates how much time is available before the WinPE5 and WinPE10/WinPE11 recovery environment automatically reboots. Note this is a Microsoft constraint for the WinPE environment.

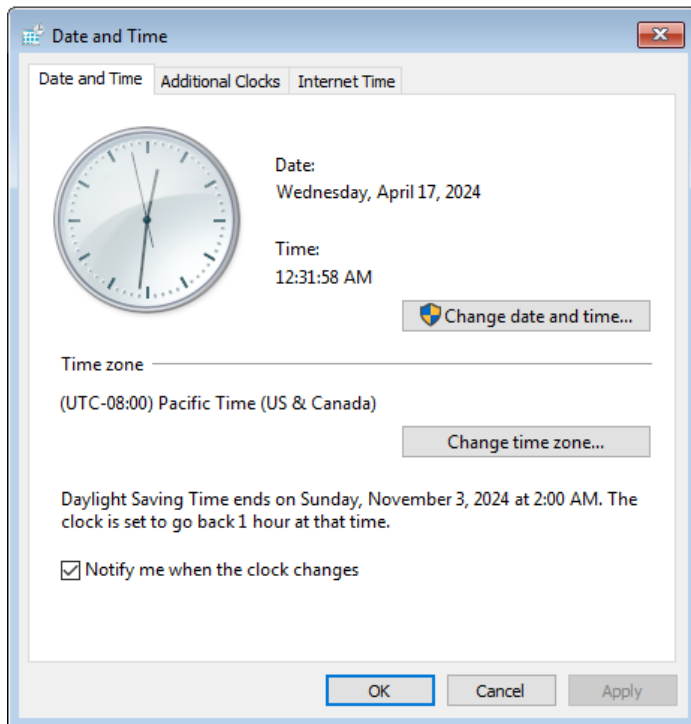
You may configure the format of the displayed date/time and the keyboard layout, by pressing the locale **ENU** icon. Note this icon will be shown according to the locale of the host system used to create the ISO/USB flash drive using the CRISP utility so it may not match the version shown here. So if, for example, the ISO/USB flash drive was built on a machine configured with a UK locale it will be displayed as **ENG**.




By default the standard display uses a keyboard layout to match the default locale as discussed above. However, this may be changed to one of the listed alternatives. Note that this does not change the display language which is always English.

Select **Date, Time** and **Time Zone** to configure the time zone for the recovery.

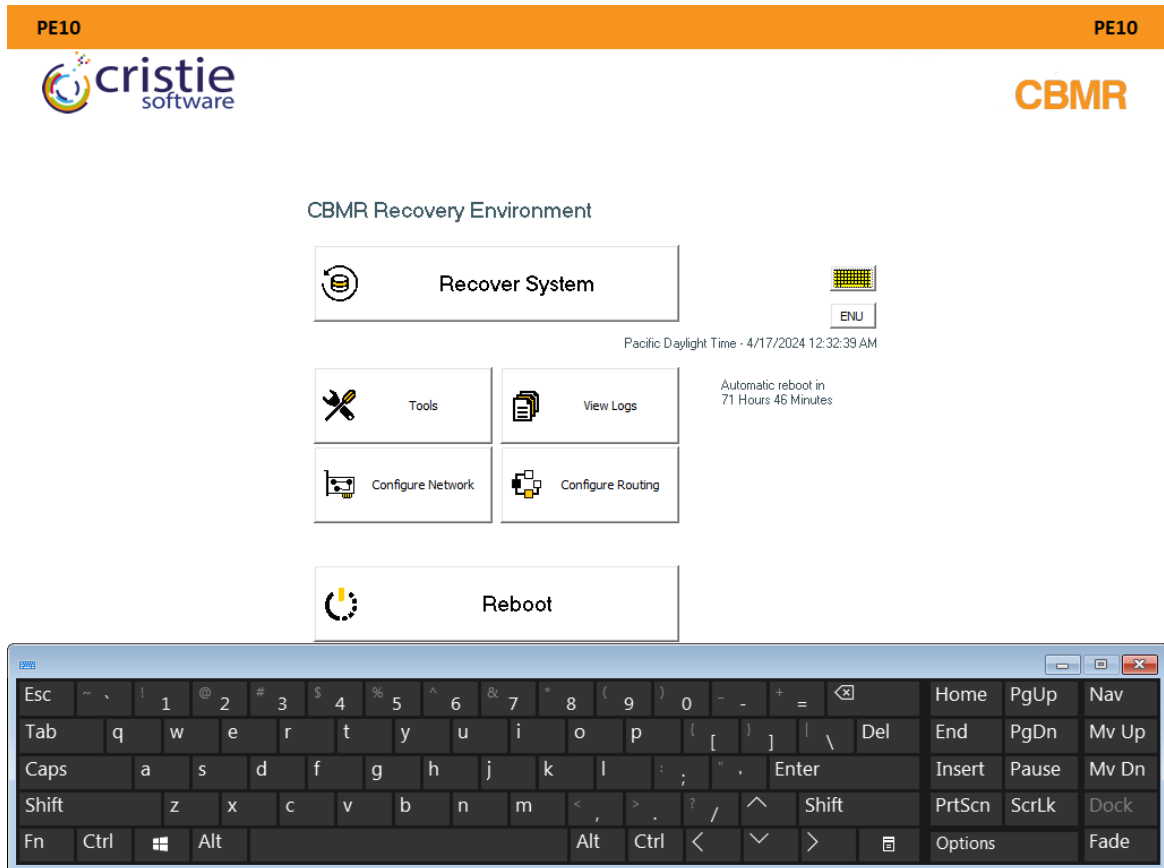




*Note: the Additional Clocks and Internet Time tabs are operational. In fact it is possible to synchronise the system time with an NTP time server if required.*

Finally if your recovery environment does not provide keyboard support (perhaps a driver issue) use the on-screen keyboard which can be displayed by clicking . This then shows a clickable keyboard at the bottom of the screen. The keyboard layout displayed will correspond to the currently selected locale.





Use this for any data entry.

*Note the DR environment requires a working mouse as a minimum.*

## 4.2 Begin the Restore Process

Click the **Recover System** option to begin the recovery sequence.

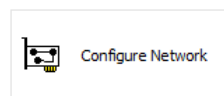
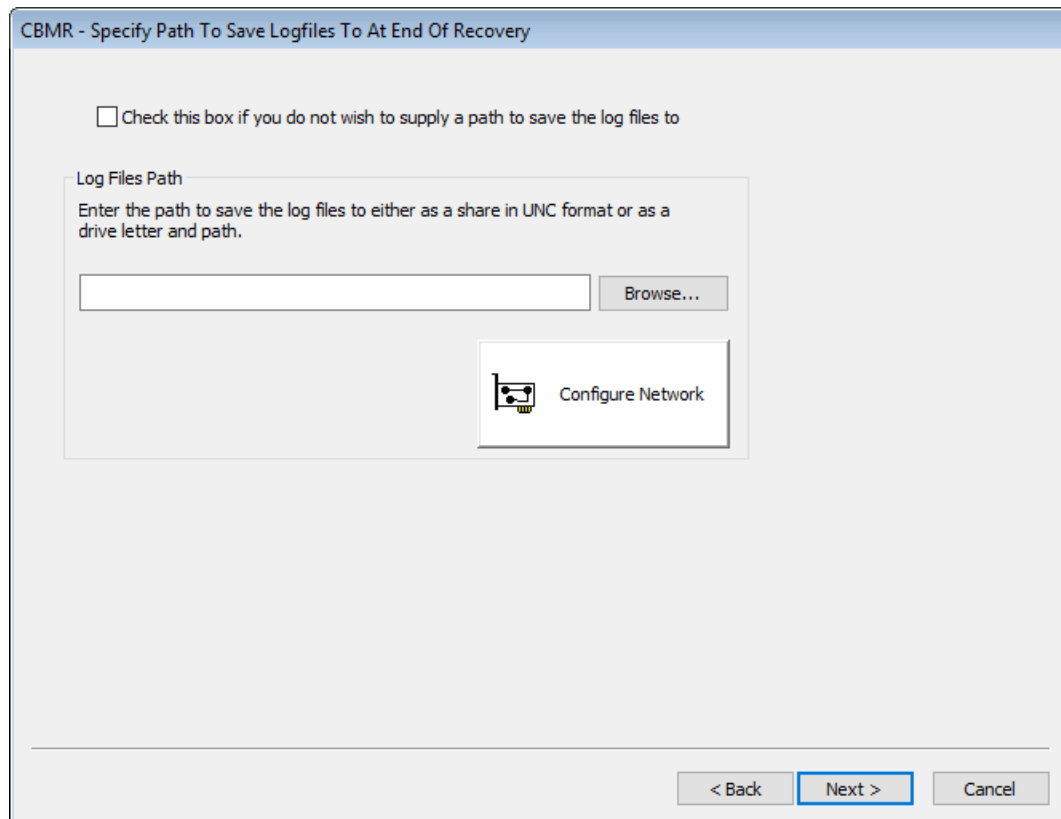


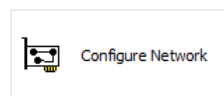
Press **Next>** to proceed to the first step of the sequence. Press **Cancel** to abort the recovery sequence at this point.

