TBMR For Windows

Bare Machine Recovery for IBM Spectrum Protect

User Guide

Version 9.6.1 released April 2024

Cristie Software Ltd.
New Mill, Chestnut Lane, Stroud GL5 3EW, United Kingdom
Tel:+44(0)1453 847000 | sales@cristie.com | support@cristie.com | www.cristie.com

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

Tel: +44 (0) 1453 847009
Email: support@cristie.com
Website: https://www.cristie.com

Contents

1 Document Conventions

The following typographical conventions are used throughout this guide:

`/etc/passwd`	represents command-line commands, options, parameters, directory names and filenames
Next >	used to signify clickable buttons on a GUI dialogue
Note:	describes something of importance related to the current topic

2 Overview

This document describes the essential elements of **Bare Machine Recovery for IBM Spectrum Protect** (**TBMR**) and Disaster Recovery based upon a tailored WinPE5, WinPE10 or WinPE11 recovery module. It is based upon version 9.6.1 of the software.

This document describes the steps required to install, configure and use the Bare Machine Recovery for IBM Spectrum Protect (TBMR) product. Refer to the product Readme for installation requirements and late breaking information associated with this release.

2.1 Prerequisites

> ***Note: Please refer to the product Readme for the supported operating systems, RAM and free disk space required. A full list of supported IBM Spectrum Protect clients and servers is included in the Readme.***

It is recommended that Windows **VSS** (**Volume Shadow Copy Services**) is enabled for all drives being backed up to ensure that all open files are captured by the IBM Spectrum Protect backup process. This will allow important OS and application data files that are normally held open to be successfully and consistently backed up.

> ***Note that by default the IBM Spectrum Protect backup client will enable VSS for System State and System Services, but not necessarily all application data files.***

2.2 Backup Process

TBMR allows you to perform a bare machine recovery of your system direct from a IBM Spectrum Protect backup.

To do this you must first prepare your system using the process outlined below:

Installation (refer to the TBMR Installation and Licensing Guide)

- *Install the TBMR configuration software on the client system to be protected*
- *License the software (using a Trial or Full license)*

Configuration

- *Save the configuration parameters.*
- *Install and run the Cristie Recovery ISO Producer (CRISP) tool on a suitable system to create the TBMR WinPE5, WinPE10 or WinPE11 based DR environment. This only needs to be done once.*

Backup system and user data

- Perform regular standard IBM Spectrum Protect backups as required

You will then be ready to Restore the system from the Disaster Recovery Backup.

2.3 Recovery Process

In the event of a disaster, having previously taken a IBM Spectrum Protect backup of the system and stored the configuration information, Windows WinPE5, WinPE10 or WinPE11 mode DR enables you to restore your system to the state at the last IBM Spectrum Protect backup.

The TBMR recovery console must be created first by using the Cristie Recovery ISO Producer (CRISP) tool. The output from this tool is a bootable WinPE5, WinPE10 or WinPE11 ISO which can be either burnt to physical CD/DVD media, imaged to a USB flash drive or used directly in a virtual environment.

If your machine supports bootable USB flash drives or CD/DVDs, this is the most convenient way to boot the DR module. If the system does not support bootable USB flash drives or CD/DVDs, you can boot from the network. Contact Cristie for details on how to set this up.

Windows WinPE5, WinPE10 or WinPE11 offers several advantages, namely:

- *a familiar Windows GUI*
- *the ability to inject new mass storage drivers during the boot process*
- *all variations of Windows dynamic disks are supported (ie. mirrored, spanned, striped and RAID-5)*
- *NTFS volumes/partitions are created natively*
- *support for NTFS mounted folders (junctions) and hard links*
- *the restored backup contains the original file security information*

The WinPE5, WinPE10 or WinPE11 recovery process has five main steps:

1. *Load Configuration data*
2. *Rebuild storage devices (hard disks)*
3. *Restore OS files from an IBM Spectrum Protect backup*
4. *Dissimilar Hardware and inject new drivers (if necessary)*
5. *BIOS (MBR) to UEFI (GPT)/UEFI to BIOS conversion*
6. *Boot into the recovered system*

3 Create The Bootable Recovery Environment

The supplied CRISP tool is used to create the TBMR recovery environment. This environment is based upon a customised version of Microsoft's WinPE version 5 (WinPE5), WinPE10 or WinPE11.

Cristie Software Ltd. recommend using the WinPE10 or WinPE11 based environment if possible. This is based upon Windows 10/11 and is more likely to be compatible with modern hardware. Use the WinPE5 legacy version for Windows 2012R2 or earlier.

Once created the recovery environment is booted on the target system and then manages the restore process.

The CRISP tool should be run in conjunction with the supplied CRISP WinPE5, WinPE10 and WinPE11 Filesets for TBMR 9.6. The fileset(s) should be installed alongside the CRISP on the same host.

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

Output from the CRISP tool is either a bootable WinPE5, WinPE10 or WinPE11 ISO file which can then be burnt to physical media (CD or DVD) or mounted directly in a VM environment or a bootable USB flash drive. This media is then booted on the target machine to manage the recovery operation.

> ***Note: Microsoft Powershell is now available in the WinPE5, WinPE10 or WinPE11 DR environments. However this option must be selected when you create the ISO or bootable USB flash drive.***

4 The TBMR Create Configuration Tool

Configuration information is saved by default to the **TBMRCFG** folder on the Windows system partition. This cannot be changed.

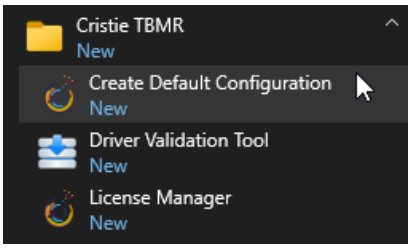
The Cristie tool that provides this function is called **TBMRCfg.exe** which is located in the TBMR installation folder (normally **Program Files\Cristie\TBMR**). This is a command line only tool which is licensed for use for a 30 initial day trial period. A full license is required to use the program beyond the trial period.

As part of this process, details about the hard disks, operating system, storage controller (s), network adapter(s) and network settings will be queried and stored. You can override some of these details if you wish. The result of the configuration creation (success or failure) is recorded in the Windows Application Event Log.

The next sections discuss this process in more detail.

4.1 Creating the Configuration Information

The easiest way to create the configuration manually is to select the Create Default Configuration shortcut provided on the Start menu for TBMR. Note however that an initial configuration is created during the TBMR installation process.



This will create a new configuration using the default settings.

```
================================================================================
              TBMR Configuration Utility Version 9.6 for x64
            Copyright (C) 2009-2024 Cristie Software Limited
================================================================================

Copying the EFI files ...
Successfully copied the EFI files
Created a snapshot of C:\ --> A:\
Searching for files missed under C:\Users ...
Searching for files missed under C:\Windows\ServiceProfiles ...
Searching for files missed under C:\Windows\WinSxS ...
Successfully copied the missed assembly directory
Searching for files missed under C:\Windows\System32 ...
Saving hard-link information ...
Successfully saved hard-link information
Configuration was stored successfully
```

If you need to select non-default settings, then you will need to create the configuration manually. Run a command window and navigate to the folder where TBMR is installed.

The TBMR configuration program is called **TBMRCfg.exe**. Enter the command `TBMRCfg.exe /?`, this will display the command line options available.

```
c:\Program Files\Cristie\TBMR>TBMRCfg /?

================================================================================
               TBMR Configuration Utility Version 9.6 for x64
              Copyright (C) 2009-2024 Cristie Software Limited
================================================================================


Usage: TBMRCFG.EXE [options]

Options are:

/help or /?  - Show usage
/format <Drives to format|all> - Format  additional volumes during recovery
         Specify drives separated by comma as in /format D,E,F

         For a volume that does not have a drive letter but mounted
         under a folder, enter the mounted folder as in
         /format D,D:\MountedVolume
         /format all will format all partitions on all disks

/skiphardlinks - Skip hard-link processing for CoBMR block-based backups
                 and RBMR volume group backups only

The configuration will always be stored in %%SystemDrive%%\TBMRCFG

c:\Program Files\Cristie\TBMR>
```

The command line options are very simple:

/help or **/?**

shows **TBMRCfg** usage. This displays the command option summary.

/format <Drives to format | all>

The /format option allows disk volumes other than the Windows drive to be formatted during the recovery. By default, only the Windows volume will be formatted. There is an exception to this if Windows is not contained within the first partition of the disk. In that case, both the Boot partition and the Windows partition will be configured for formatting. However, regardless of this setting, the WinPE5, WinPE10 or WinPE11 based recovery environment will allow any or all partitions to be formatted.

So, for example, if volumes D:, E: and F: are to be additionally formatted during recovery, enter:

`TBMRCfg.exe /format D,E,F` (separate the drive letters using a comma)

Enter the following to back up all partitions on all drives on the system:

```
TBMRCfg.exe /format all
```

Volumes mounted on local folders not having a drive letter can be specified like this:

```
TBMRCfg.exe /format D:\MountedVolume
```

where D:\MountedVolume is the folder mount point. An example using both normal partitions and a mounted volume is:

```
TBMRCfg.exe /format D,D:\MountedVolume
```

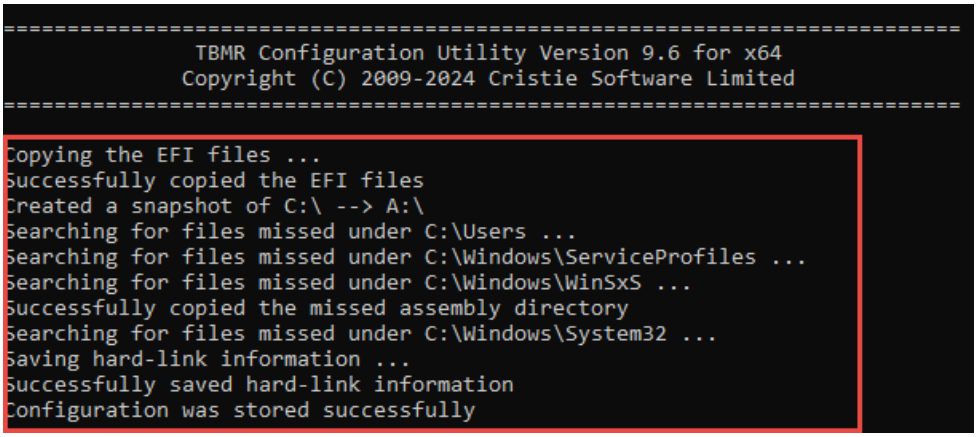
TBMRCfg stores the configuration in %SystemDrive%\TBMRCFG folder (%SystemDrive% is the drive associated with the Windows folder, usually C:\). This location cannot be changed.

> *Note: it is important to remember that the TBMR configuration must be created before the BA Client backup is made. Cristie suggests that this is done by creating a job to run on the IBM Spectrum Protect Scheduler containing a script that calls the TBMR Cfg.exe program installed in the TBMR installation folder.*

4.2 Backup of Boot and SystemState Files

On all Windows OS's, files additional to the standard IBM Spectrum Protect backup dataset must be copied and saved. These include boot files and SystemState objects which are not normally backed up by the BA Client on these OS's.

Some of the additional files backed up are also locked at the time of backup and must be backed up using the Windows Open File Manager **VSS**. So when TBMRCfg runs, it invokes VSS to take a snapshot copy of these extra files:



4.3 Creating a TBMRcfg Pre-Schedule

Spectrum Protect TBMR Pre-schedule.

The configuration program of Cristie TBMR includes creating a file that records how your system is built, e.g. amount of RAM, CPU, number of disks, filesystems, OS level etc. It is imperative that this file is kept up to date to reflect any changes to your systems.

With the Pre-Schedule command the configuration can run automatically before the Spectrum Protect backup, this way the config is always up to date.

In order to execute tbmrcfg.exe as a pre-schedule command for your Windows Spectrum Protect TSM incremental backups, you need to add a line to the dsm.opt file of the system you are protecting.

Open the dsm.opt file and enter the content below:

```
PRESCHEDULECMD 'C:\"Program Files"\Cristie\TBMR\tbmrcfg.exe'
```

NOTE: please notice the ' and ' at the beginning and end of the path. These are required for the program to run correctly.

Save the file.

The next time Spectrum Protect TSM triggers a backup of the system, the tbmrcfg program will run first to update the Cristie configuration file.

5 Using a IBM Spectrum Protect Backup for Disaster Recovery

TBMR allows a previously created IBM Spectrum Protect backup or backupset to be used as a DR backup.

As long as the TBMR configuration has been created (see previous section) and a IBM Spectrum Protect backup is performed afterwards, then it will be possible to recover the system using the DR environment.

Please take note of the following important considerations:

When performing backups ensure that the IBM Spectrum Protect snapshot client option VSS is selected.

> ***Note: this document does not describe how to create IBM Spectrum Protect backups. Please refer to your IBM Spectrum Protect Administrator's Guide for details.***

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

5.1 Encrypted Backups

TBMR supports encrypted IBM Spectrum Protect backups. This can be enabled in IBM Spectrum Protect by adding the line:

```
INCLUDE.ENCRYPT "*:\...\*"
```

to the dsm.opt file. TBMR works by creating the system configuration into the folder TBMRCFG. So the line above would mean that when the IBM Spectrum Protect backup is created, the TBMRCFG folder is also encrypted. This is not a problem, but would mean that you will be prompted for the password during the recovery. If you wish to avoid this prompt, add this additional line to dsm.opt after the line above:

```
EXCLUDE.ENCRYPT "*:\TBMRCFG\*"
```

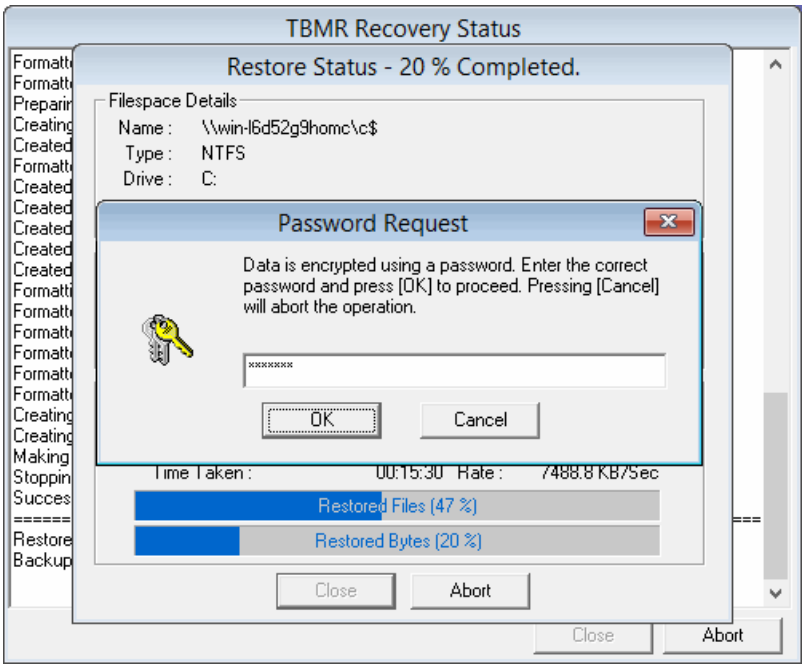
You can choose to always prompt for the encryption key password by adding this line to dsm.opt:

```
ENCRYPTKEY prompt
```

You will be prompted for the encryption key as follows:

You should also select the appropriate encryption algorithm for your backup.

If the folder containing the TBMR configuration has been encrypted, then during the recovery you will be prompted for the password:



If the configuration folder has been excluded from the encryption (as described above), you will be prompted for the password during the Restore Files phase of the DR.

Please enter the same password you entered during the backup.

> ***Note 1: if you have elected to have the password stored locally (via the BA Client Preferences menu) and the TBMR configuration has been created post this change, then you will not be prompted for the password during the recovery. You may also need to perform a 'dummy' backup first to get the password stored locally before generating the TBMR configuration.***

> ***Note 2: Cristie recommends using a single password for the entire encrypted backup. With IBM Spectrum Protect it is possible to backup parts of the system with a different password. This could lead to confusion during the recovery and is discouraged.***

5.2 Image Backups

TBMR supports IBM Spectrum Protect backups of the form incremental, image and backupsets. However, for image backups, it is essential that in addition to the image backup, an incremental backup of the TBMRCFG folder is made to the same Node.

This is because it is not possible to retrieve the configuration details from an image backup.

> ***Note: if this extra incremental backup is not made, then it will not be possible to perform a DR. It is also not possible to restore an image backup to a smaller disk partition.***

5.3 Backupsets

TBMR now supports DR recovery from IBM Spectrum Protect backupsets. At the moment, TBMR only supports online backupsets (ie. those maintained in a Node on a IBM Spectrum Protect server). Typically a backupset is created with a **dsmadmc** command such as:

```
Generate Backupset <Nodename> <Prefix> Description="This is a backupset test"
Retention=Nolimit Wait=Yes Datatype=File TOC=Yes DevClass=File
```

Where <Nodename> is the name of the node on the IBM Spectrum Protect server, <Prefix> is a short prefix to add to the backupset name.

Note that a backupset is created from a backup already present in the specified node. If this backup does not already contain a backup of the TBMRCFG folder generated by the TBMRCfg program, it will not be possible to recover the system from the backupset.

It is essential to specify TOC=Yes. **TBMR cannot recover a backupset created without a TOC (Table of Contents).**

5.4 Transitional Nodes

If you backup to a node located on an Spectrum Protect Server version 7.1.8 or 8.1.2 and above, using an Spectrum Protect version that is less 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 Spectrum Protect client version later 8.1.2 or later that enforces SSL communication. This will prevent older Spectrum Protect clients from accessing the node.

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

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

6 Restoring your System

This section discusses the steps required to run a recover sequence using the TBMR Recovery Environment. This is booted from the media created by CRISP in conjunction with the CRISP WinPE5, WinPE10 and WinPE11 Filesets for TBMR 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 TBMR recovery sequence consists of the following steps.