### 4.2.1 Logfile Save Path

Before starting the restore process you should configure a location to save the recovery logs. This can be a network location or physical media (such as a USB flash drive). The logs will be automatically saved to the configured location at the end of the restore process without further intervention.





For example, use the  option to first map a network share location and then **Browse** to select a folder on the share.



If you do NOT want to automatically save the the logfiles please check the tick-box to skip this step.

☒ Check this box if you do not wish to supply a path to save the log files to

Click **Next >** to continue to the next step.

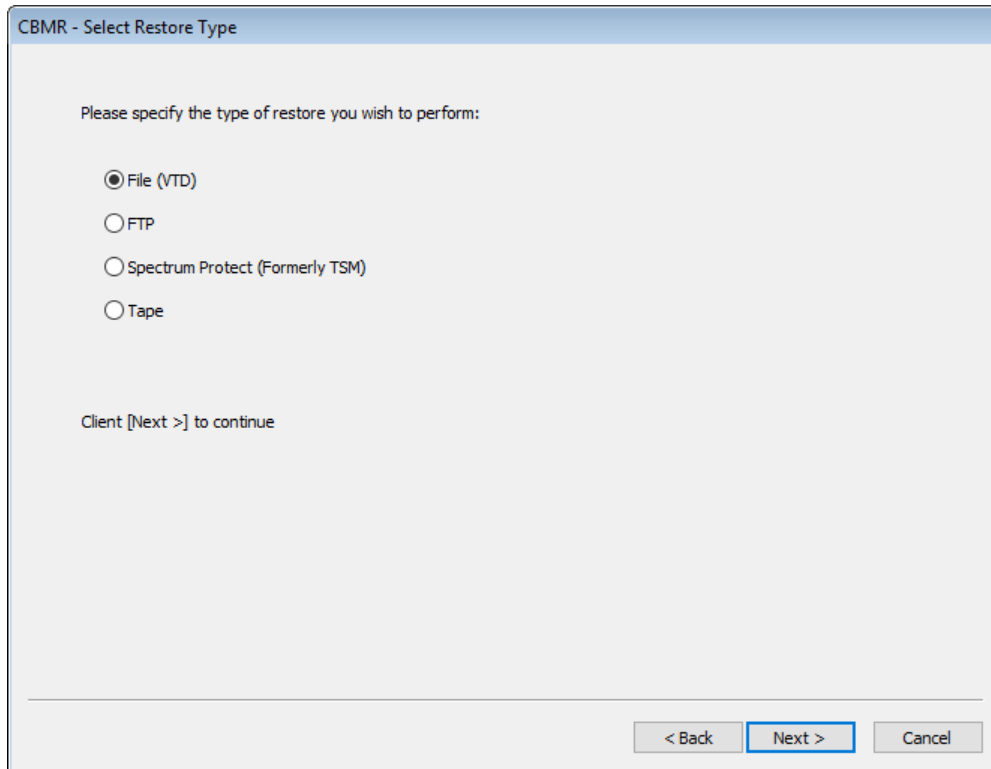
*You will still have the opportunity at the end of the restore process to save the logfiles if you wish.*





## 4.2.2 Select Restore Type

The following dialogue then prompts you to identify the restore **Type**.



Press **Next>** to proceed to the first step of the sequence. Press **Cancel** to abort the recovery sequence at this point.

## 4.2.3 File Restore Type


If you selected a **File** restore type, then the following dialogue appears. In the example below the **Network Setup** functionality has been used to map drive V: to the location of the backup file in Virtual Tape Drive (VTD) format.



CBMR - File Backup Location

File Path:  
Enter the location of the VTD either as a share in UNC format or as a drive letter and path.

V:\nigelp\cbmr-backups\Windows\NP-Win2022.VTD [Browse...](#)

 [Configure Network](#)

☐ Point-in-time (PIT) restore

Wednesday, April 17, 2024 12:34:26 AM

< Back Next > Cancel

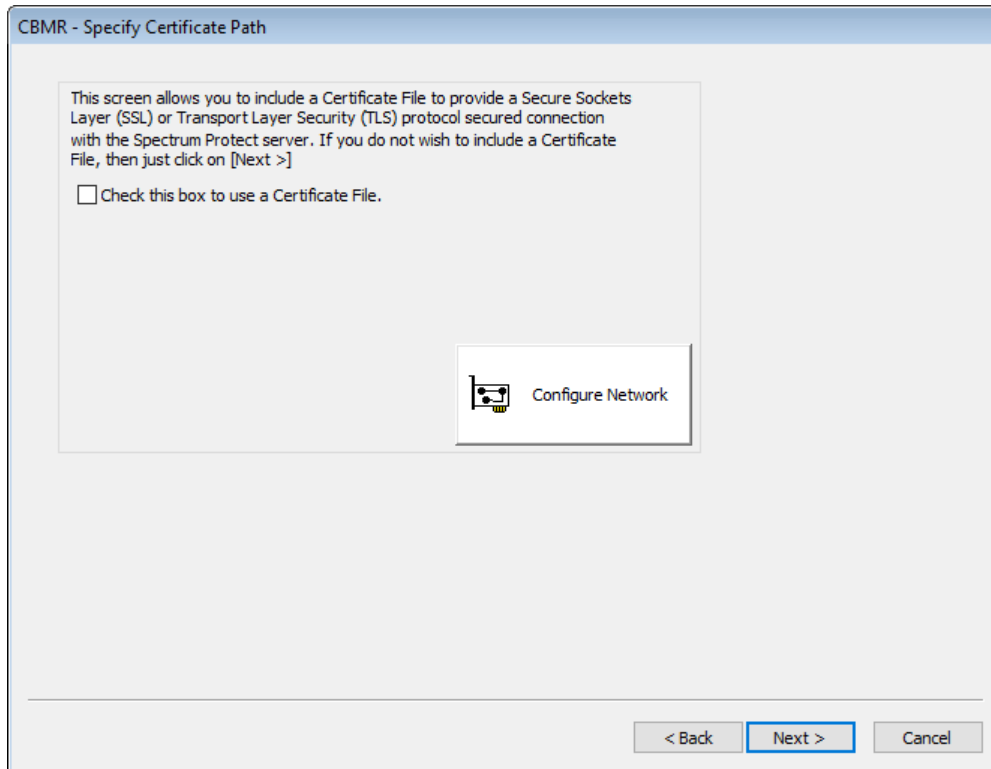
*Note Point-in-time (PIT) restore mode is not supported for File type DR restores.*

Click [Next>](#) to continue.



#### 4.2.4 IBM Spectrum Protect Restore Type

If you selected a Restore Type of **IBM Spectrum Protect**, the following dialogue appears.



If the IBM Spectrum Protect server hosting your backup uses an SSL/TLS certificate (such as version 8.1.2 or later), you may then select a certificate to use from the next dialogue page:



The screenshot shows a Windows-style dialog box titled "CBMR - Specify Certificate Path". Inside, there is a text box with the following instructions: "This screen allows you to include a certificate file or zip file of the client key database to provide a Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol secured connection with the Spectrum Protect server. If you do not wish to include a certificate file or zip file of the client key database, then just click on [Next >]". Below this is a checked checkbox with the label "Check this box to use a certificate file or a zip file of the client key database." Underneath the checkbox, it says "Enter the certificate file or zip file name either as a share in UNC format or as a drive letter and path." There is a text input field containing the path "V:\nigelp\TSM-Certificates\8.1.11\cert256.arm" and a "Browse..." button to its right. Below the input field is a button labeled "Configure Network" with a small icon of a computer and a network cable. At the bottom of the dialog box are three buttons: "< Back", "Next >", and "Cancel".

Click **Check this box to use a Certificate file** and then either enter the certificate file path direct or use [Browse](#) to navigate to a network share containing the certificate. Before using browse, first use [Network Setup](#) to assign a network drive (if required).

*Note: If you specify a certificate it must be accessible during the recovery sequence using the path specified.*

Click [Next >](#) to continue. Provide the details for the **IBM Spectrum Protect server** and **Node** used to contain the backup:

CBMR - Specify Spectrum Protect Location

Spectrum Protect Server Details

Server Address: 10.10.2.84

Port: 1501

Spectrum Protect Client Details

Node Name: NP-WIN2022

Node Password: ••••••••

Filespace Name: CBMR

☐ Point-in-time (PIT) restore

Tuesday , April 12, 2022 3:58:53 AM

< Back Next > Cancel

Selecting the **Point-in-time (PIT)** restore mode will allow the system to be recovered from the most recent backup before the specified date and time. This means the version of any file restored will be earlier than the specified date and time. Selecting the down-arrow in the calendar control will bring up a calendar:



CBMR - Specify Spectrum Protect Location

Spectrum Protect Server Details

Server Address: 10.10.2.84

Port: 1501

Spectrum Protect Client Details

Node Name: NP-WIN2022

Node Password: ••••••••

Filespace Name: CBMR

☒ Point-in-time (PIT) restore

Tuesday , April 12, 2022 3:58:53 AM

Sun	Mon	Tue	Wed	Thu	Fri	Sat
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	7

☐ Today: 4/12/2022

< Back Next > Cancel

This can be used to scroll the months/years backwards and forwards as necessary.

**Note: a future date will result in the latest backup being recovered.**

If PIT mode is not selected then, by default, the latest filespace versions will be restored.

Select **Next>** to continue.

At this point the client backup on the specified server will be accessed and the machine configuration extracted.



### 4.2.5 FTP Restore Type

If you selected a Restore Type of **FTP**, the following dialogue appears. Provide the details for the FTP server and folder used to contain the backup:

CBMR - FTP Backup Location

FTP Server Details

Server Address: 10.10.11.98

Port: 21

Target folder on FTP server:

NP-Win2022

Username: nigelp

Password: ••••••••

☐ Point-in-time (PIT) restore

Tuesday , April 12, 2022 4:01:27 AM

< Back Next > Cancel

Selecting the **Point-in-time (PIT)** restore mode will allow the system to be recovered from the most recent backup before the specified date and time. This means the version of any file restored will be earlier than the specified date and time. Selecting the down-arrow in the calendar control will bring up a calendar:



CBMR - FTP Backup Location

FTP Server Details

Server Address: 10.10.11.98

Port: 21

Target folder on FTP server:

NP-Win2022

Username: nigelp

Password: ••••••••

☒ Point-in-time (PIT) restore

Tuesday, April 12, 2022 4:01:27 AM

Sun	Mon	Tue	Wed	Thu	Fri	Sat
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	7

Today: 4/12/2022

< Back Next > Cancel

This can be used to scroll the months/years backwards and forwards as necessary.

**Note:** a future date will result in the latest backup being recovered.

If PIT mode is not selected then, by default, the latest backup will be restored.

Select **Next>** to continue. At this point the FTP backup on the specified server will be accessed and the machine configuration extracted.

#### 4.2.6 Specify Key Repository

Select **Next>** to specify a **Key Repository path**, **Passphrase** or **Clear Key**. These parameters are used if the backup is encrypted. If a key or passphrase is not used you may skip this step.



The screenshot shows the 'CBMR - Specify Key Repository' dialog box. It has a title bar with the text 'CBMR - Specify Key Repository'. Inside, there's a section titled 'Key Repository' with the instruction: 'Enter the encryption key repository filename either as a share in UNC format or as a drive letter and path.' Below this is a text input field containing 'T:\nigelp\CBMR\Win2019\KeyRepository.ini' and a 'Browse...' button. To the right of the input field is a 'Configure Network' button with a network icon. Below this is a section titled 'Passphrase or Clear Key' with the instruction: 'Or, you can provide encryption passphrase or Clear Key here:' and an 'Enter' button. At the bottom, there's a warning: 'Warning: If you don't specify the key repository file, passphrase or clear key and the backup is encrypted, you will be asked to enter the encryption passphrase during the recovery.' At the very bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

If the backup was encrypted and no Key Repository file has been entered, then a prompt will appear for the encryption key or passphrase to be manually specified. For example:

The screenshot shows the 'CBMR - Specify Key Repository' dialog box with an 'Enter Encryption Key' sub-dialog box open. The main dialog box has a title bar with the text 'CBMR - Specify Key Repository'. Inside, there's a text area with the message: 'Successfully connected to local CBMR recovery client. The backup is encrypted. A Passphrase or Clear Key must be provided'. The 'Enter Encryption Key' sub-dialog box is in the foreground. It has a title bar with the text 'Enter Encryption Key' and a close button. Inside, there's a section titled 'Please Enter Encryption Passphrase or Clear Key:' with a lock icon. Below this is a checkbox labeled 'Use Clear Key'. Below the checkbox is a checkbox labeled 'Show Clear Text'. Below 'Show Clear Text' is a text input field labeled 'Passphrase:'. Below the 'Passphrase' field is a section labeled 'Clear Key:' with a series of seven input fields separated by dashes. At the bottom of the sub-dialog box are two buttons: 'OK' and 'Cancel'. The main dialog box has an 'OK' button at the bottom center and '< Back', 'Next >', and 'Cancel' buttons at the bottom right.



*It is not possible to recover the configuration files from an encrypted backup without the key or passphrase.*

Select [Next>](#) to continue to **Confirm Volume Layout**.

## 4.2.7 Storage Pools

If your original source host contained any Windows Storage Pools then this step will be run to allow the pool/disk setup to be configured. If no Storage Pools were configured in your selected backup this step will be skipped.

*Note: Storage Pool recovery only works with the WinPE5 version of the CBMR DR environment. Do not use the WinPE10 version for Storage Pool recovery.*

The pool/disk configuration dialogue looks like this:

**CBMR - Storage Pools**

Stored Storage Pools (2)

Name	Capacity	Free Space
Pool-A	8.97 GB	6.72 GB
Pool-B	18.97 GB	14.97 GB

To configure, select a Virtual Disk from the table below and right-click to assign target Physical Disks to it.

Stored Virtual Disks (1)

Name	Layout	Provisioning	Capacity	Allocated	Volume
Pool-A-Disk0	Simple	Thin	5.00 GB	768.00 MB	E:

Stored Physical Disks (1)

Name	Capacity	Bus	Usage	Chassis	Media Type
VMware Virtual SATA Hard...	5.00 GB	SATA	Automatic	sata0	SSD

Proposed Physical Disks (0)

< Back   **Next >**   Cancel

The pool configuration requires you to map the original pool/virtual disk configuration to the physical disk layout detected on the target. This may have more or fewer disks than the original so this re-mapping needs to be done manually.

There are 3 sections in the dialogue:

- **a list of the original configured pools with their corresponding capacity and the free space at the time of the backup.**

- **a list of the original virtual disks defined for a selected pool together with the corresponding virtual disk layout, provisioning, capacity, size in use and volume letter.**
- **a list of the original physical disks and the proposed physical disks discovered on the target system for the selected virtual disk.**

To assign physical disks to a virtual disk right-click the virtual disk to display the Virtual Disk Layout dialogue.

This is a recovery of a Windows 2019 server with 2 Storage Pools, named Pool-A and Pool-B. Pool-A is currently selected which is showing the Virtual Disk that was in the Storage Pool on the source system. The screenshot below shows the Physical Disks that the Virtual Disk was built from on the source system. There were 2 of them and they were all SATA (shown as Bus Type SATA).

Note that the **Proposed Physical Disks** has a count of zero, i.e. there are no target Physical Disks selected yet to recreate this Virtual Disk from, where **Stored** = **Source system** and **Proposed** = **Target system**.

Right-click on the virtual disk, to display the disk selection dialogue.

**CBMR - Virtual Disk Layout**

Storage Pool Virtual Disk

Name	Pool-A-Disk0
Layout	Simple
Provisioning	Thin
Capacity	5.00 GB
Allocated	768.00 MB
Volume	E:

Stored Physical Disks (1)

Name	Capacity	Bus	Usage	Chassis	Media Type
VMware Virtual SATA Hard...	5.00 GB	SATA	Automatic	sata0	SSD

Proposed Physical Disks (2)

Name	Capacity	Bus	Usage	Chassis	Media Type
<input type="checkbox"/> PhysicalDisk1	10.00 GB	SAS	Automatic		SSD
<input type="checkbox"/> PhysicalDisk2	10.00 GB	SAS	Automatic		SSD
<input checked="" type="checkbox"/> PhysicalDisk3	5.00 GB	SATA	Automatic		SSD
<input checked="" type="checkbox"/> PhysicalDisk4	5.00 GB	SATA	Automatic		SSD

OK Cancel

In the example above the 2 target physical disks that makeup the original virtual disk are selected. Note the proposed disk count is now non-zero.



Repeat this process for all the remaining virtual disks in each pool. This results in a configuration similar to this:

CBMR - Storage Pools

Stored Storage Pools (2)

Name	Capacity	Free Space
Pool-A	8.97 GB	6.72 GB
Pool-B	18.97 GB	14.97 GB

To configure, select a Virtual Disk from the table below and right-click to assign target Physical Disks to it.