1. *Install and run the **Cristie Recovery ISO Producer** (**CRISP**) tool on a suitable system to create the TBMR WinPE5, WinPE10 or WinPE11 based recovery environment either as a CD/DVD ISO image or direct to a USB flash drive. This only needs to be done once per IBM Spectrum Protect client used.*
2. *Boot the TBMR 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 IBM Spectrum Protect 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.*

6.1 Booting the WinPE5, WinPE10 or WinPE11 DR Environment

Insert the bootable TBMR WinPE5 ,WinPE10 or WinPE11 DR CD/DVD or USB flash drive and reboot the machine. By default you will be prompted to **Press any key to boot from the CD or DVD** unless you have disabled this feature when creating the ISO/USB flash drive in CRISP.

This prompt is only made for a few seconds before the system will attempt to boot the underlying OS, so you will need to react quickly.

> ***Note: It is possible to suppress this prompt completely during the ISO/USB flash drive creation stage. If the prompt is disabled then the DR ISO/USB flash drive image will always booted by default. Please refer to CRISP documentation which describes how to do this.***

To support devices (for example a new mass storage controller) not supported in the current DR environment, WinPE5, WinPE10 or WinPE11 allows drivers for any device to be injected at any time post boot. Refer to the section titled Load a Driver for information on how to do this. Ensure you add the correct driver version; 64-bit for WinPE5/WinPE10/ WinPE11.

6.2 WinPE5, WinPE10 or WinPE11 Based TBMR Recovery Environment

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

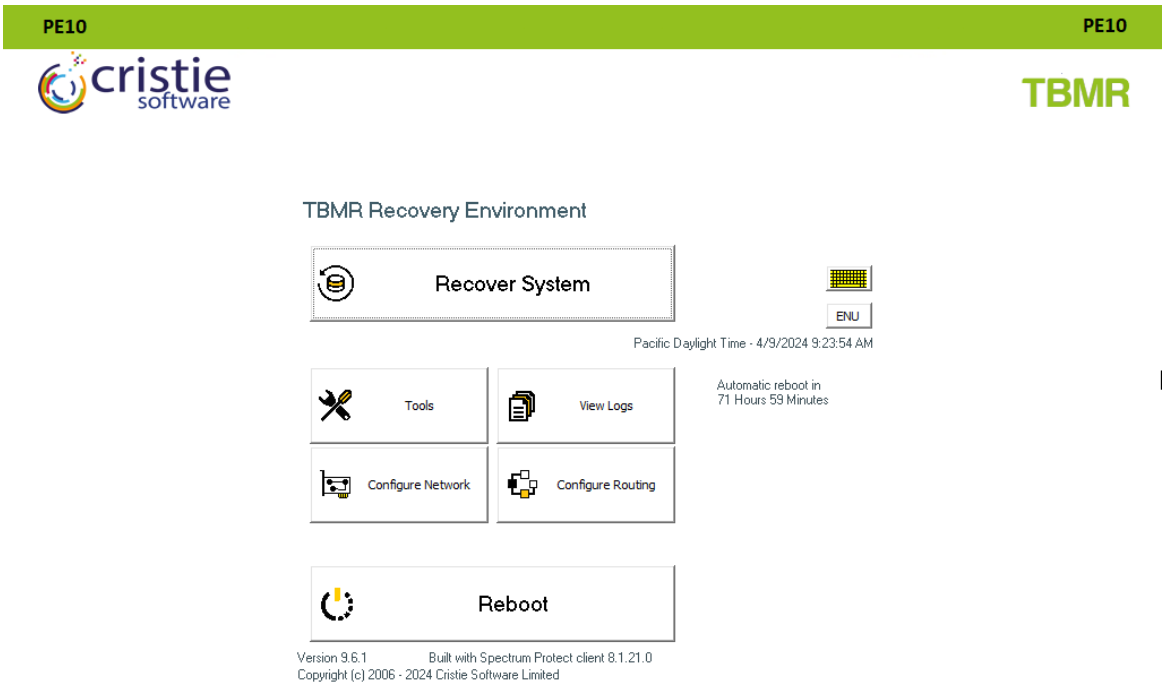
During the boot process, WinPE5, WinPE10 or WinPE11 drivers for your **Plug and Play** devices will be loaded - in particular the **Mass Storage** devices and **Network Adapters**. When the WinPE5, WinPE10 or WinPE11 system has fully booted, it is possible to remove the CD/DVD or USB flash drive if you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

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

6.2.1 TBMR 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 **TBMR 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.

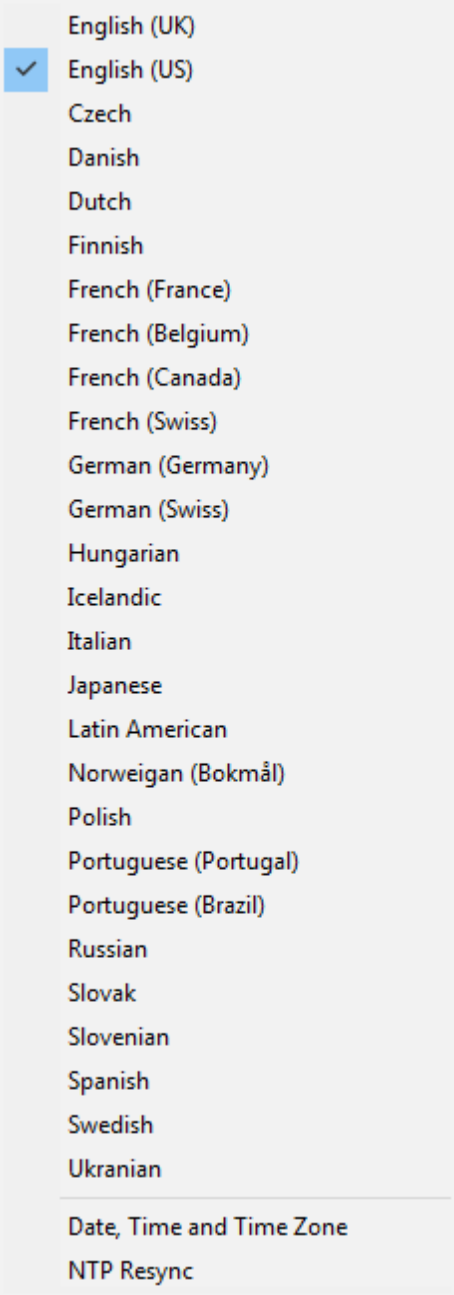
A reboot countdown clock is shown 

. 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 

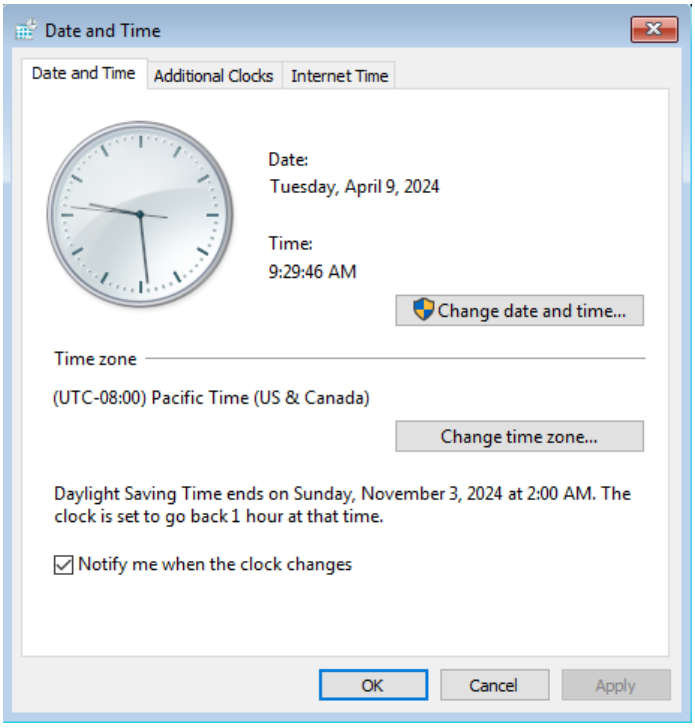
icon. Note this icon will be shown according to the locale of the host system used to create the ISO/USB flash drive using the CRISP utility so it may not match the version shown here. So if, for example, the ISO/USB flash drive was built on a machine configured with a UK locale it will be displayed as 

.



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.

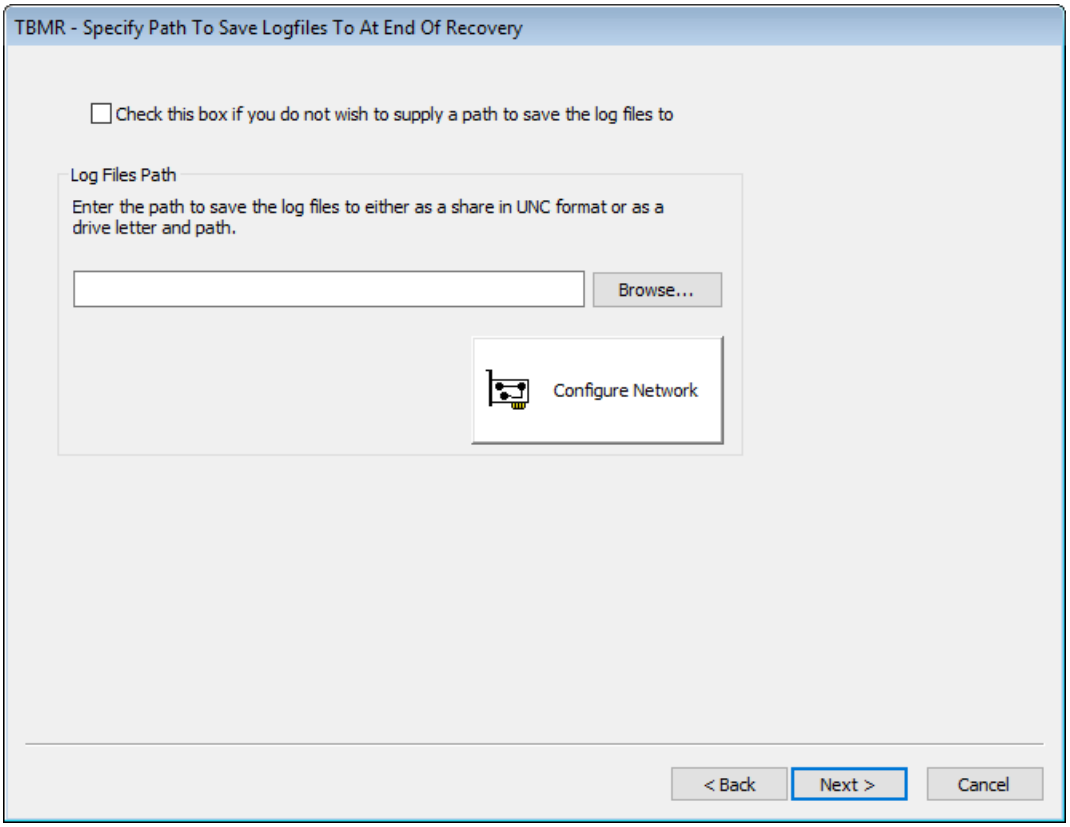
Note the DR environment requires a working mouse as a minimum.

6.2.2 Begin the Restore Process

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

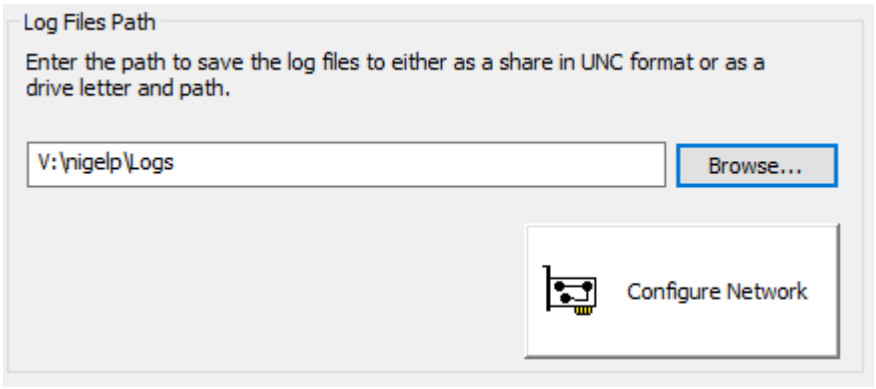
6.2.2.1 Logfile Save Path

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.

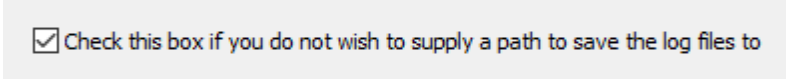


For example, use the 

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.

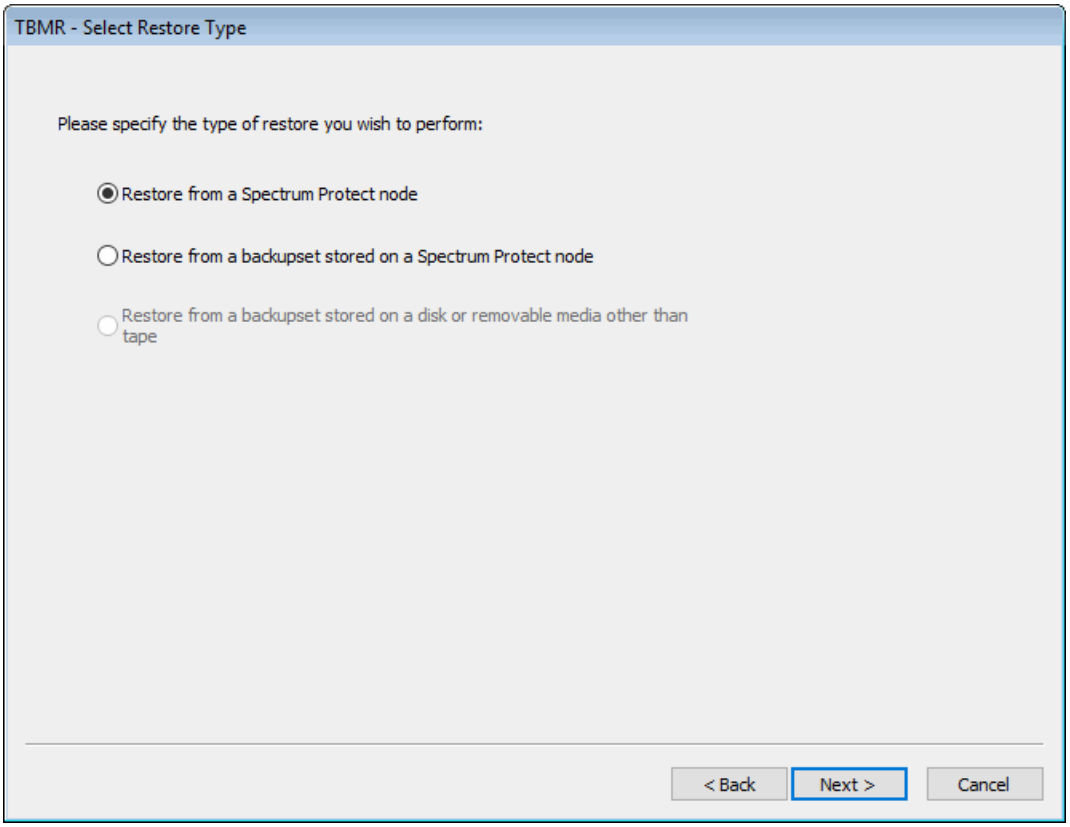


Click Next > to continue to the next step.

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

6.2.2.2 Select Restore Type

It is possible to restore from an IBM Spectrum Protect node or an online backupset. Make your choice and press Next> to continue.

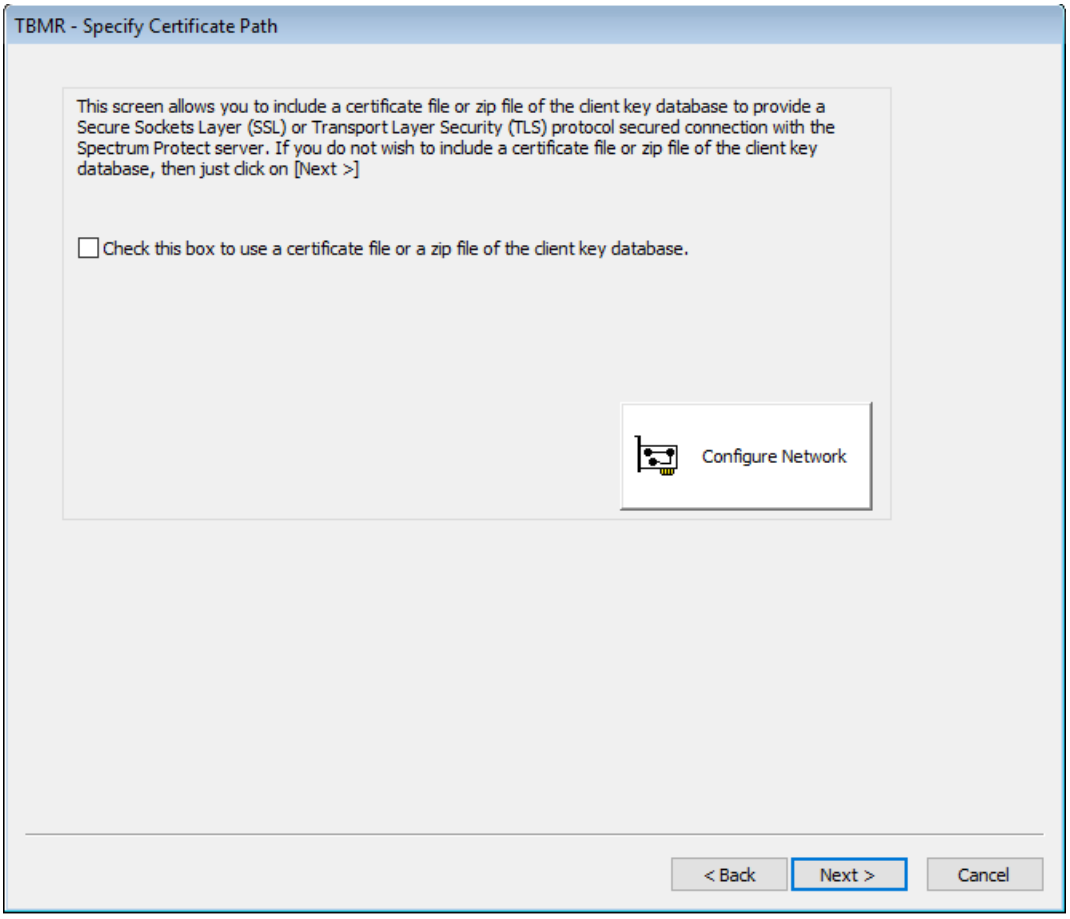


Restore from Node

If you selected **Restore from a IBM Spectrum Protect Node**, select Next>. This will then display the **Specify Certificate Path** dialogue as shown in the next section.