Stored Virtual Disks (2)

Name	Layout	Provisioning	Capacity	Allocated	Volume
Pool-B-Disk0	Simple	Thin	5.00 GB	768.00 MB	F:
Pool-B-Disk1	Simple	Thin	5.00 GB	768.00 MB	G:

Stored Physical Disks (1)

Name	Capacity	Bus	Usage	Chassis	Media Type
VMware, VMware Virtual S	10.00 GB	SAS	Automatic	SCSI0	SSD

Proposed Physical Disks (2)

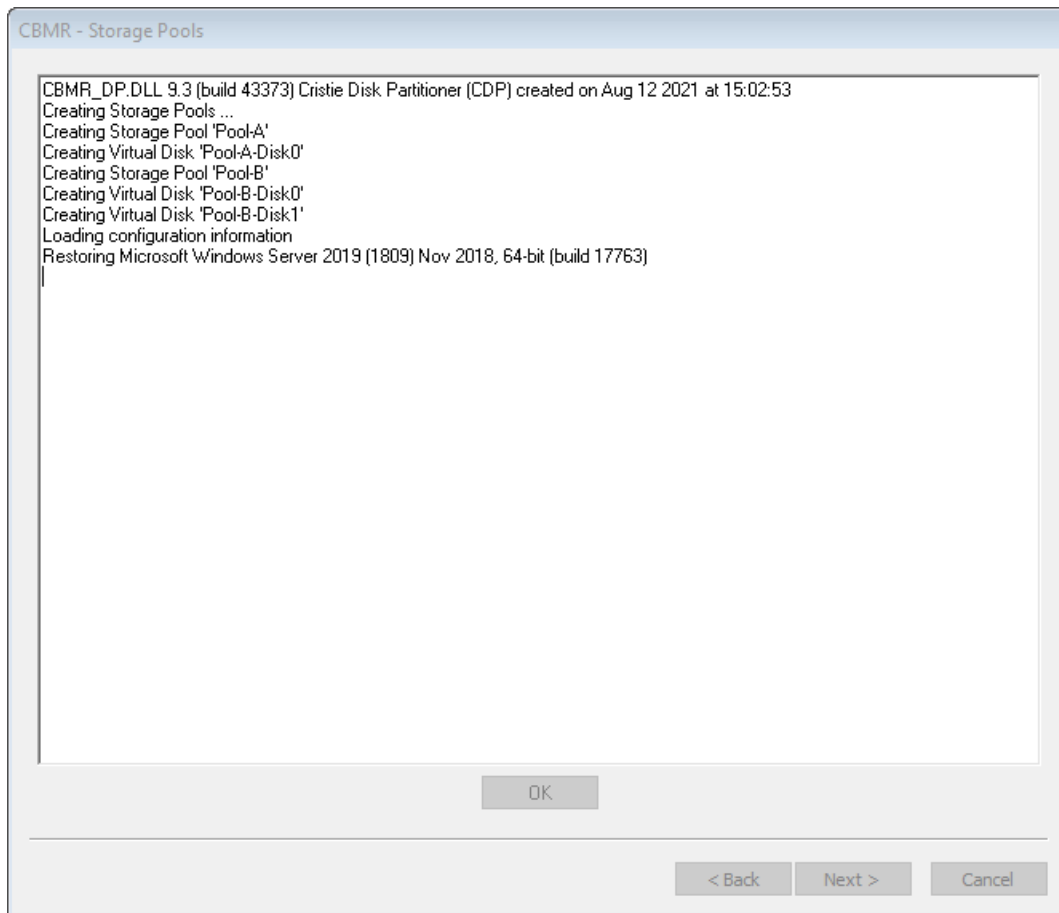
< Back   Next >   Cancel

*Note: There are some constraints on this configuration. For example, it is not recommended to have fewer or more physical disks mapped to your target virtual disk compared with the original source configuration.*

Now click **Next >** to continue or **< Back** to return to the previous dialogue.

At this point the Storage Pools and virtual disks will be created.





**Note:** if no target disks are assigned during the Storage Pool step then recovery will still proceed but no Storage Pools will be restored.

Recovery now runs as normal with no further Storage Pool configuration required.

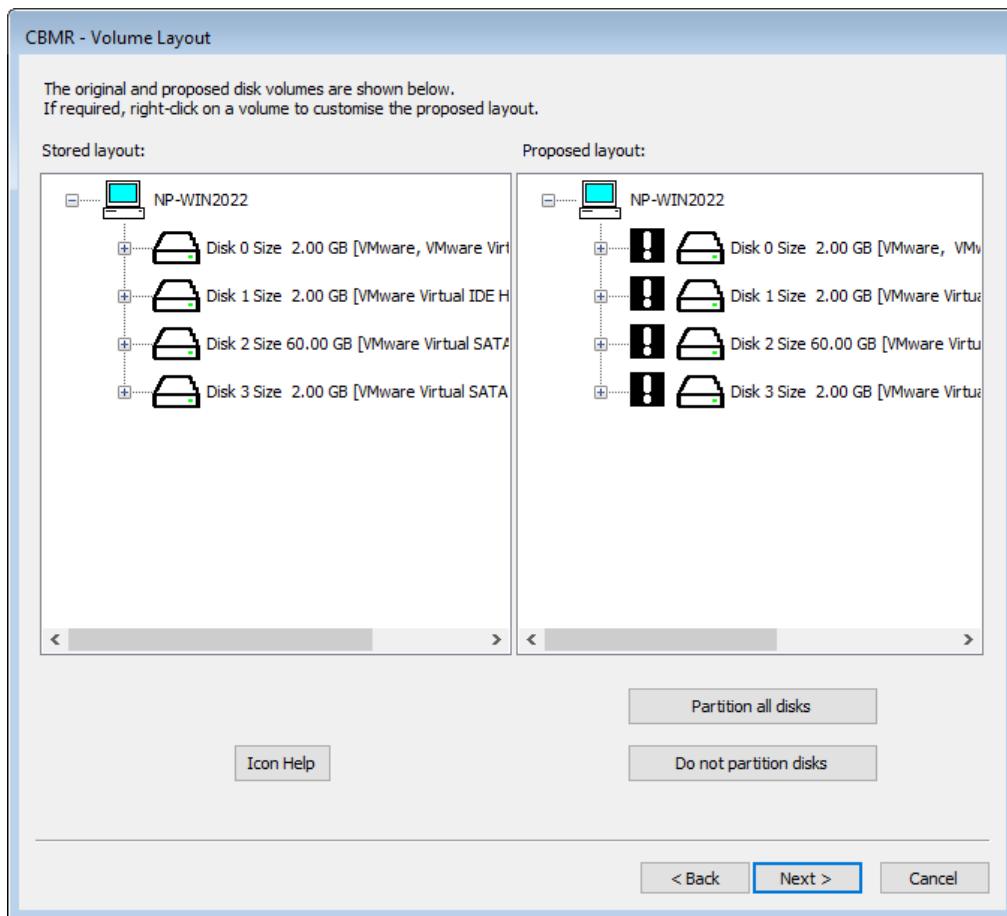
There are certain constraints with this release of Storage Pool support.

- *Storage Pools and virtual disks are recognized by CBMR WinPE5, so if you boot a target system that has them, then WinPE5 will see them and mask out the "real" disks resulting in only the virtual disks being shown.*
- *The use of NVMe type disks when using VMWare WorkStation is not recommended when using Storage Pools.*
- *Physical disks used in Storage Pools should have minimum size of at least 8 GB.*
- *Only the CBMR WinPE5 DR environment is supported for recoveries of Storage Pools.*
- *During the Volume Layout phase you can right-click on target disks and swap them etc, but you can't swap a Storage Pool virtual disk with a real disk or vice-versa.*