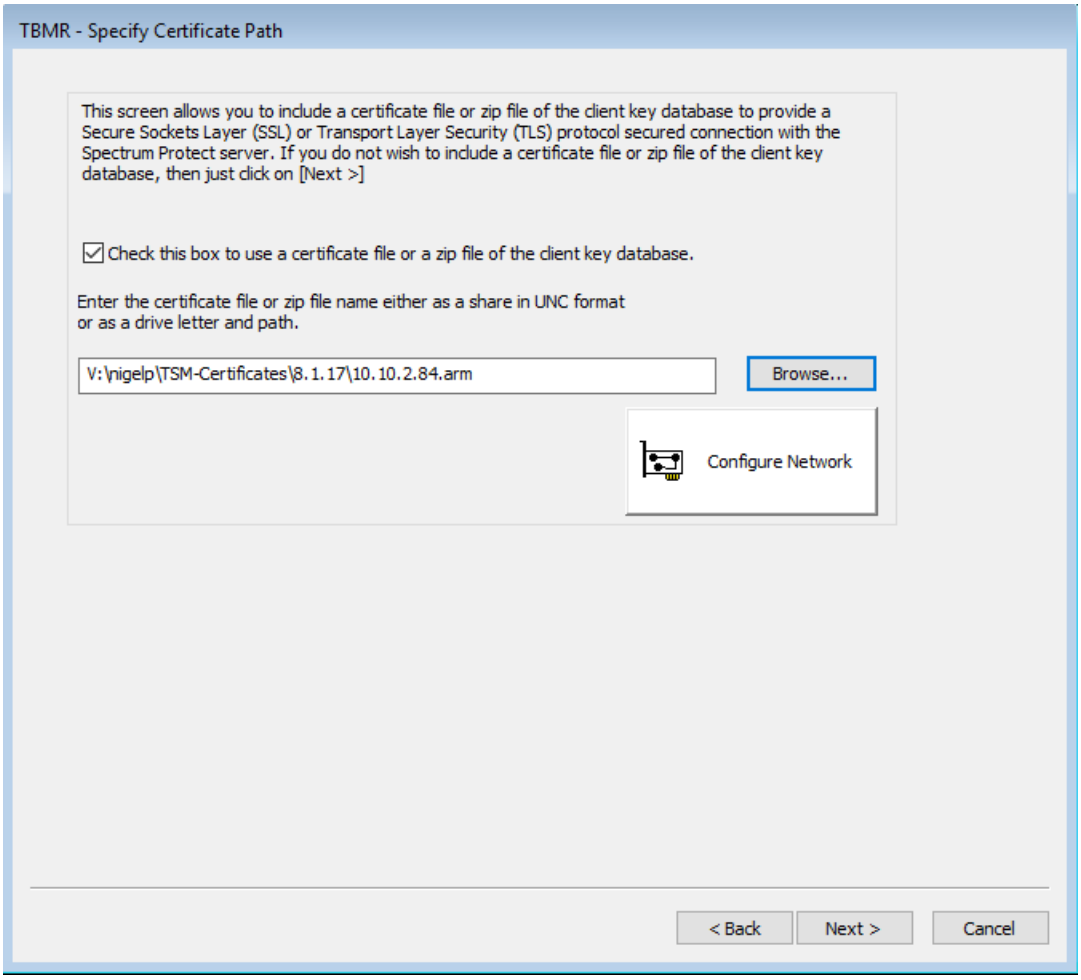
Specify Certificate File

The first step of Restore from Node allows a **Secure Sockets Layer** (**SSL**) or **Transport Layer Security** (**TLS**) certificate to be provided to the IBM Spectrum Protect server. If you do not require to add an SSL or TLS certificate click Next > to continue directly to the next step.



To add a certificate, click the check box to open up a browser window. Then enter the full path or browse to the location of the certificate file or a zip file containing the certificate(s).

Note: Using a certificate is mandatory for IBM Spectrum Protect servers 8.1.2 or later.

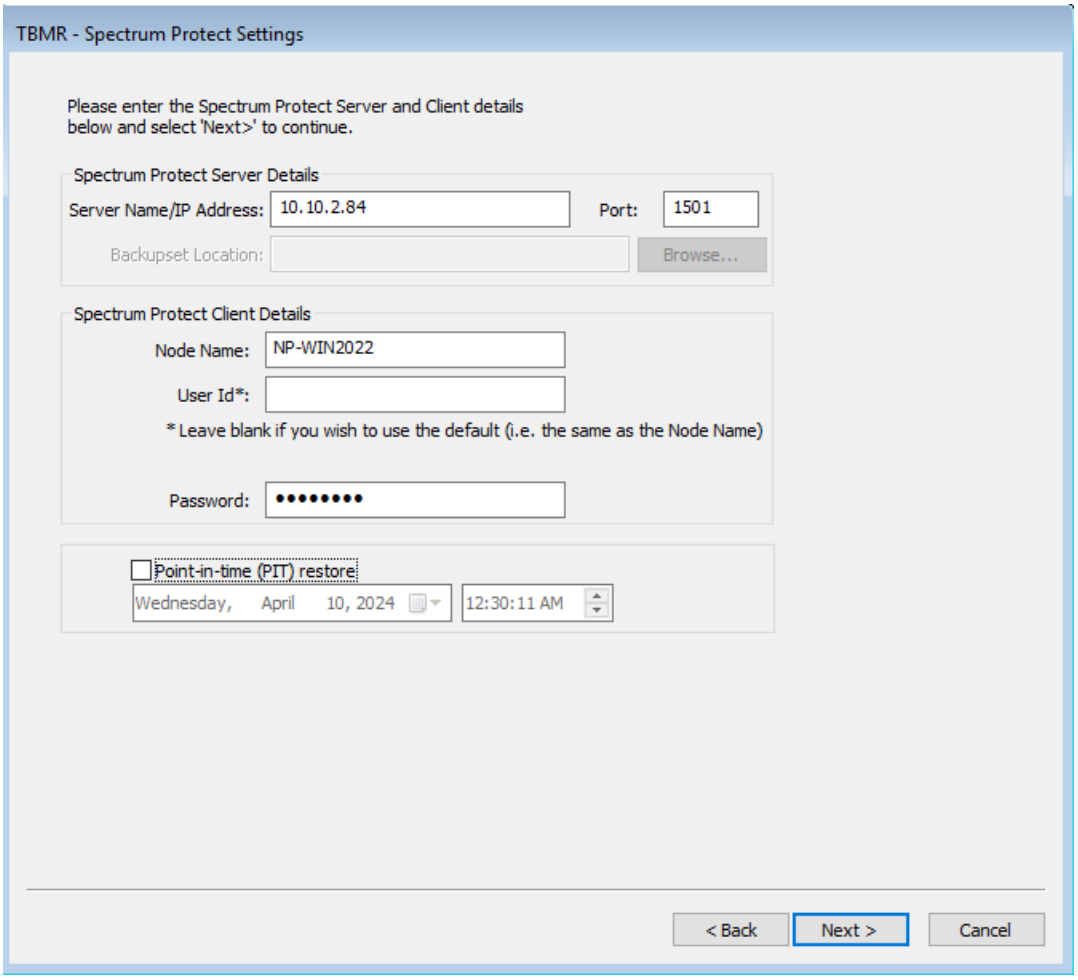


Use the 

button to connect a network share if required (as in the example). Click Next > to continue to the next step.

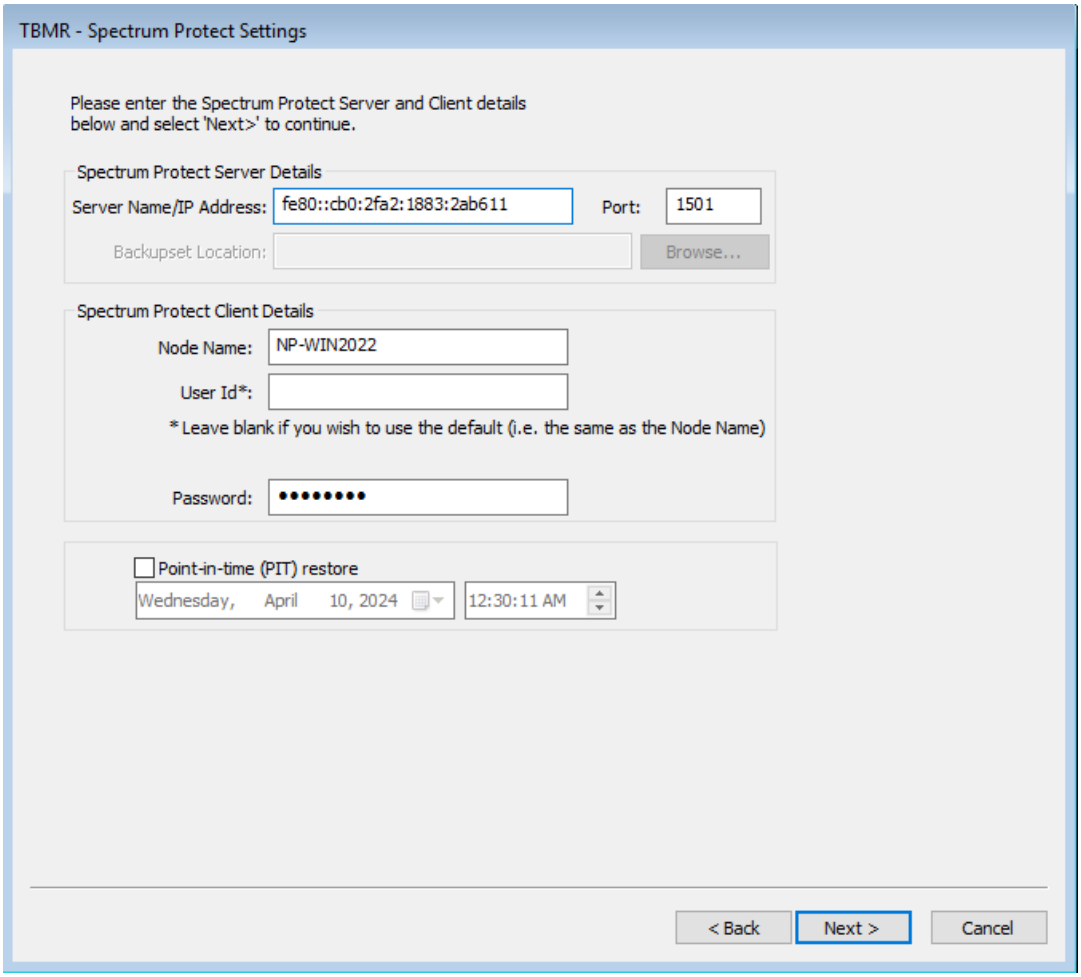
Specify IBM Spectrum Protect Details and Recovery Date/Time

The next step of the restore process identifies the location of the **IBM Spectrum Protect Server and Node** used to back up the Client. The IBM Spectrum Protect server IP address may be expressed in either IPv4 or IPv6 format.



Identify Spectrum Protect server using an IPv4 IP address

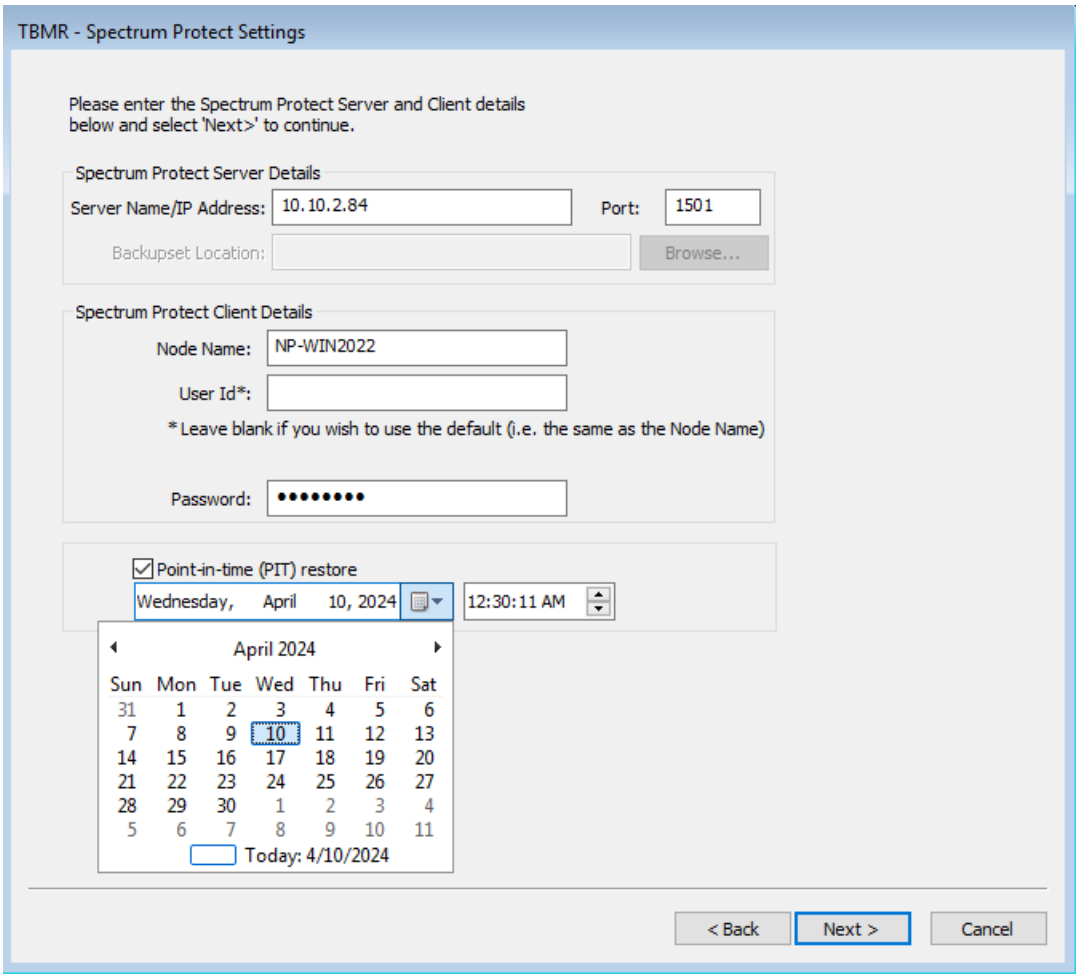
Or,



Identify Spectrum Protect server using an IPv6 IP address

> ***Note: You may use an alternative to the normal Node credentials (such as the Administrator account) to access the account. In this case enter the username of the alternative in the User Id field and the corresponding password.***

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:

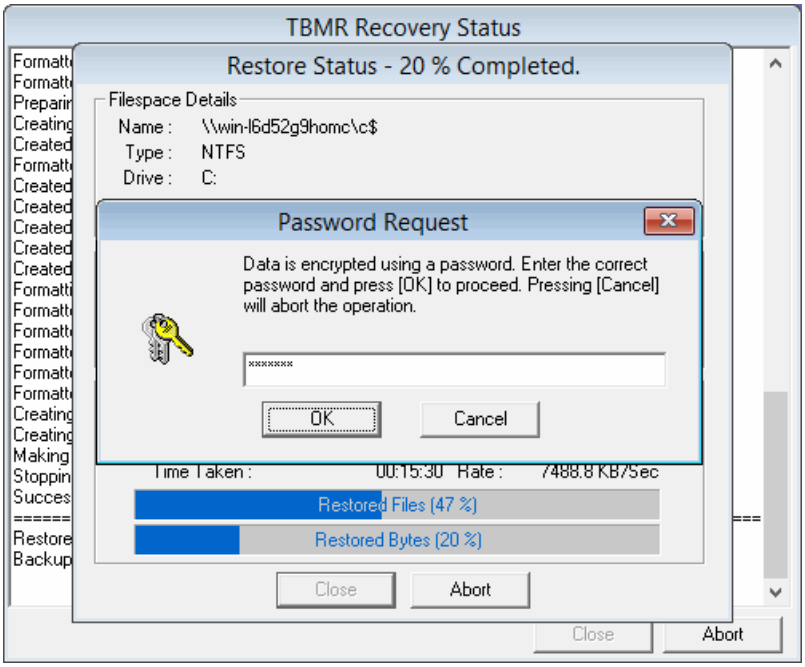


This can be used to scroll the months/years backwards and forwards as necessary.

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

If PIT mode is not selected then, by default, the latest file versions will be restored. Select Next> to continue.

If the backup including the TBMR configuration folder **TBMRCFG** is encrypted, a prompt for the encryption password will be displayed if not held locally:



Enter the password used during the backup. Press OK> to proceed. At this point the Node will be accessed on the specified server and the machine configuration extracted.