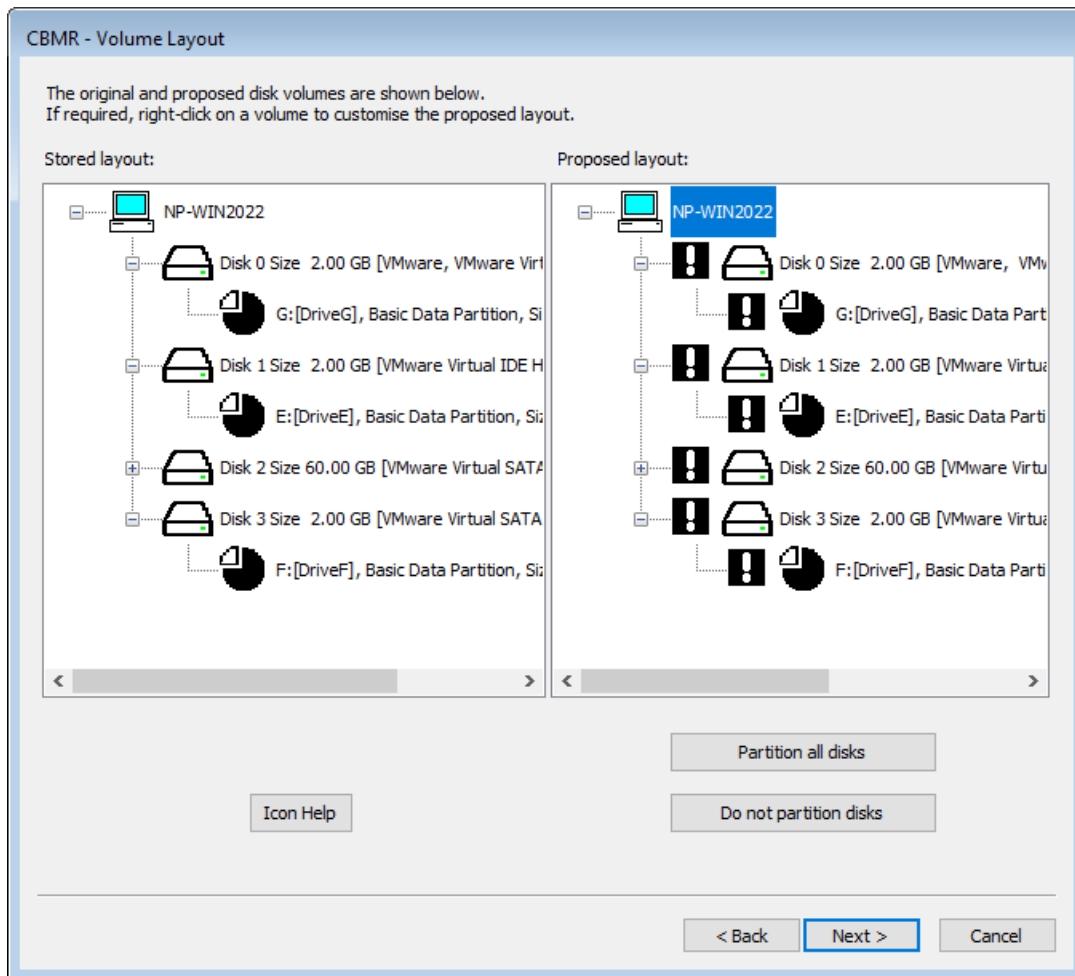


### 4.2.8 Confirm Volume Layout

The next step in the **Automatic recovery** shows a list of the disks and partitions to be recovered.



For a system with Storage Pools the Volume Layout will resemble this example:



The left-hand panel of the dialogue shows the original disk layout and partitions. The right-hand panel shows how the recovered disks will be partitioned after the recovery.

If you wish to quickly enable the partitioning of all target disks click .

If you wish to quickly disable the partitioning of all target disks click .

A white tick box ☒ next to a disk signifies that the disk and its underlying partitions will be left intact. Placed next to a partition/volume means that the corresponding partition/volume **WILL NOT** be partitioned.

A white exclamation mark ☐ placed next to a disk means it **WILL** be partitioned during recovery. Placed next to a partition or volume means that the corresponding partition/volume **WILL** be partitioned.

A black/white exclamation mark ☐ placed next to a disk means at least one partition/volume **WILL** be partitioned.

A white box ☐ indicates that the disk will be completely ignored during the recovery.

There are 3 disk types available:





indicates a standard disk

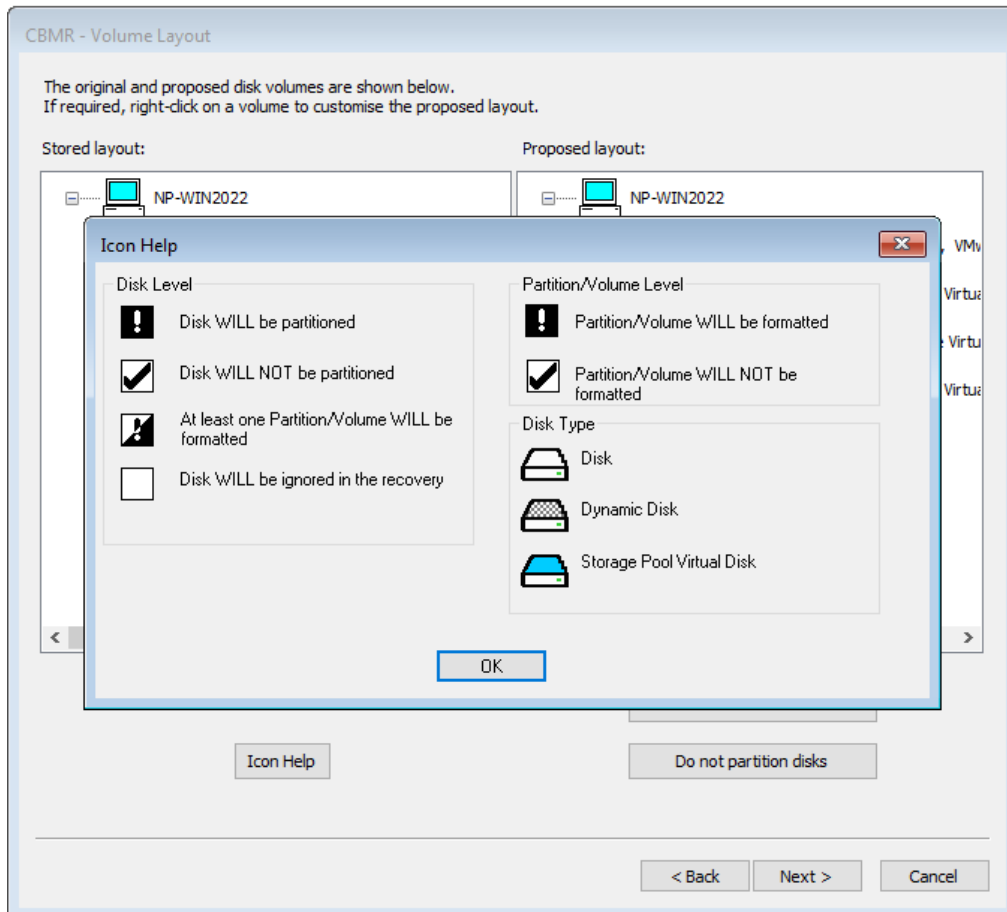


indicates a dynamic disk



indicates a Storage Pool virtual disk

Click on the [Icon Help](#) button to display a summary of this:



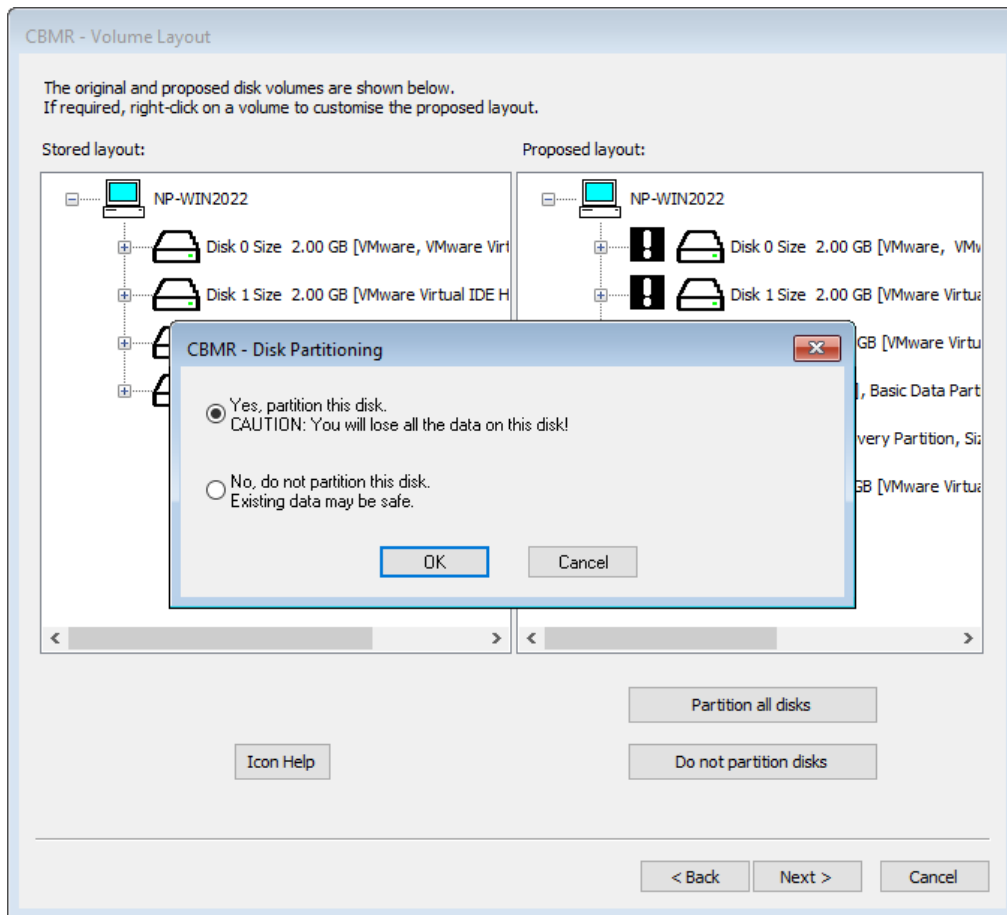
When the recovery is to the original system, the contents of both panels will look similar if the number of disks is the same. Possibly the disk sizes will be different.