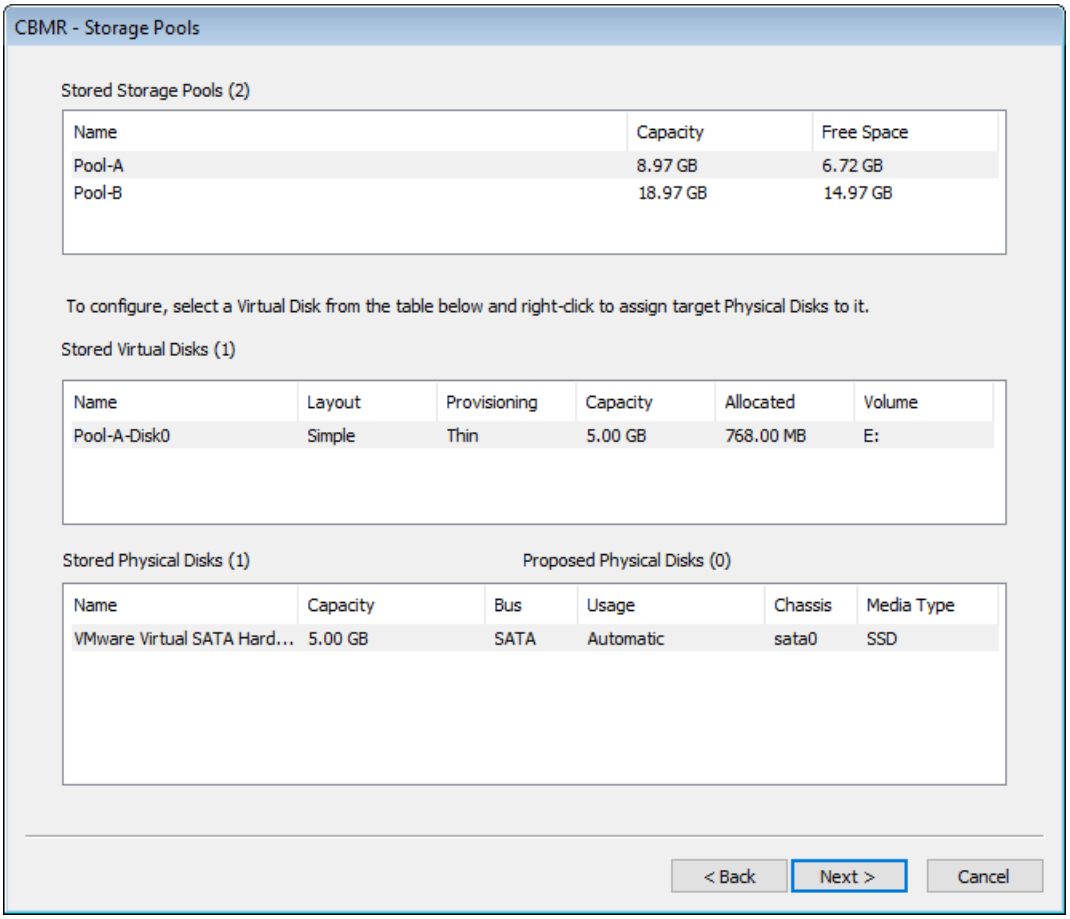
> ***Note: TBMR assumes that TCP/IP is the communication method used between the Client and the Server. Other IBM Spectrum Protect communication methods are not supported.***

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 TBMR DR environment. Do not use the WinPE10 version for Storage Pool recovery.***

The pool/disk configuration dialogue looks like this:



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:

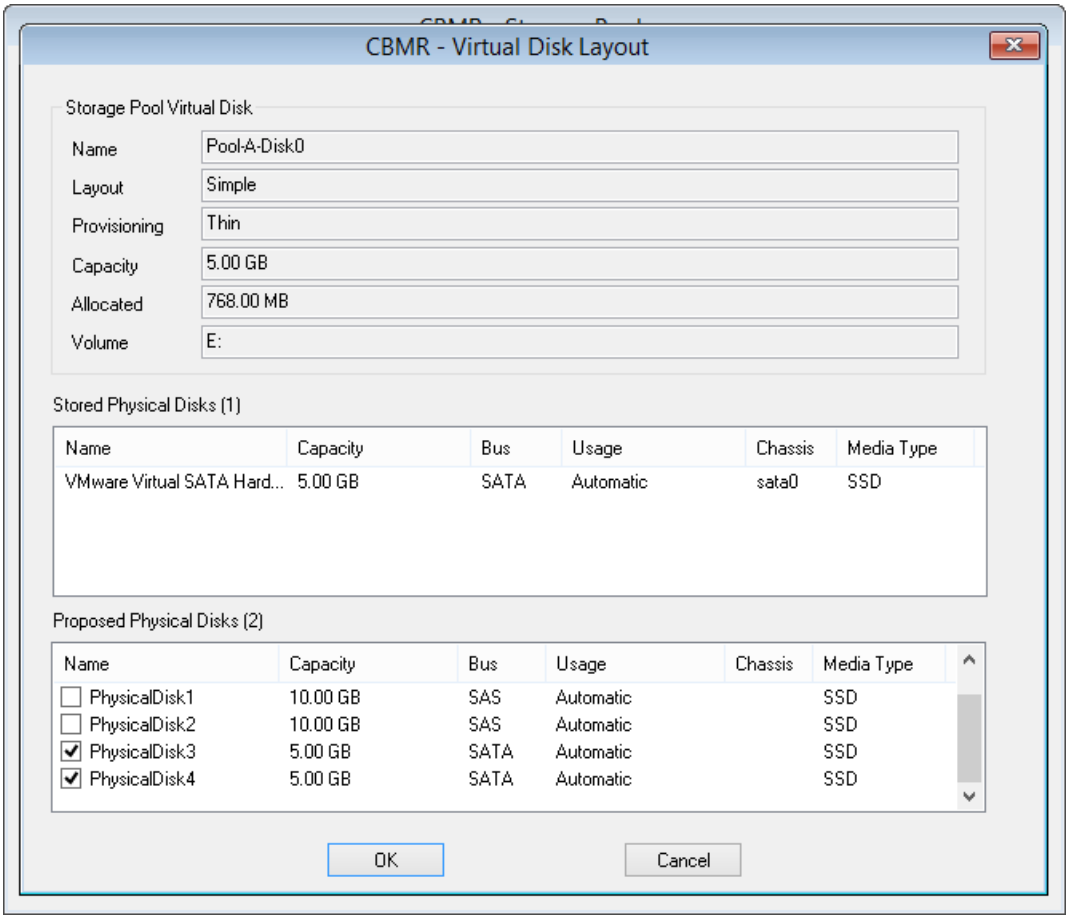
- ***a list of the original configured pools with their corresponding capacity and the free space at the time of the backup.***
- ***a list of the original virtual disks defined for a selected pool together with the corresponding virtual disk layout, provisioning, capacity, size in use and volume letter.***
- ***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).

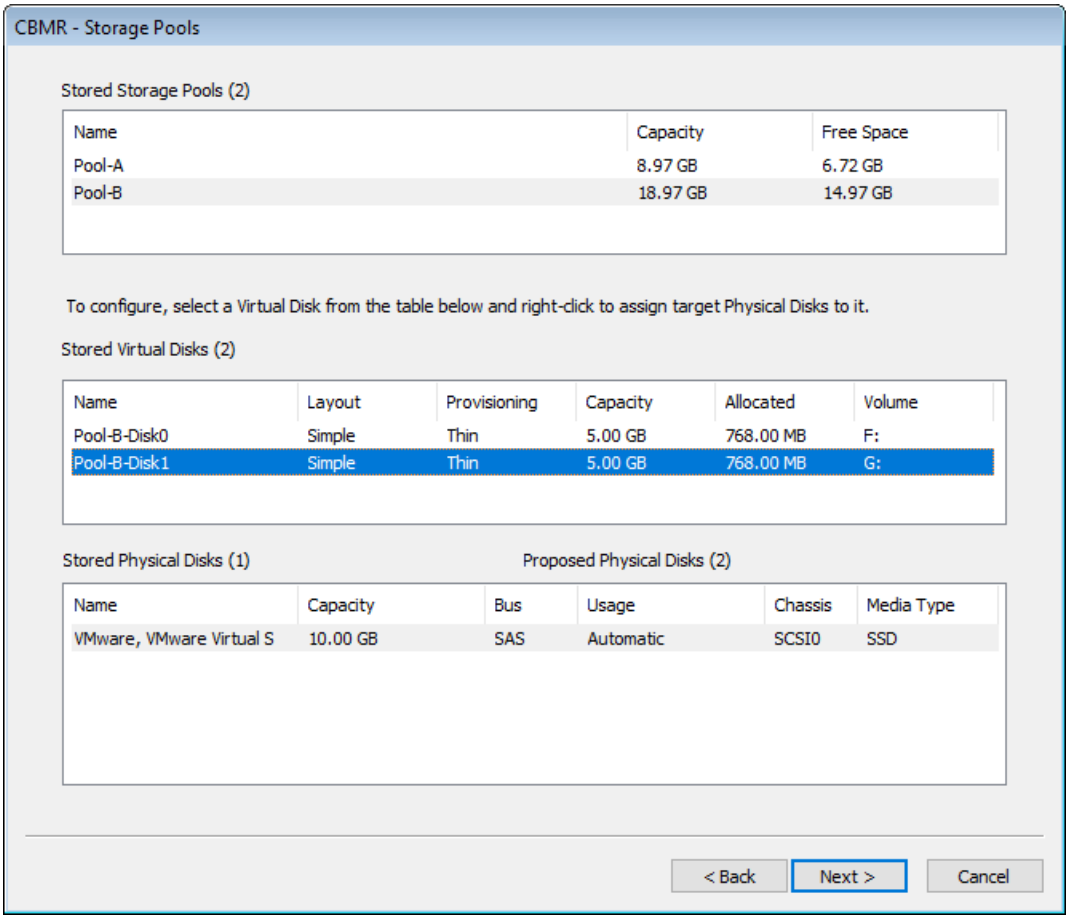
Note that the **Proposed Physical Disks** has a count of zero, i.e. there are no target Physical Disks selected yet to recreate this Virtual Disk from, where **Stored** = **Source system** and **Proposed** = **Target system**.

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



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.

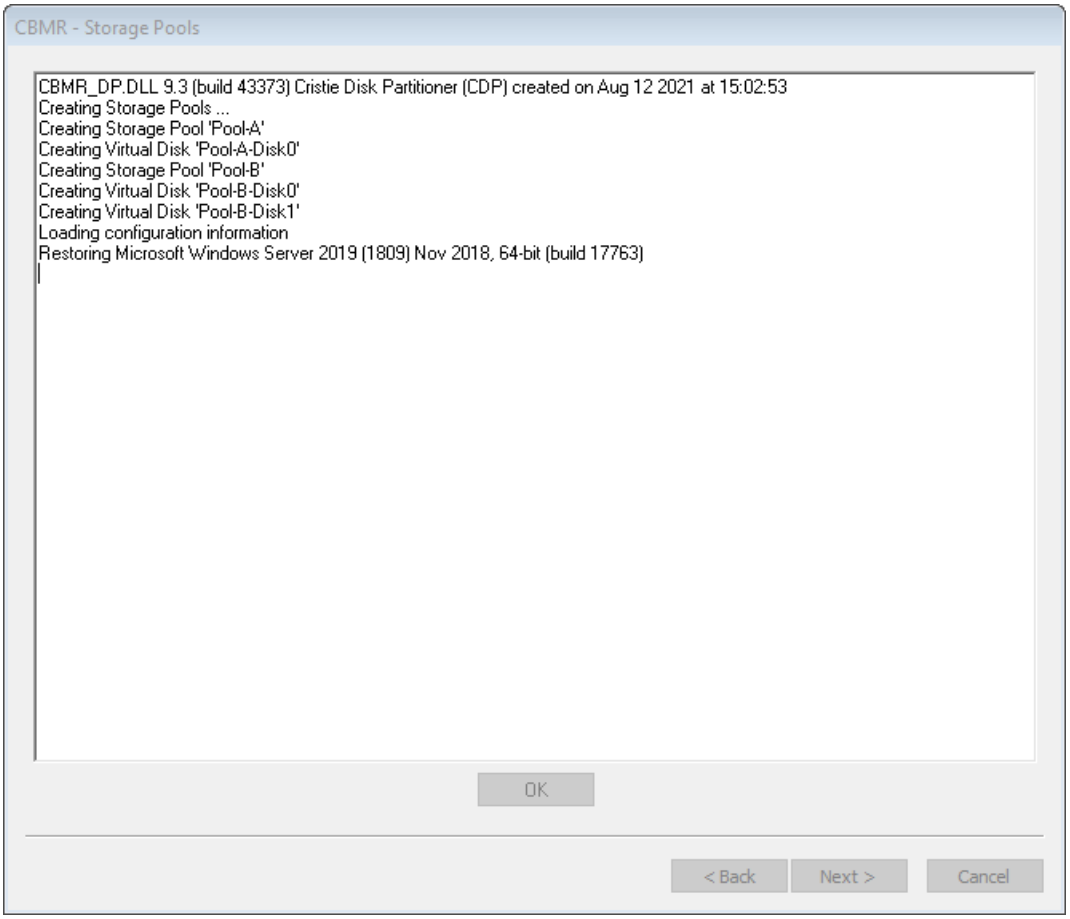
Repeat this process for all the remaining virtual disks in each pool. This results in a configuration similar to this:



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.

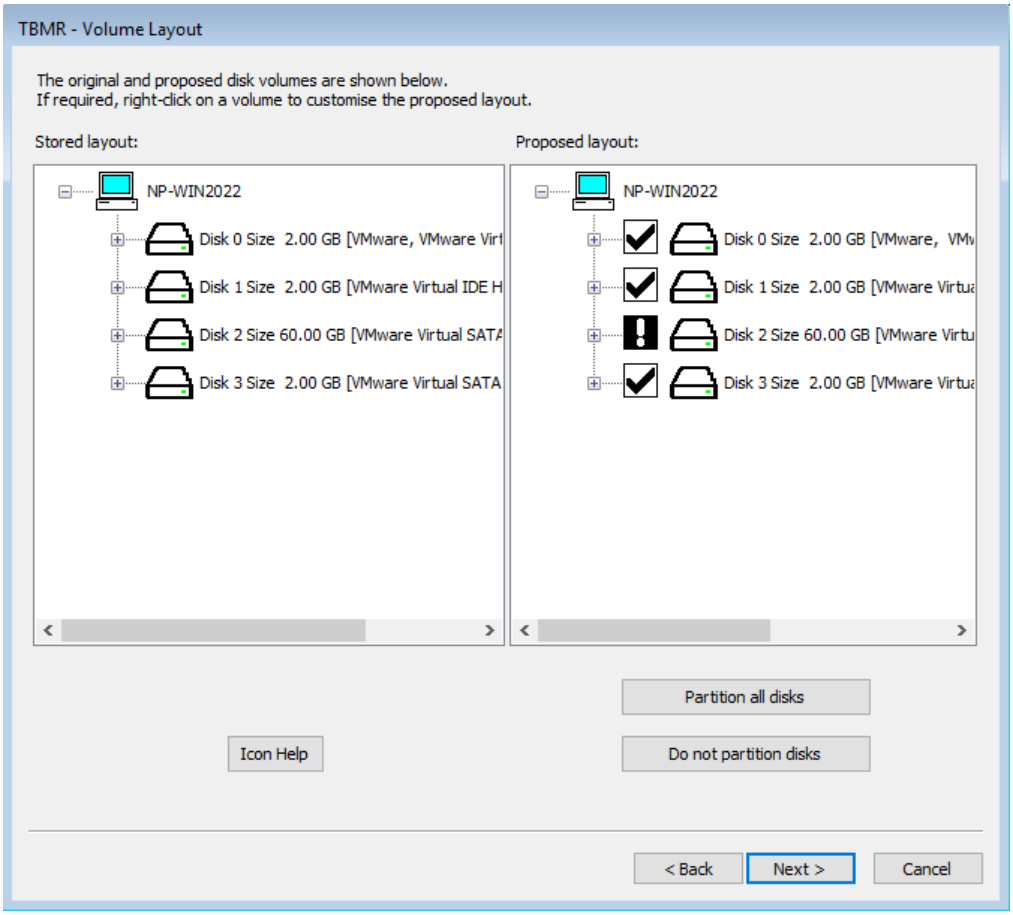
Recovery now runs as normal with no further Storage Pool configuration required.

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

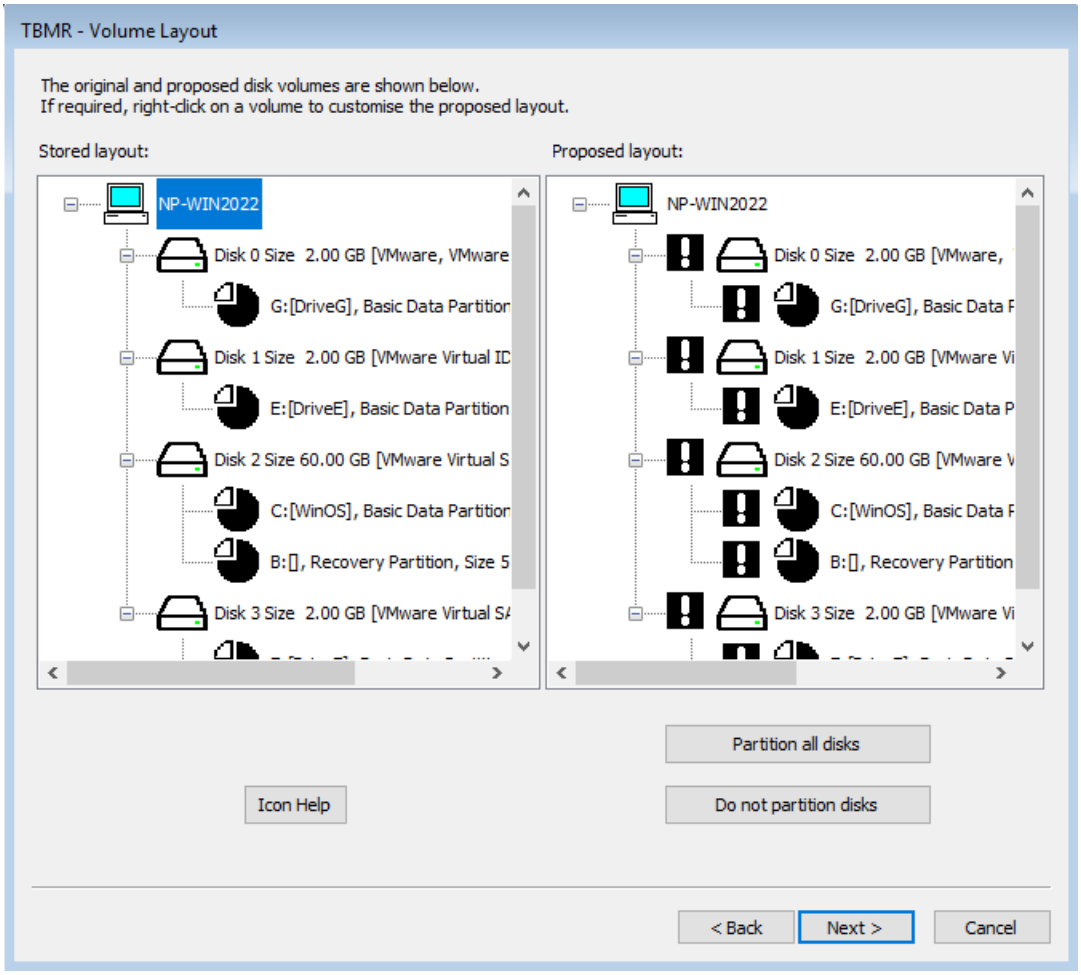
- Storage Pools and virtual disks are recognized by TBMR WinPE5, so if you boot a target system that has them, then WinPE5 will see them and mask out the "real" disks resulting in only the virtual disks being shown.
- The use of NVMe type disks when using VMWare WorkStation is not recommended when using Storage Pools.
- Physical disks used in Storage Pools should have minimum size of at least 8 GB.
- Only the TBMR 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.

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 Partition all disks.

If you wish to quickly disable the partitioning of all target disks click Do not partition disks.

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.

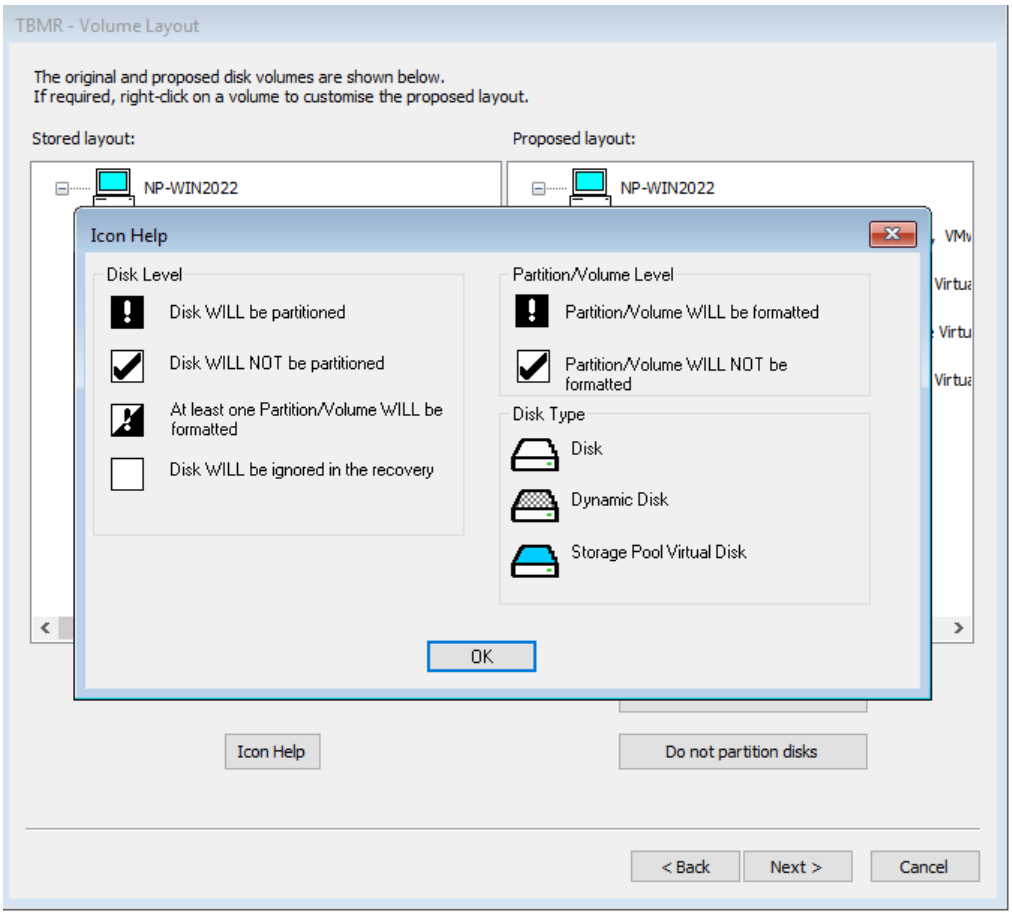
There are 3 disk types available:

 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:

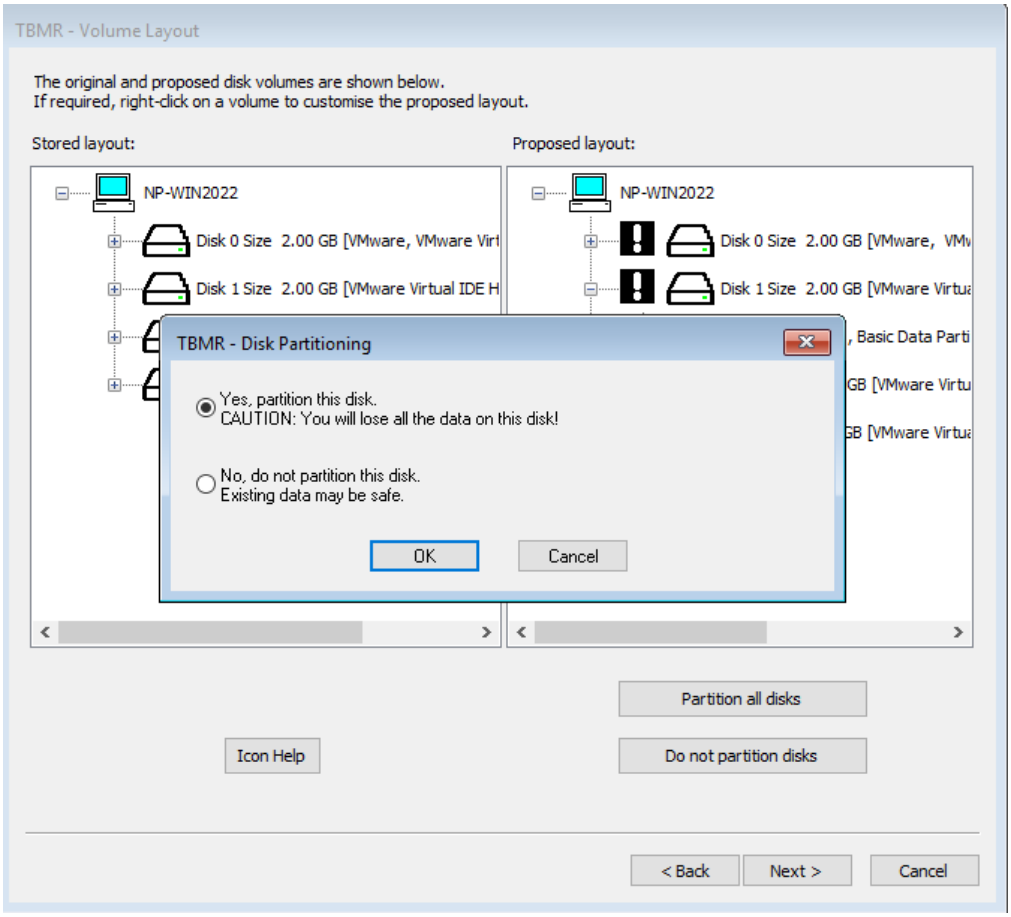


When the recovery is to the original system, the contents of both panels will look similar if the number of disks is the same. Possibly the disk sizes will be different.

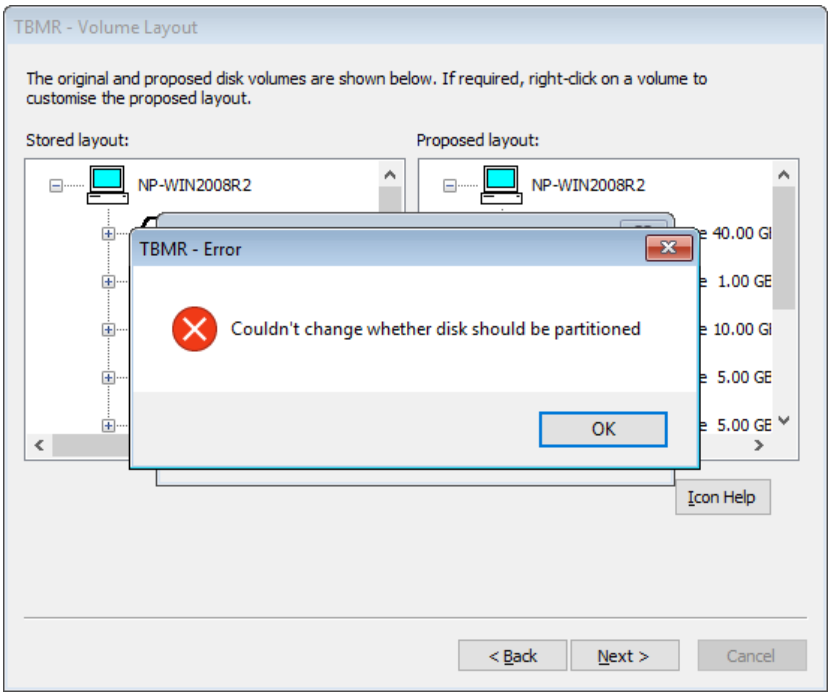
When performing a recovery to a dissimilar system, the disk mapping can be much more complex. Some of the criteria used to judge the disk mapping are:

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

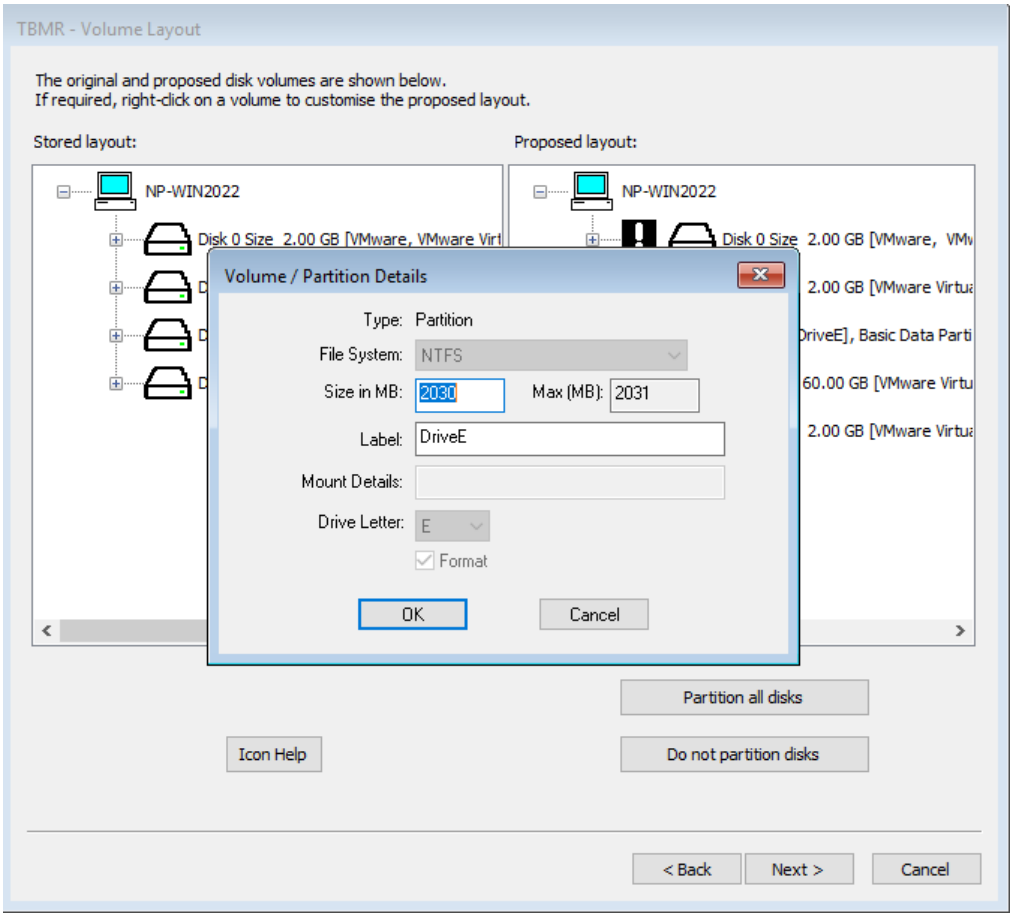
You may right-click on any disk shown in the right-hand panel to select whether the disk will be partitioned or not.



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



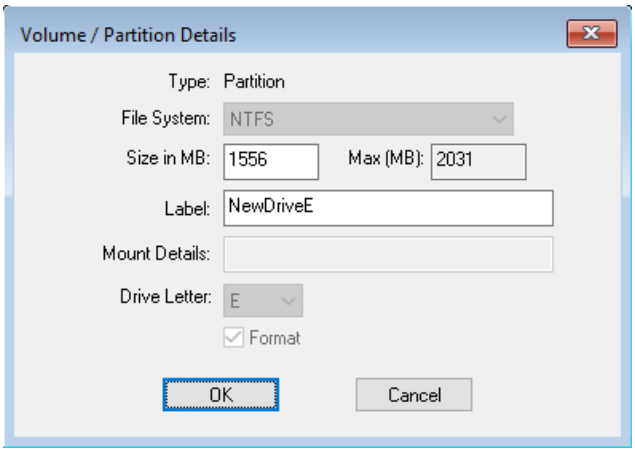
You may also right-click on a partition to allow you to selectively modify the partition parameters.



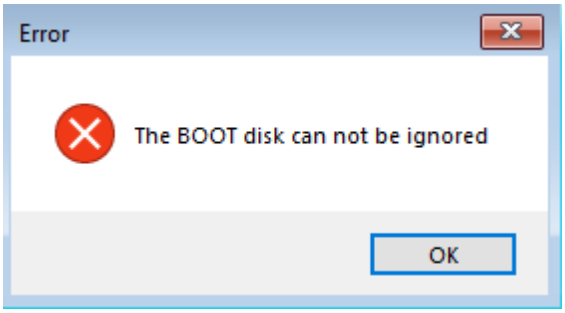
You may **Modify** the following partition parameters:

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

The screenshot below shows an example:



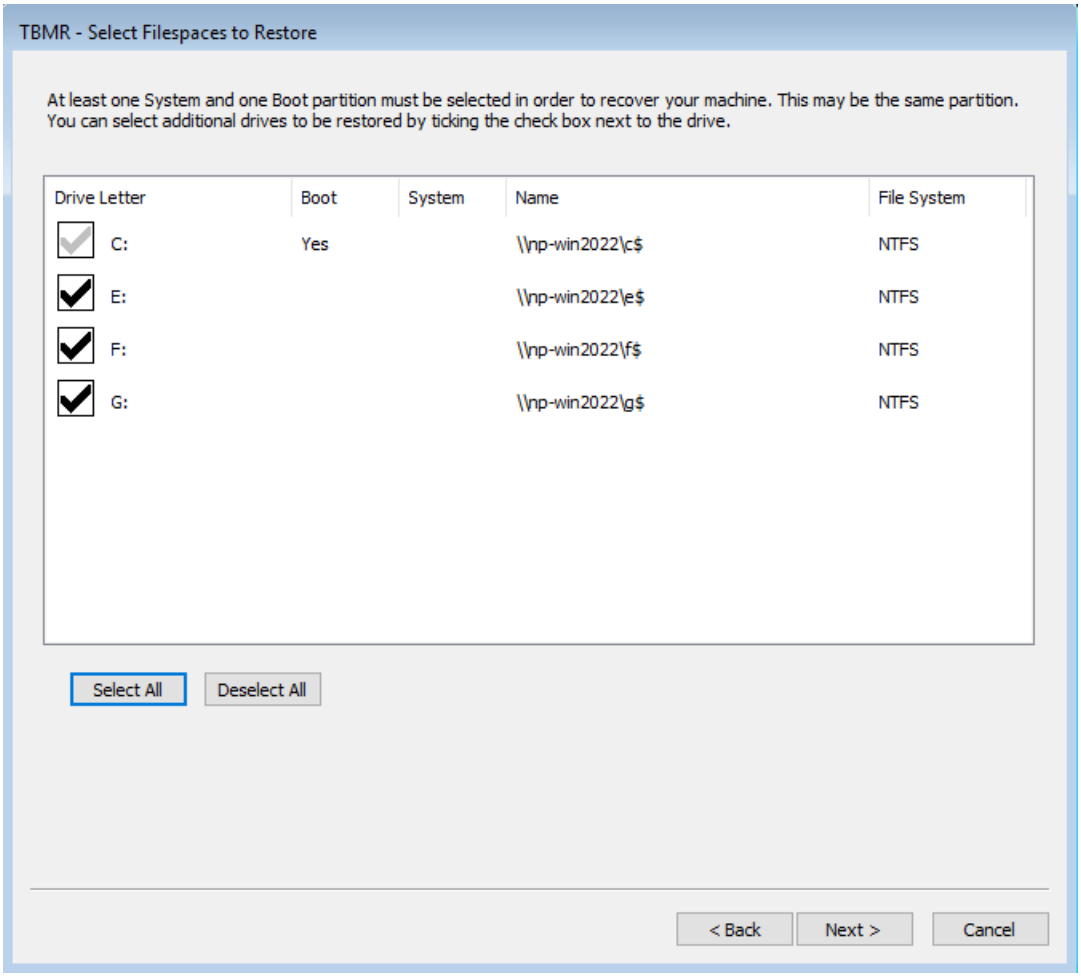
If you attempt to either not format or delete a Windows system partition, an error such as this will be displayed:



At this stage, nothing has happened to the disks. Press Next> to continue with the recovery.