When performing a recovery to a dissimilar system, the disk mapping can be much more complex. Some of the criteria used to judge the disk mapping are:

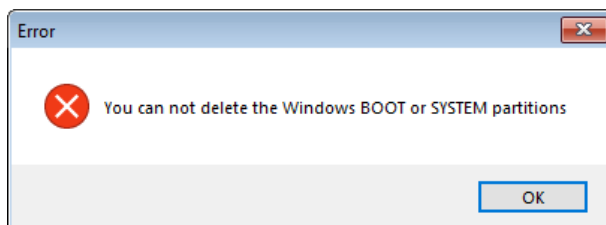
- *disk geometry*
- *disk capacity*
- *if currently formatted, the disk signature*

You may right-click on any disk shown in the right-hand panel to select whether the disk will be partitioned or not.



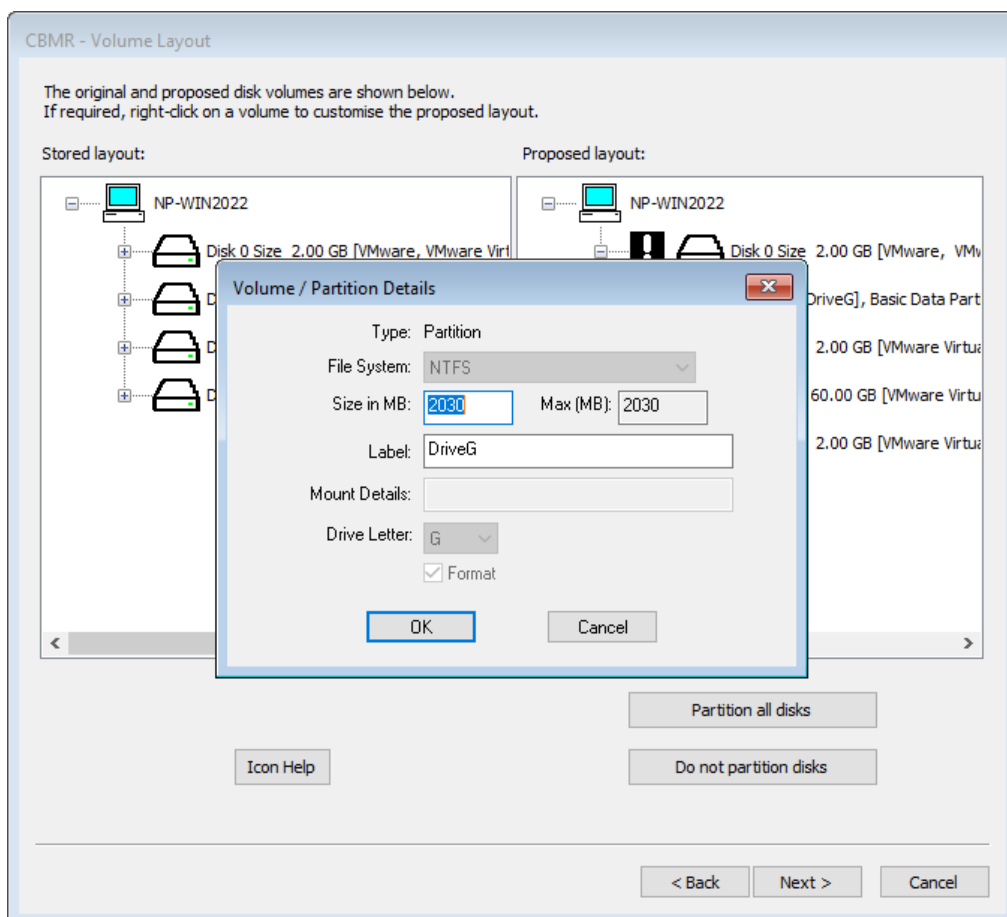


Any attempt to incorrectly turn off formatting will result in this error:




You may also right-click on a partition to allow you to selectively modify the partition parameters.

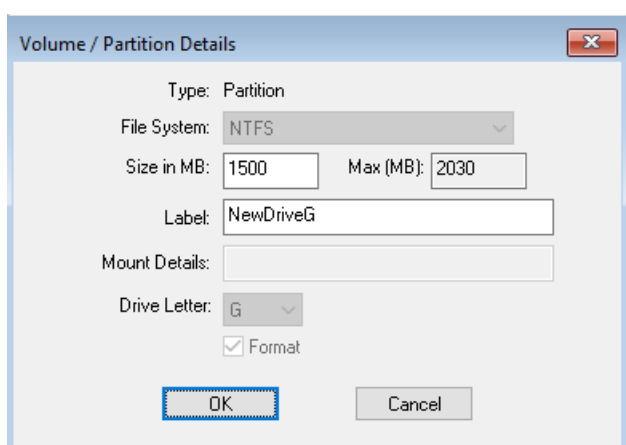




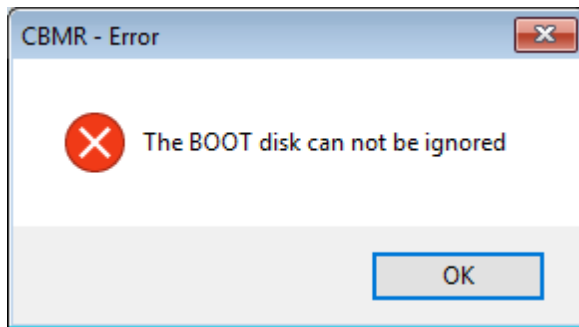
You may **Modify** the following partition parameters:

- size in MB (only if disk is shown with a )
- label
- format (yes/no)

The screenshot below shows an example:



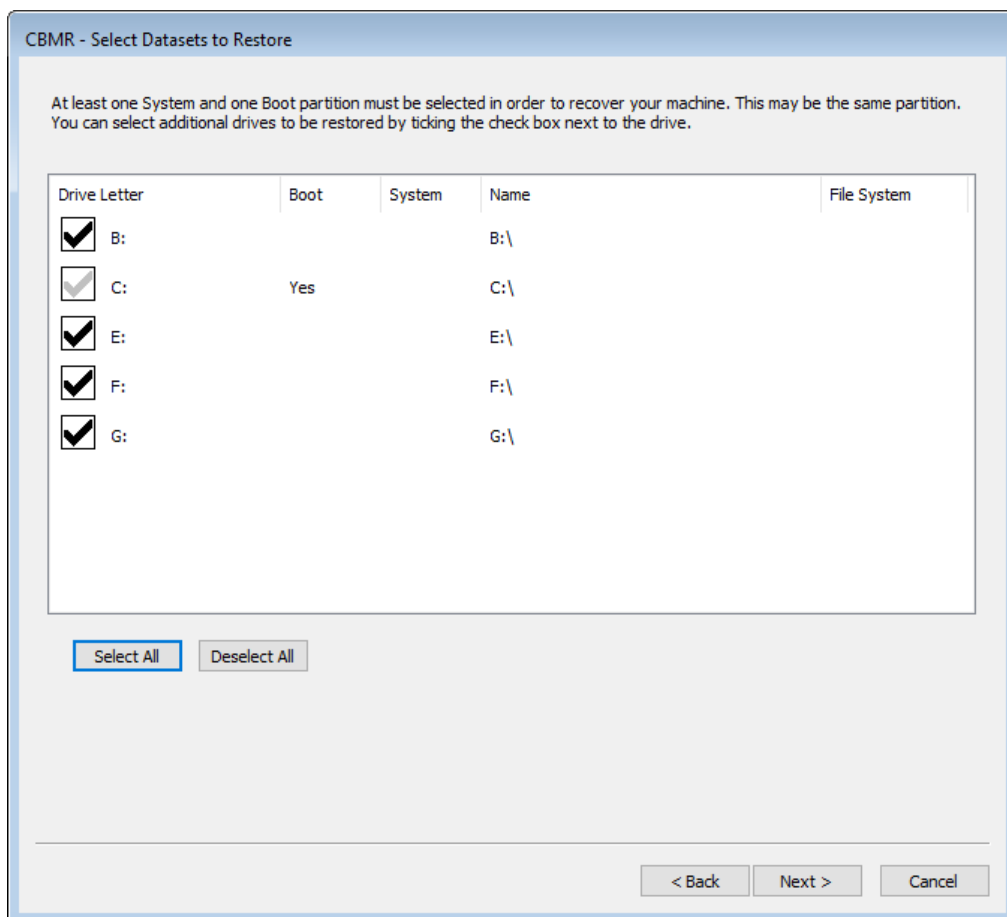
If you attempt to either not format or delete a Windows system partition, an error such as this will be displayed:



At this stage, nothing has happened to the disks. Press [Next>](#) to continue with the recovery.

#### 4.2.9 Select Datasets to Restore

The next step prompts for the datasets to restore. Generally, each dataset represents a disk partition or volume. Put a tick against each dataset that should be restored:



Click [Next>](#) to continue to the **Clone Settings** dialogue.



### 4.2.10 Clone Settings

Use this dialogue to change the recovered system's **hostname** and **IP addresses** if required. Select to use either DHCP or enter a valid static IP address.

You may change the IP address for each NIC interface independently. NICs that are currently connected to a network are tagged with **(Operational)**.

**Note:** The **Use DHCP** tick-box shown on the left side of the dialogue indicates whether DHCP was used on the source system. If its ticked it indicates DHCP was used on the source. If unticked a static IP address was used.

If you wish to retain the current hostname and IP addresses leave the fields at their default values and select **Next >** to continue to the next section.

**Note:** When you click on the "Next >" the button will change to "Finish", when you click on "Finish" the restore will start. If dissimilar hardware is detected, then when you click on "Next >" the Dissimilar Hardware dialogue will be displayed instead. Click "Finish" on that dialogue to start the restore.

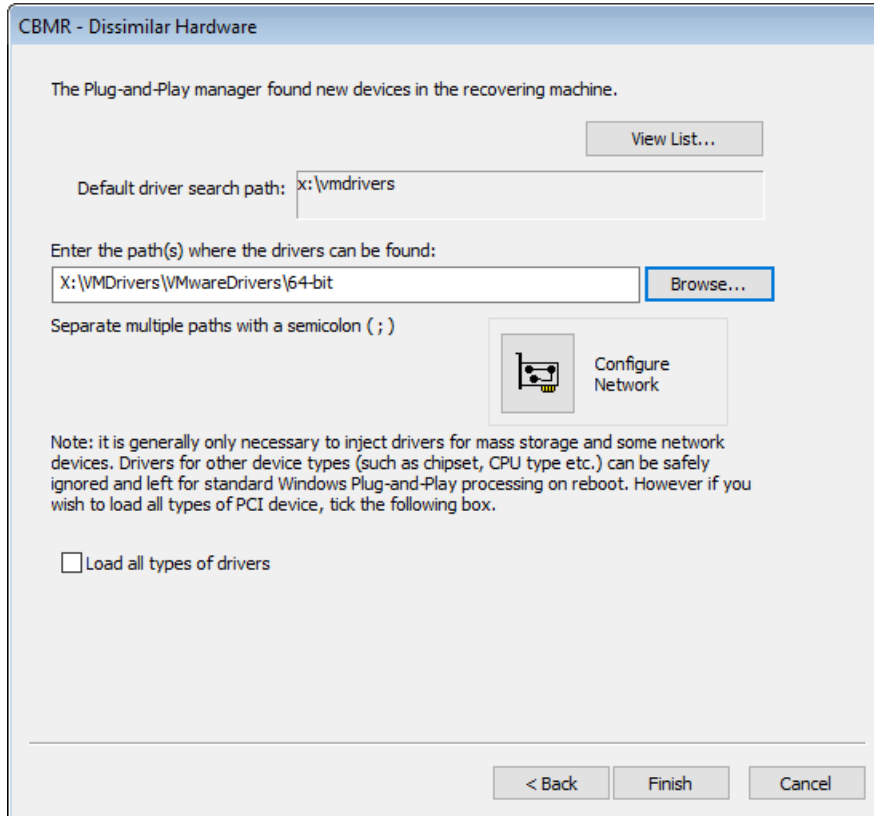
When recovering to a system with a different MAC address (generally during a dissimilar DR), the default IP address settings default to DHCP and not the original IP.

The **Next >** button will change to **Finish**. Click this when ready to continue.

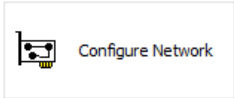


### 4.2.11 Dissimilar Hardware

Next, the DR process performs a check to determine if there are new devices in the recovering machine that were not present in the original system. If this is true, then this is a 'dissimilar' DR and the following dialogue will be shown to allow the user to specify the location of the new driver files for these devices.

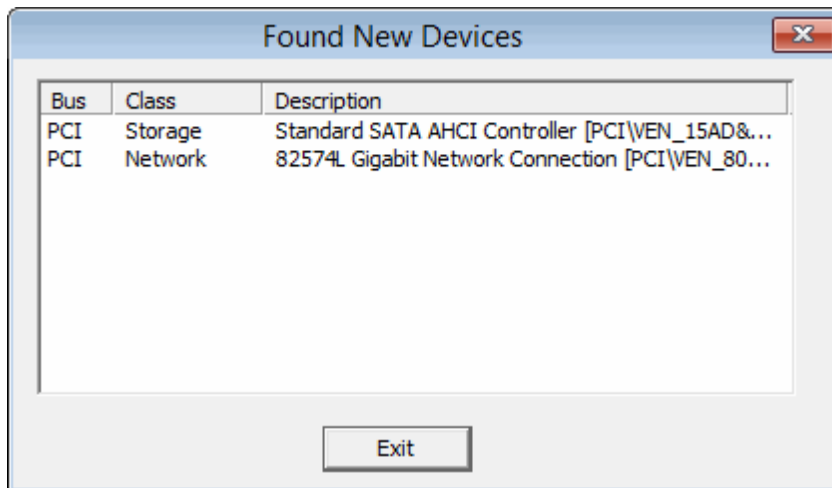


Specify the default path or paths to be searched for the missing driver files. The paths may

be on a local device (eg. a USB disk) or a network share. Use the  button if you need to map a network share. In either case, the paths must be accessible to the WinPE5, WinPE10 or WinPE11 environment.

Select [View List...](#) to see a list of the new devices.





Ensure the specified path or paths contain the correct 64-bit drivers for the dissimilar machine. At the end of the DR sequence, the specified paths will be searched for the missing drivers and automatically injected into the recovered system.

By default, it is only necessary to inject drivers for mass storage devices and, in some some cases, network devices. The 'Load all types of drivers' tick box will force the DR to look for all drivers in addition to mass storage and network devices. For example, this could include graphics cards, USB and chipset devices, but these are rarely required and not recommended.

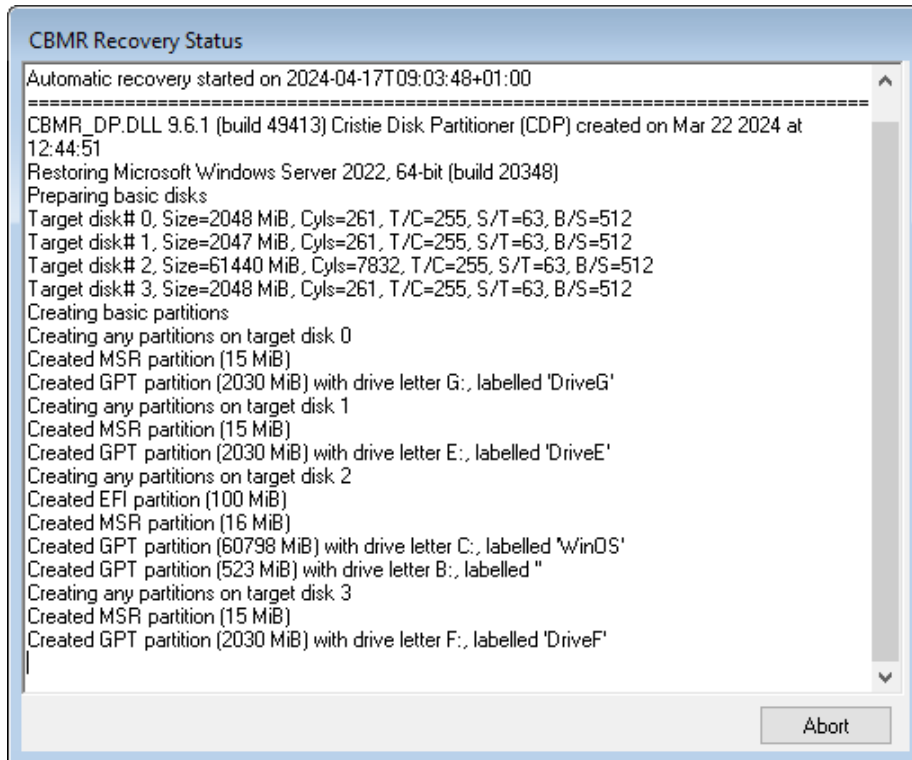
Note that if drivers are not found for the new boot disk then, although WinPE5, WinPE10 or WinPE11 will be able to recover the files to the disk, there is a good chance that it will not boot correctly.

Press **Finish>** to proceed with the recovery.



#### 4.2.12 Disk Recovery Sequence

The sequence begins by preparing the disks selected for formatting.