Select Filespaces To Restore

The next step prompts for the filespaces to restore. Generally, each filespace represents a disk partition or volume. Put a tick against each filespace that should be restored or **Select All**:

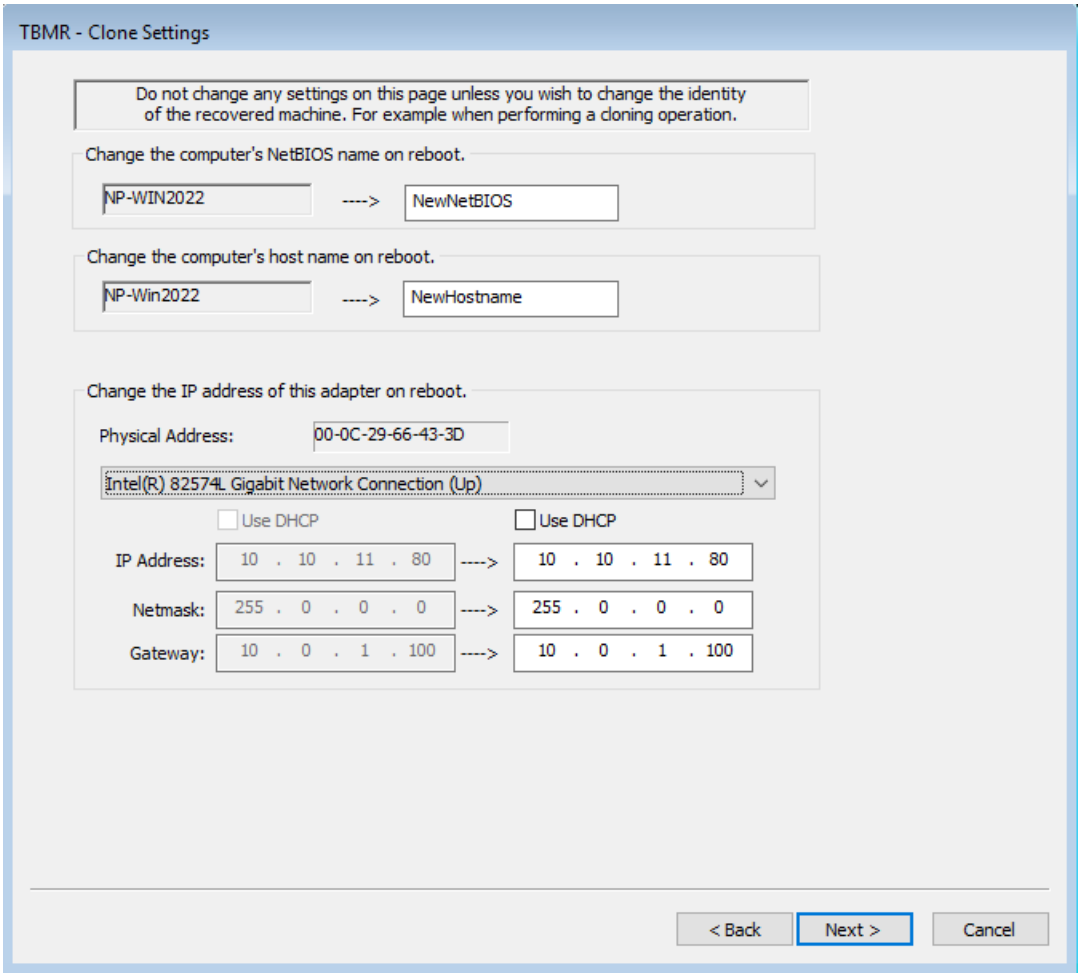


> *Note: the system and boot partitions (even if on different partitions) will always be restored by default.*

Click Next> to continue to the next step.

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.

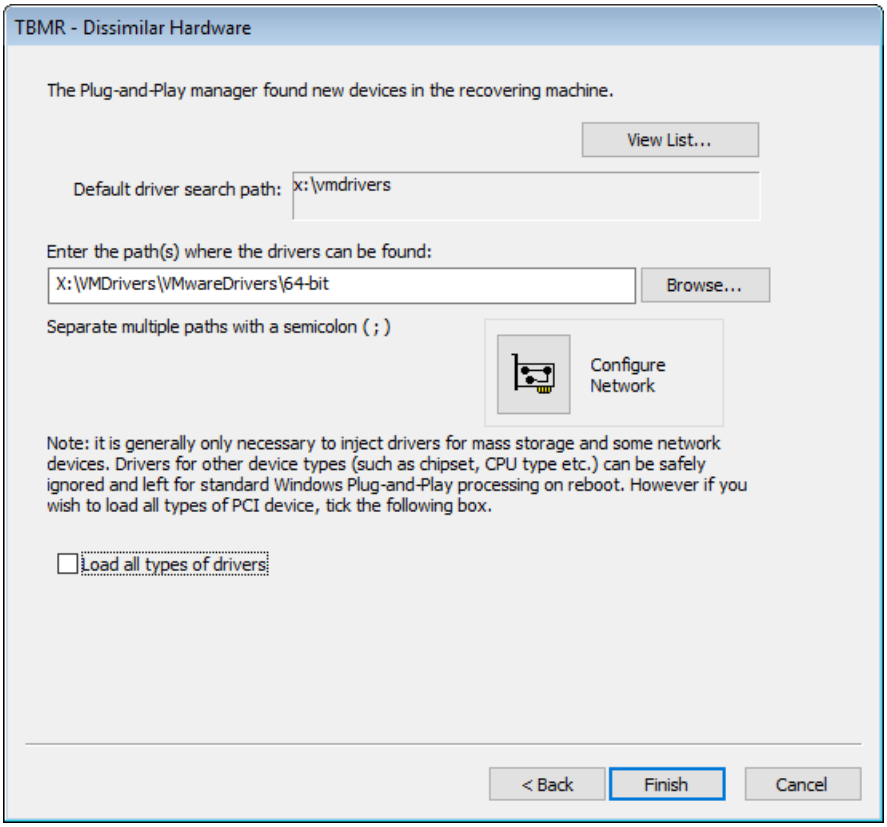
> *Note: When you click on the "Next >" the button will change to "Finish", when you click on "Finish" the restore will start. If dissimilar hardware is detected, then when you click on "Next>" the Dissimilar Hardware dialogue will be displayed instead. Click "Finish" on that dialogue to start the restore.*

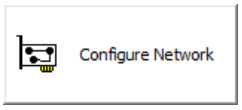
When recovering to a system with a different MAC address (generally during a dissimilar DR), the default IP address settings default to DHCP and not the original IP.

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

Dissimilar Hardware

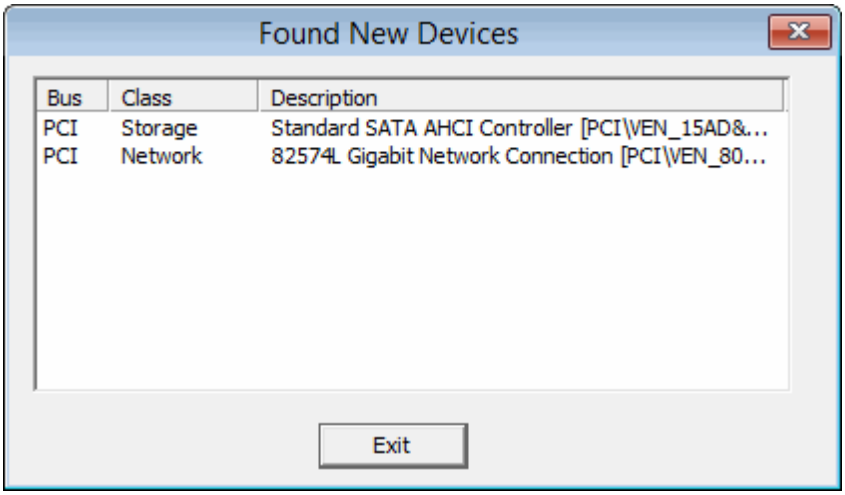
Next, the DR process performs a check to determine if there are new devices in the recovering machine that were not present in the original system. If this is true, then this is a 'dissimilar' DR and the following dialogue will be shown to allow the user to specify the location of the new driver files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

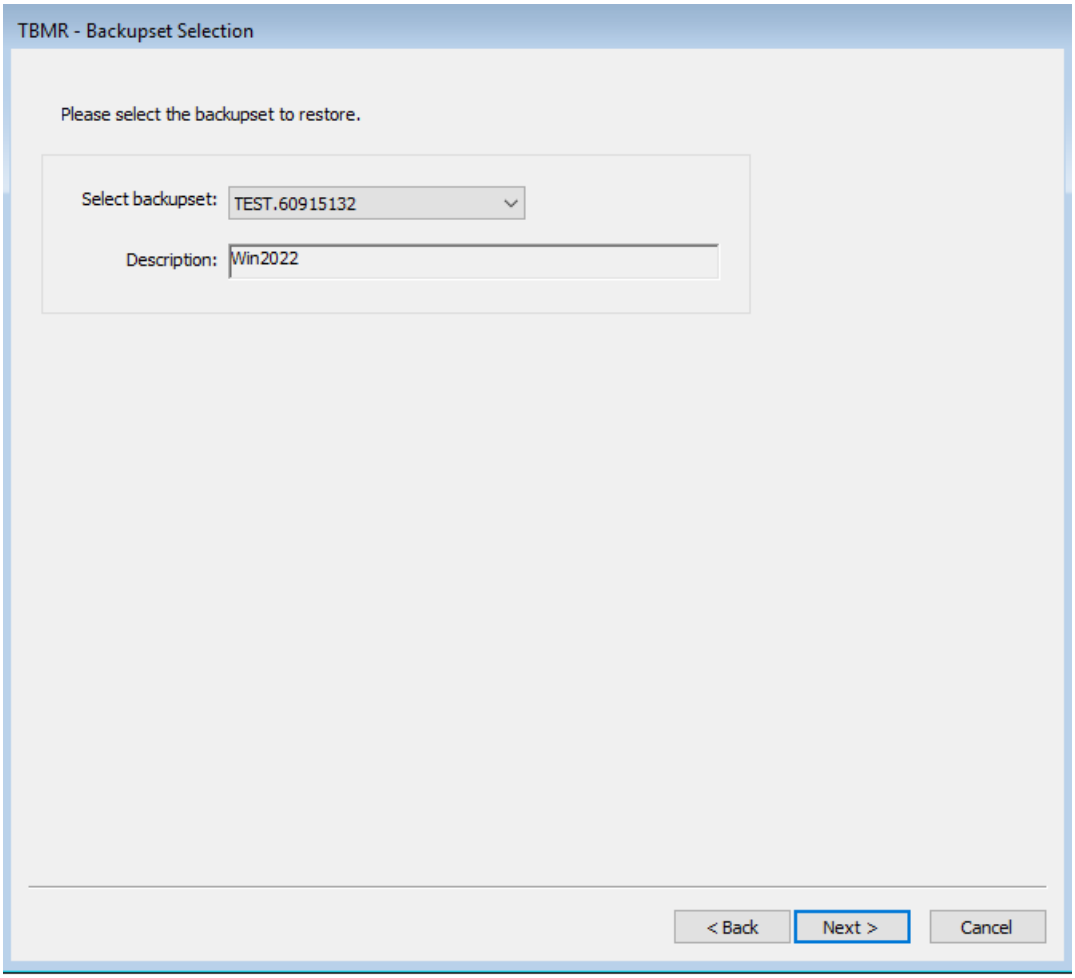
Note that if drivers are not found for the new boot disk then, although WinPE5, WinPE10 or WinPE11 will be able to recover the files to the disk, there is a good chance that it will not boot correctly.

Press Finish> to proceed with the recovery.

Restore from Backupset

The **Restore from a Backupset** process is identical to Restore from a Node.

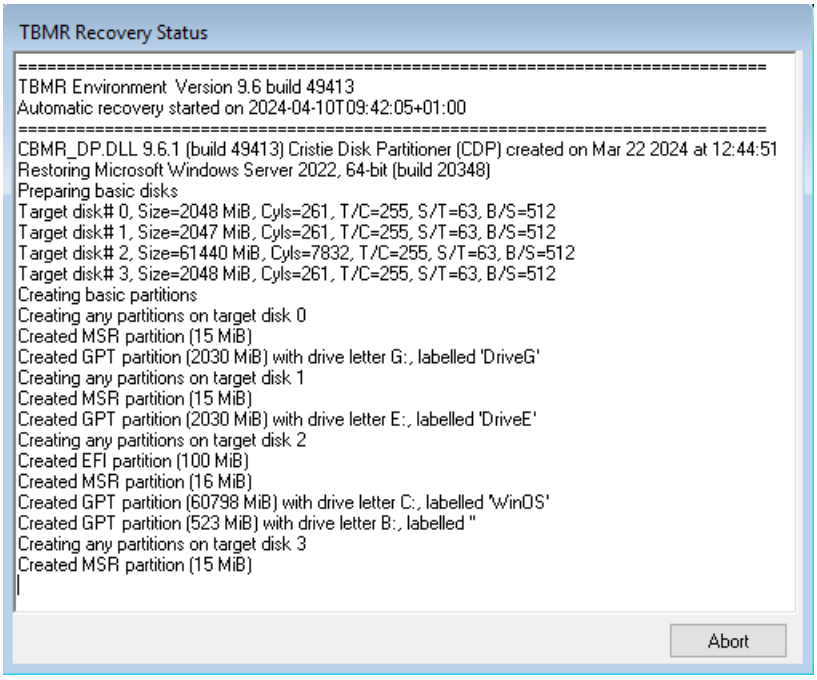
However, if the backupset Node specified contains multiple backupsets then an additional dialogue will be shown allowing the required backupset to be selected from a drop-down list:



The rest of the restore sequence runs as described in the section Restore from Node.

Disk Recovery Sequence

The **Recovery Sequence** begins by preparing the disks selected for the recovery.

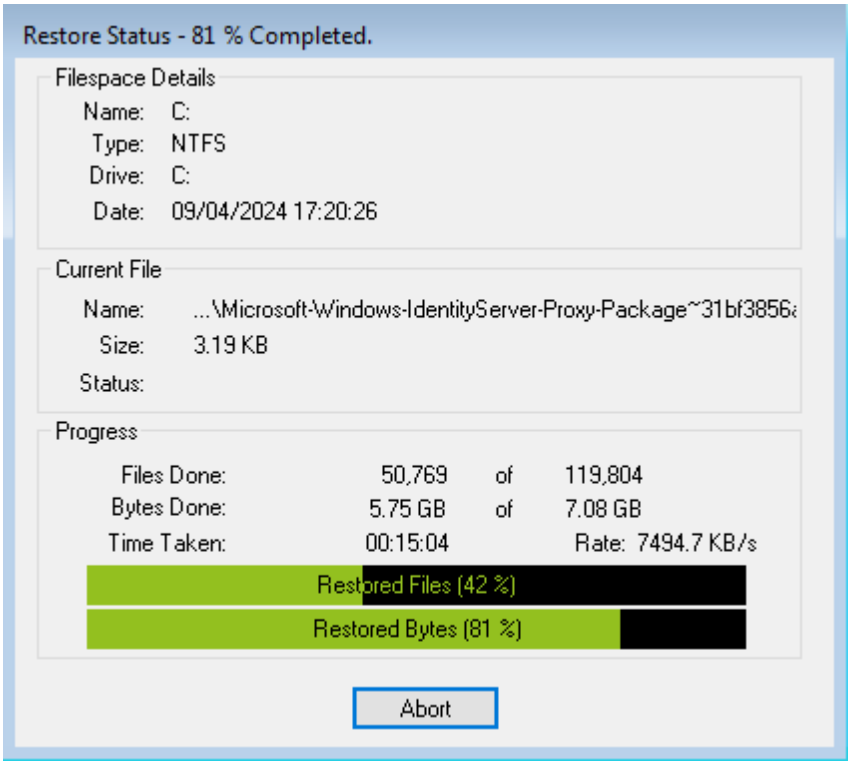


This involves:

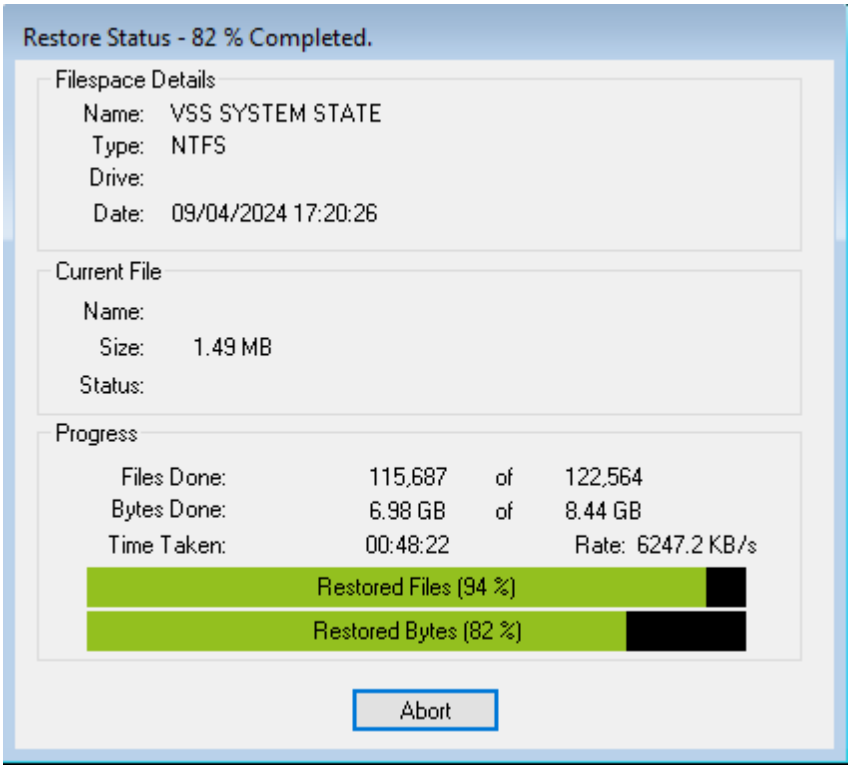
- *disk mapping original layout to new*
- *cleaning (removing any existing disk partitions)*
- *removing any existing dynamic volume databases*
- *re-creating the partitions*
- *converting to dynamic volumes if required*
- *formatting to the required partition type*
- *create partition/volume mount points*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

The next step is to recover the filespaces 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 first stage of the recovery is to make a count of the number of files to restore so that progress can be accurately reported. Next the file recovery stage is divided into different phases: first the recovery of each selected **volume filespace**,



followed by **SystemState** (after a file count):

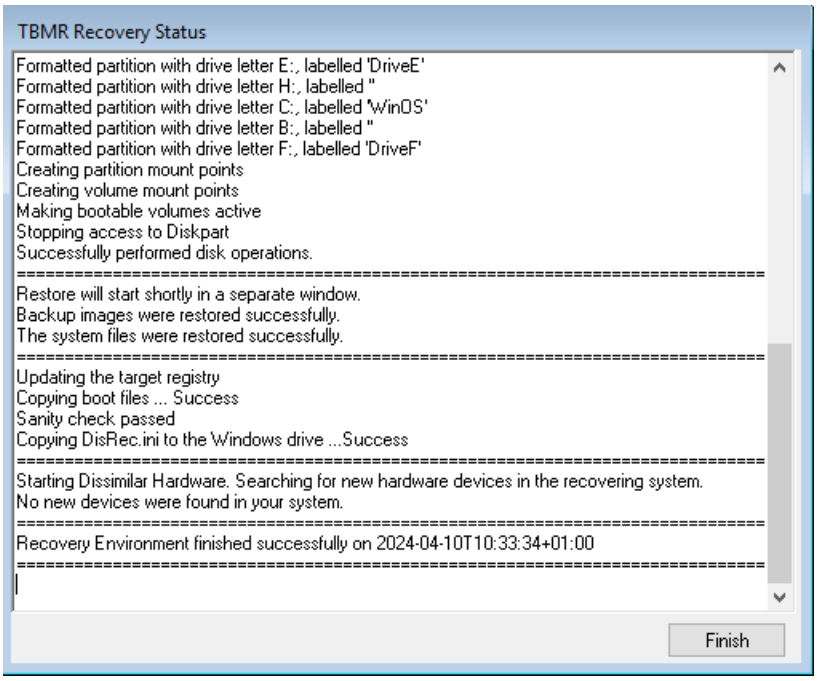


This process may take some time if the backups are large. You may select the Abort button to terminate the file recovery process early, but this may leave a disk or partition in an unpredictable state, which may render it unusable.

If any errors occur during the recovery, an error message will be shown in the 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

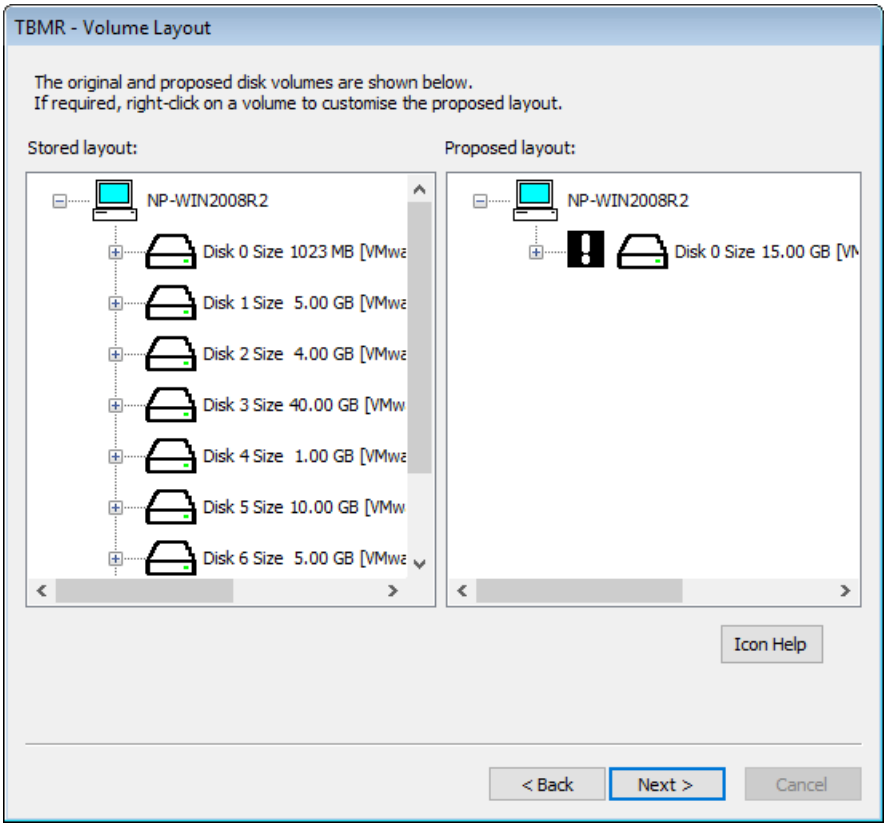


Finally, press Finish to return to the **Recovery Environment** main menu. At this point, you may want to view the recovery logs and perhaps copy the logs to a local device or remote share before selecting to reboot. If you have configured the logfile save path from the first step the logfiles will be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

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

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.

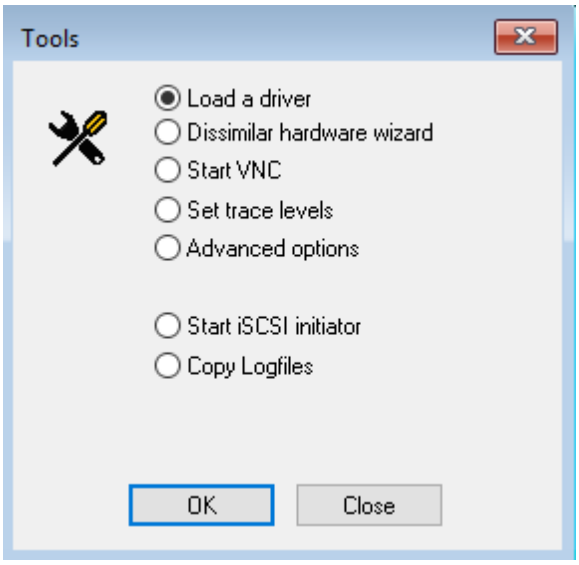
In this scenario, TBMR will select as many disks to recover as possible (in this case only one disk - the boot disk). In addition, it will scale the partitions down in proportion to their original size and occupancy. This can be complicated by having, say, mirrored dynamic volumes when the mirror will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

6.2.3 Tools

There are a number of tools that can assist with the recovery process. They are all collected under this command button:



The options available are:

- *Load a driver*
- *Dissimilar Hardware Wizard*
- *Start VNC*
- *Set trace levels*
- *Advanced options*
- *Start iSCSI initiator*
- *Copy Logfiles*

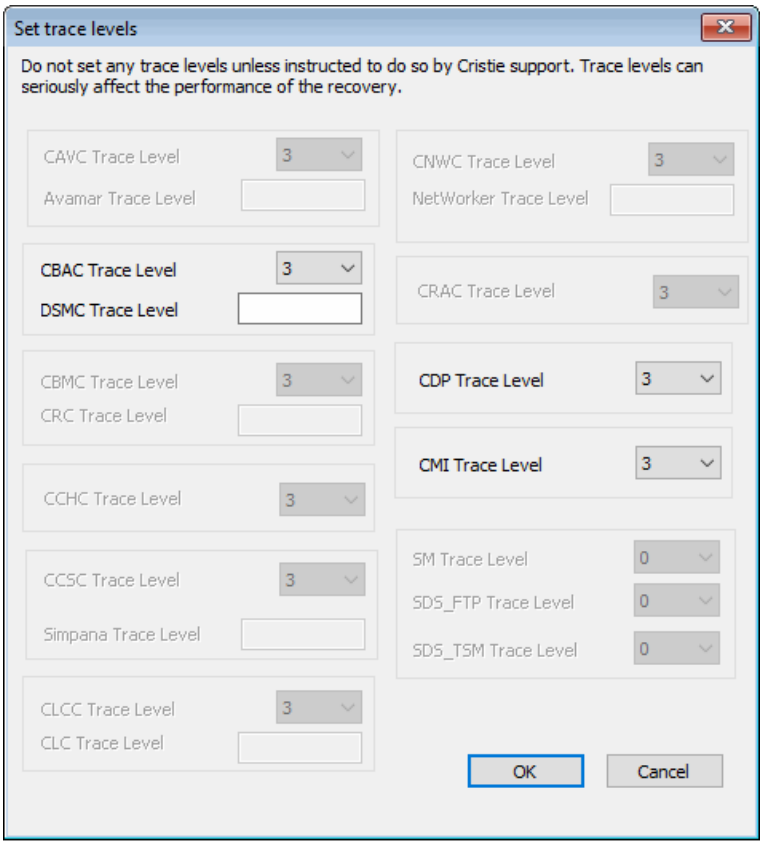
Load a driver allows a new mass storage or NIC driver to be injected into the running booted WinPE5, WinPE10 or WinPE11 DR environment. This would be used, for example, to support a mass-storage (disk) device not currently supported out-of-box. This should be done prior to starting the DR sequence.

The **Dissimilar Hardware Wizard** will allow drivers to be injected into the recovered system when the target hardware has different devices from the original (eg. RAID controllers). Normally, this will be done automatically as part of the DR sequence and will not need to be run manually.

Start VNC will run a VNC server within the WinPE5, WinPE10 or WinPE11 environment, allowing external VNC clients to remotely connect during the DR session. The start process will provide you with the current IP address of the WinPE5, WinPE10 or WinPE11 environment, which you will need to specify in the VNC client.

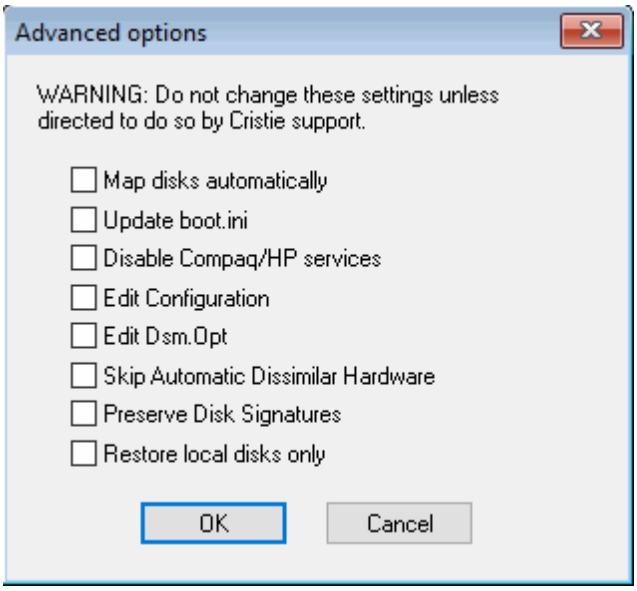
> ***Note: the VNC connection is also password protected. The VNC feature is intended for diagnosing DR problems under the guidance of Cristie Support, who will provide the password upon request.***

Set trace levels allows the DR log file trace to be increased or decreased as required:



It is recommended that the trace levels are only changed when advised to do so by Cristie Support staff. This is because they could have a severe impact upon the performance of the backup restore process.

Advanced Options should only be selected when advised to do so by Cristie Support staff.



Start iSCSI initiator - please contact Cristie Support if you wish to use this feature.

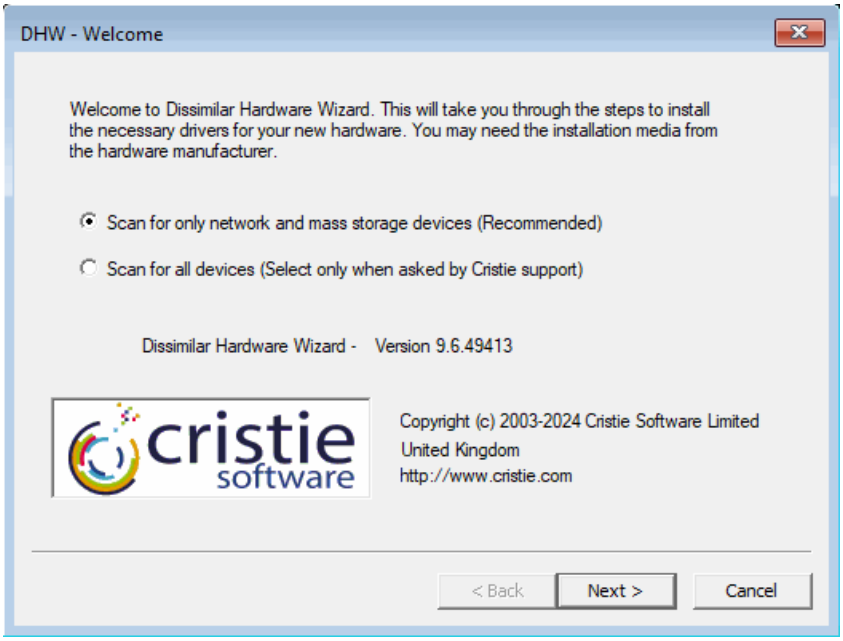
Copy Logfiles allows all the current logfiles created as part of the recovery process to be zipped up and copied to a network share or local device (such as a USB flash drive).

6.2.3.1 Dissimilar Hardware Wizard

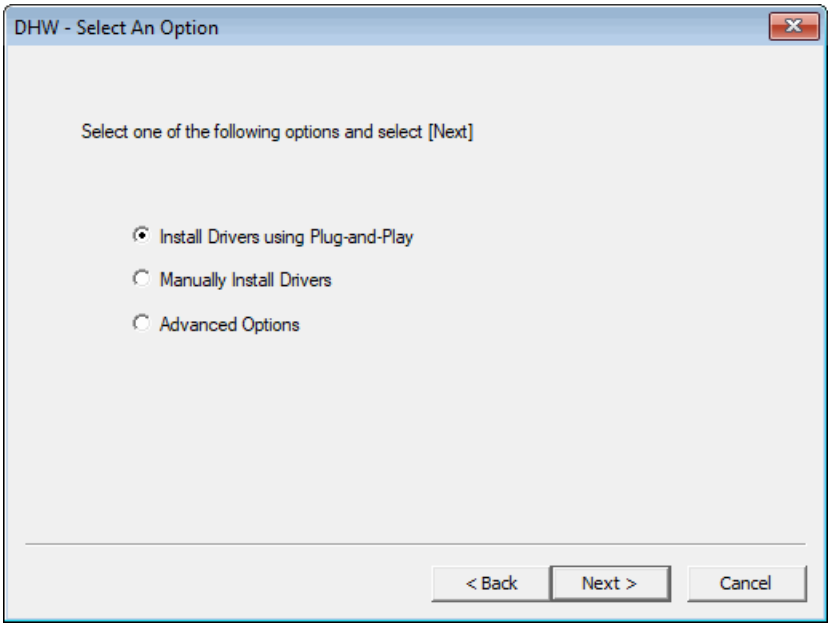
A restore to dissimilar hardware is normally detected during the Automatic or Manual DR sequence. Drivers will be injected automatically at the end of the restore sequence if a source location has been provided. However, if this process has failed for some reason, or additional drivers are required to be injected into the recovering machine, then this **Dissimilar Hardware Wizard** (DHW) tool is provided.

> ***Note: it is only necessary to load the drivers for the hard disk, NIC and, rarely, the HAL. Drivers for the hard disks and NIC can be determined by Plug-and-Play (PnP) and may be readily identified. However, changes required in the CPU model via a change in HAL cannot yet be determined by PnP - these need to be loaded manually.***

If you wish to scan for just Mass Storage and Network devices (the minimum required to boot a dissimilar system), select Next> to continue to the next step of the Wizard. This is the recommended option. Under the guidance of **Cristie Support**, you may be asked to scan for all devices. In this case, tick the **'Scan for all devices'** box before selecting Next>.