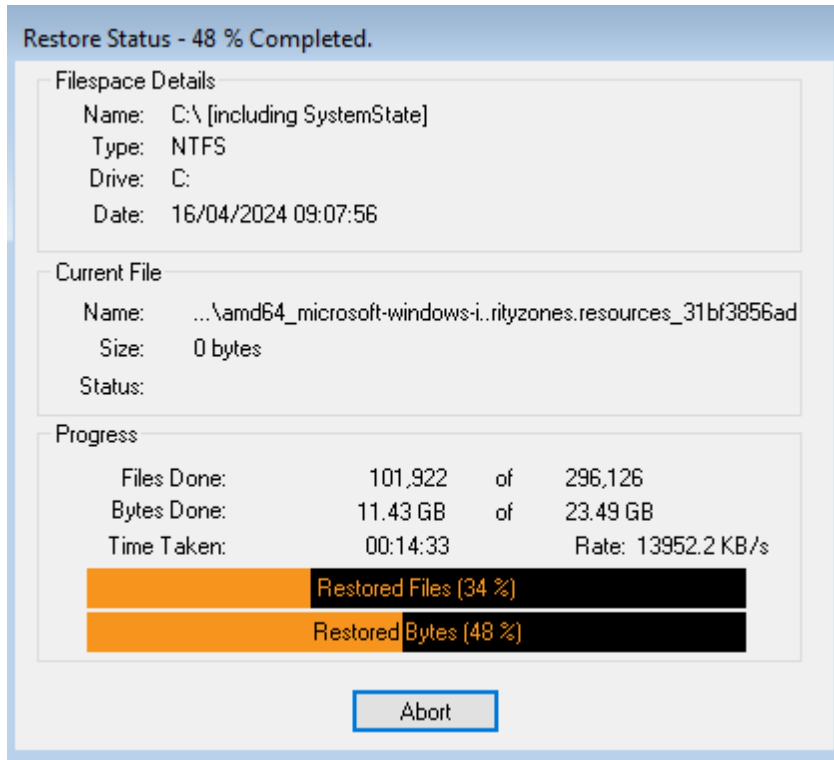
This step involves:

- disk mapping original layout to new
- cleaning (removing any existing disk partitions)
- removing any existing dynamic volume databases
- re-creating the partitions on selected disks
- converting to dynamic volumes if required
- formatting to the required partition type
- creating partition/volume mount points
- making bootable volumes active

The next step is to recover the datasets to the selected target disks/partitions. A new window appears containing the restore status of recovered files, with progress bars indicating how much of the backup has been restored. This display also shows the recovery statistics in terms of time, size and throughput.

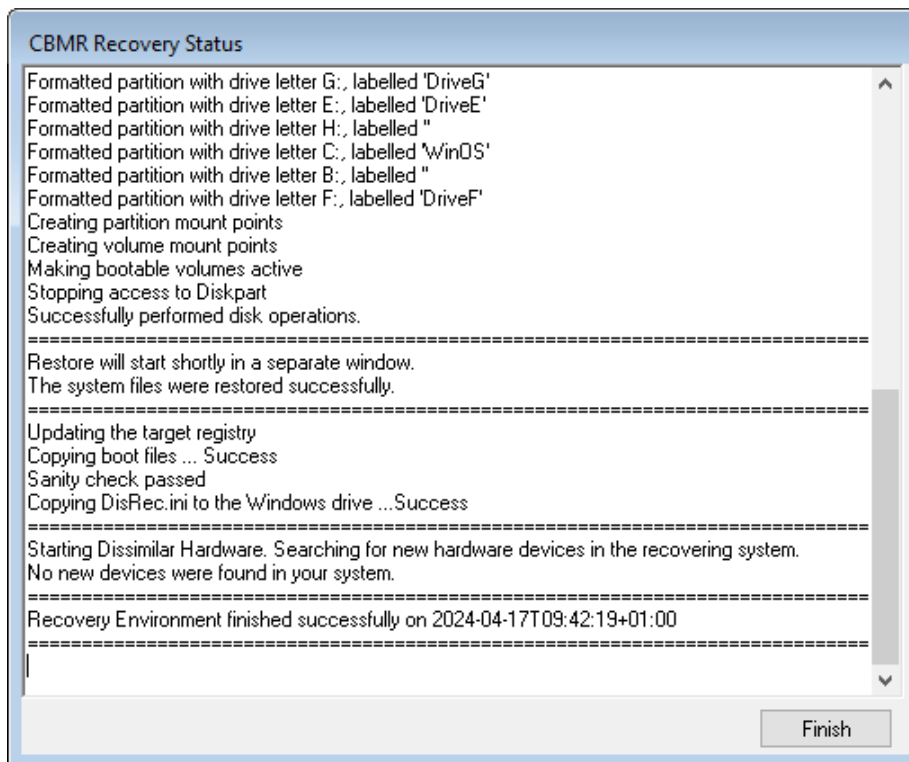
The recovery is divided into different phases: first the recovery of each selected filespace (including **SystemState**),





This process may take some time if the backups are large. You may select the [Abort](#) button to terminate the file recovery process, but this may leave the disk or partition in an unpredictable state, which may render it unusable.

If any errors occur during the recovery, an error message will be shown in the dialogue window. Refer to the logs post recovery to establish the cause of any error.





The final steps of the recovery are to:

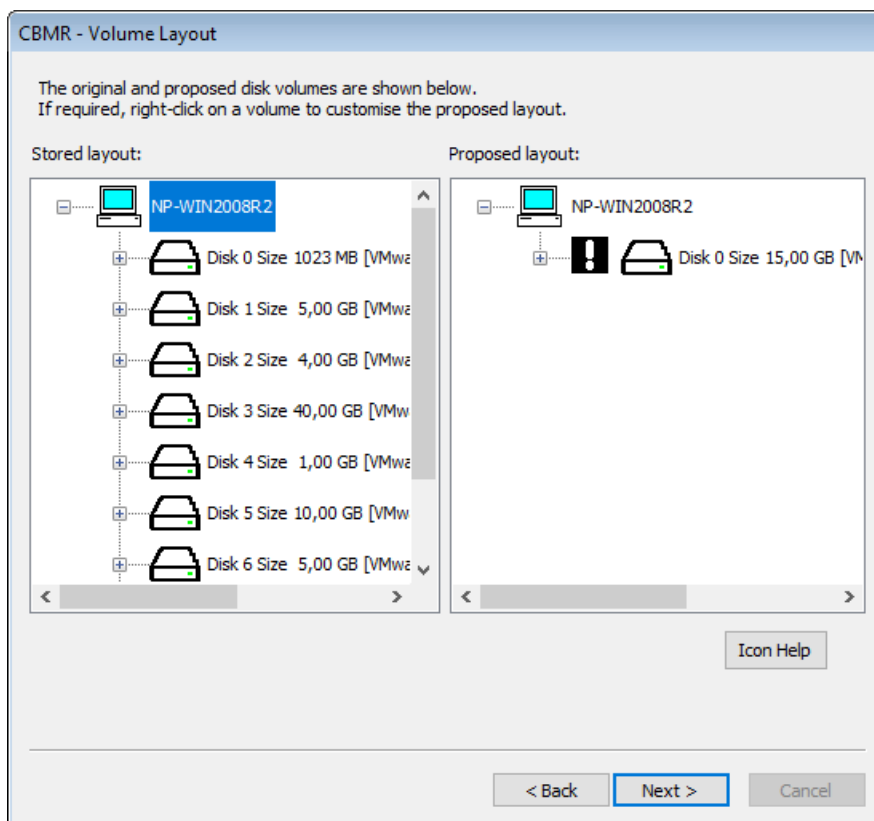
- run a sanity check to determine if all the expected boot files are present on the boot volume
- run a dissimilar hardware check to determine if new drivers are required for new boot devices

Finally, press **Close** to return to the **Recovery Environment** main menu. At this point, you may want to view the recovery logs and perhaps copy the logs to a local device or remote share before selecting to reboot. If you have configured the logfile save path from the first step the logfiles will be automatically saved anyway.

*Note: recovery logs are also saved to the recovered system to the CBMR installation sub-folder 'Temp' (e.g. "C:\Program Files\Cristie\CBMR\Temp").*

### 4.2.13 Disk Scaling

In situations where the target system has fewer or smaller disks than the original system, *Disk Scaling* will come into effect.



The above example shows a recovery from an original system with 8 physical disks, to a target system with only one disk. The target disk is also much smaller than the original system disk.

In this scenario, CBMR will select as many disks to recover as possible (in this case only one disk - the boot disk). In addition, it will scale the partitions down in proportion to their original size and occupancy. This can be complicated by having, say, mirrored dynamic



volumes when the mirror will need to be broken - if only one disk exists on the target (or it has been tagged as not to modify).

*Note 1: the Volume Layout dialogue will only show disks in the left hand panel that can be removed.*

*Note 2: during a recovery to a system with larger disks, the partition sizes will remain the same as the original by default. However, in this case, it is possible to increase partition size manually during the recovery by right-clicking on the partition icon and selecting [Modify](#).*