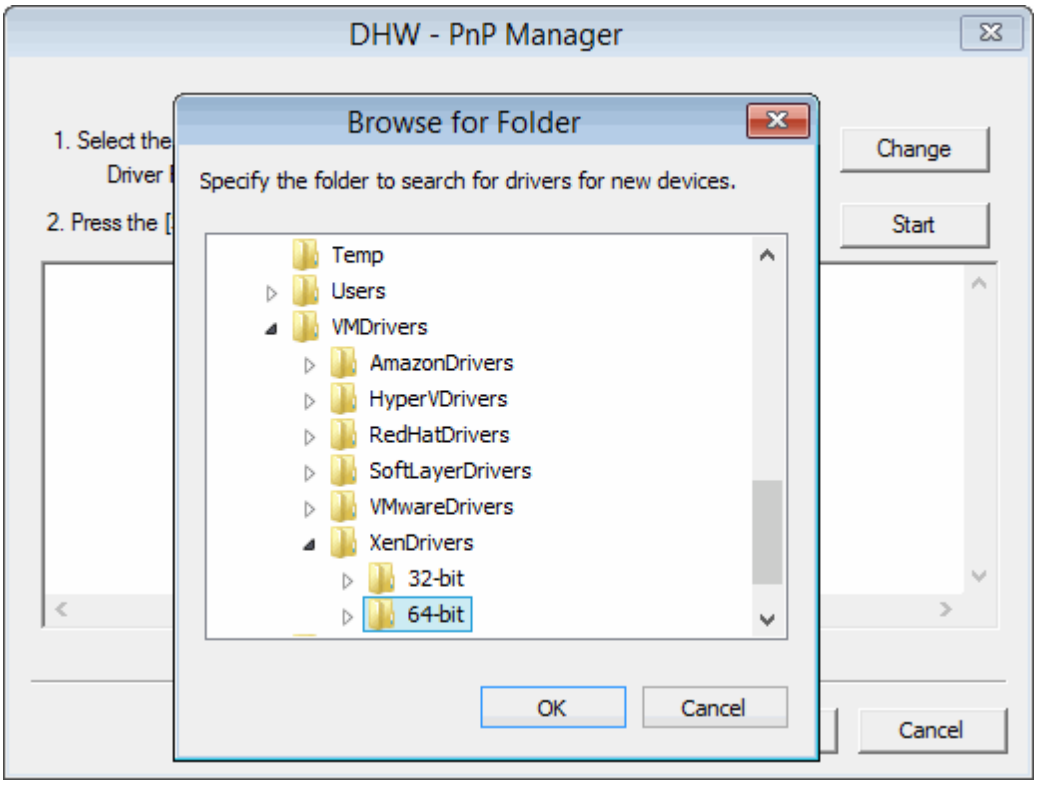


Select the **'Install Drivers using Plug-and-Play'** option:

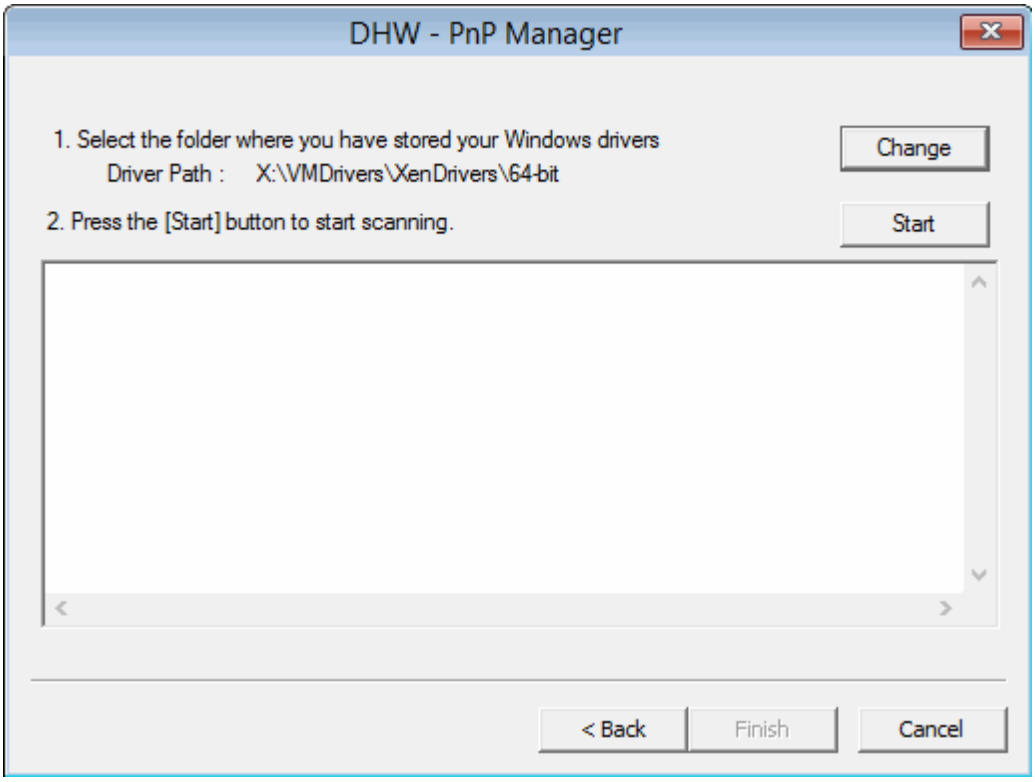


Install Drivers using Plug-and-Play

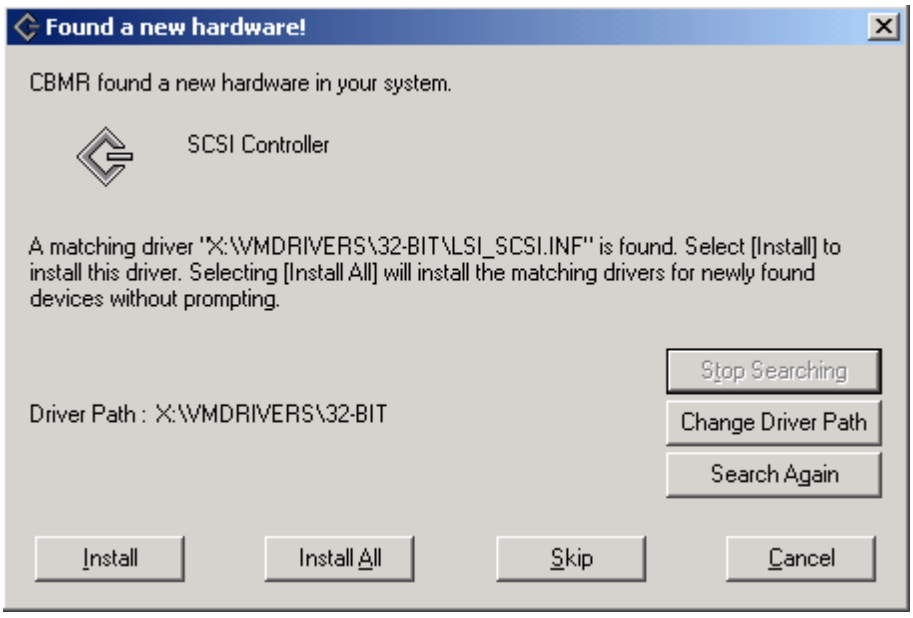
The window appears empty to start with. The set of drivers located on the recovery CD is the default choice, but in practice they should not be used. Instead, change the driver search path to where you have actually located your drivers (for example, to a network share or another CD) with the **Change** command button.



In the example above, the driver search path is changed to the VMware drivers on the WinPE boot CD. Begin the PnP driver detection by clicking Start.



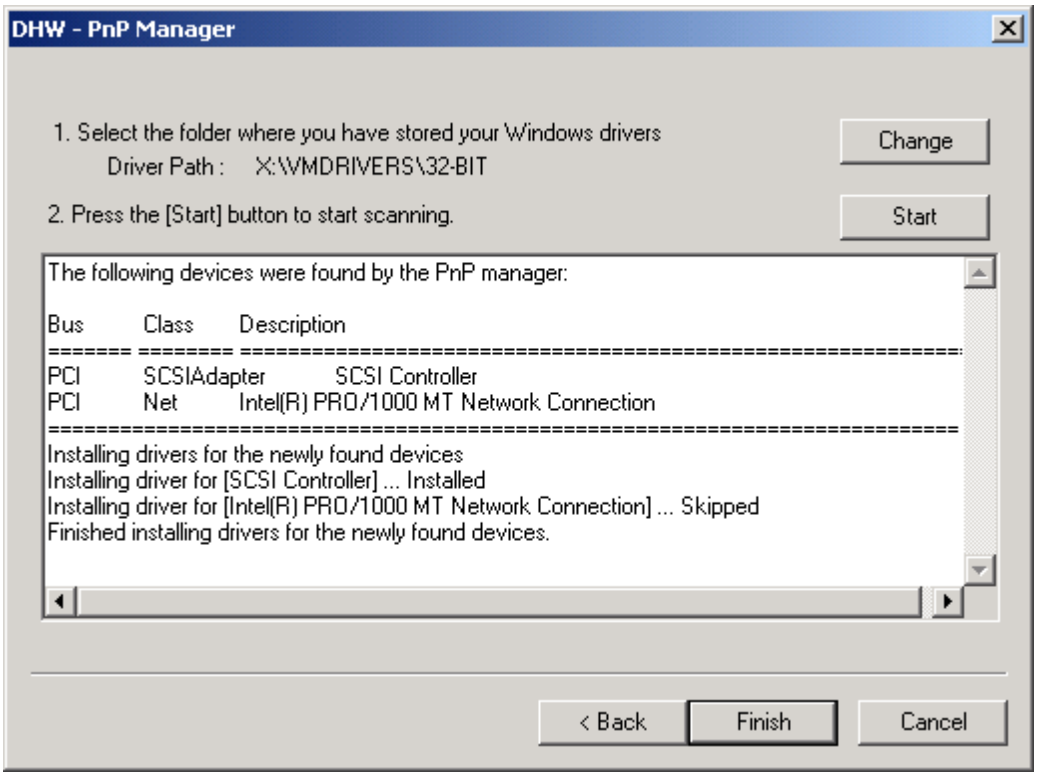
The process checks the devices that it can detect and when it finds one that does not have a driver loaded, it will offer to install it. The example below shows an LSI SCSI device being detected:



If you are satisfied that the found driver path is correct, click on Install and the driver will be installed. The device scan will continue and may find, for example, other mass storage or network devices. Follow the steps above to install.

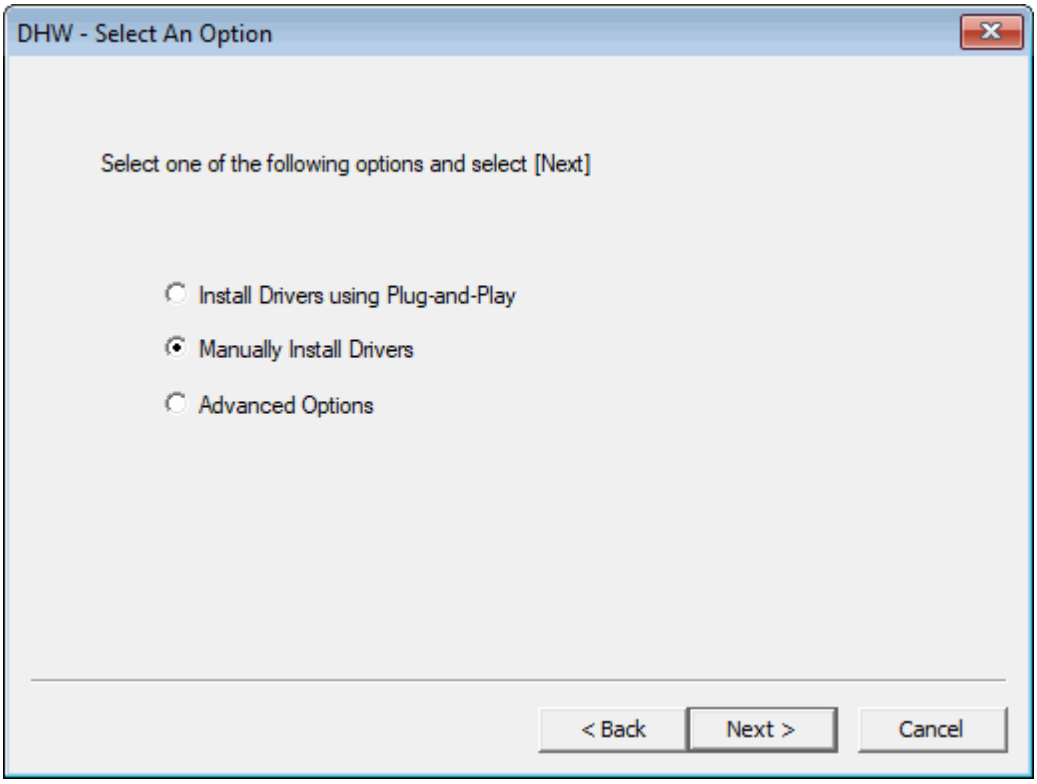
Drivers are usually .sys files. The .inf files define which driver files need to be loaded for a given device. You may need to confirm the location of the driver files for each device, or possibly find the path where they are stored. When you have the correct path, click on OK and the Wizard will look for more.

Once all of the drivers of the detected devices have been processed, the Wizard will indicate that the installation has finished. Click on Finish to proceed.

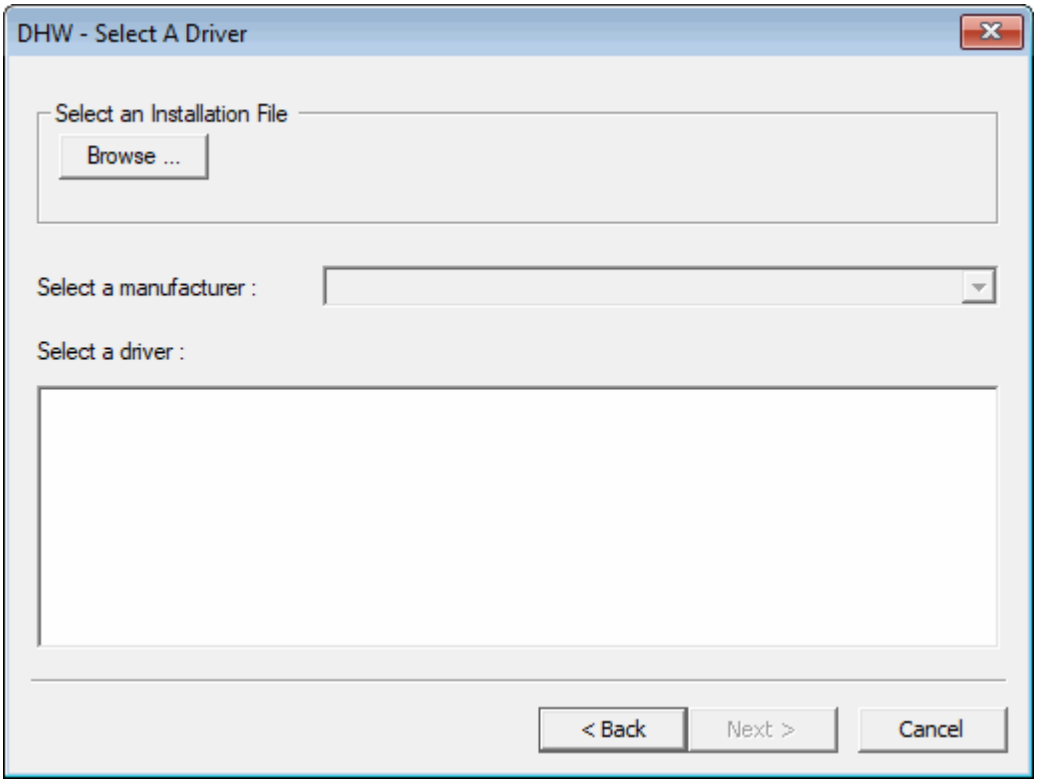


Manual Installation

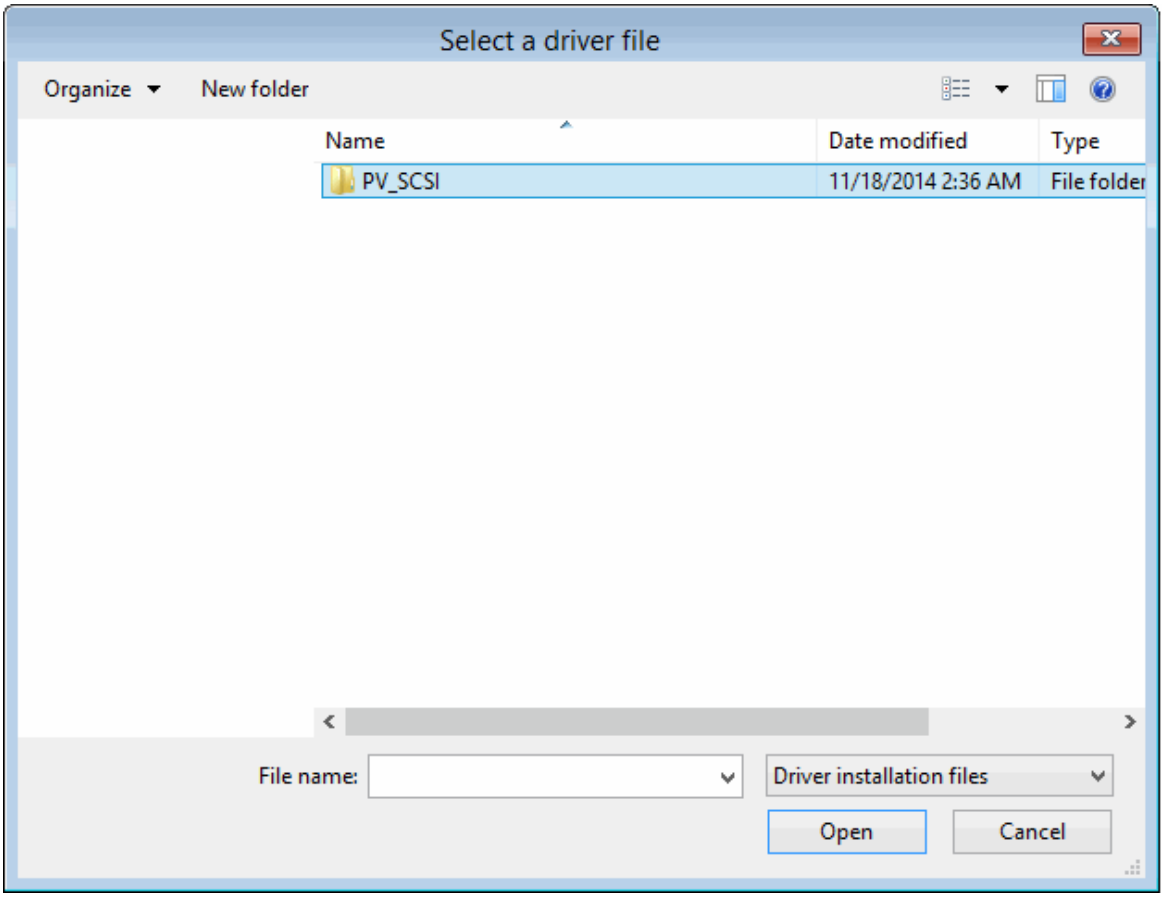
Typically, you would only manually install a driver for a CPU/HAL change. Select **'Manually Install Drivers'** from the option menu:



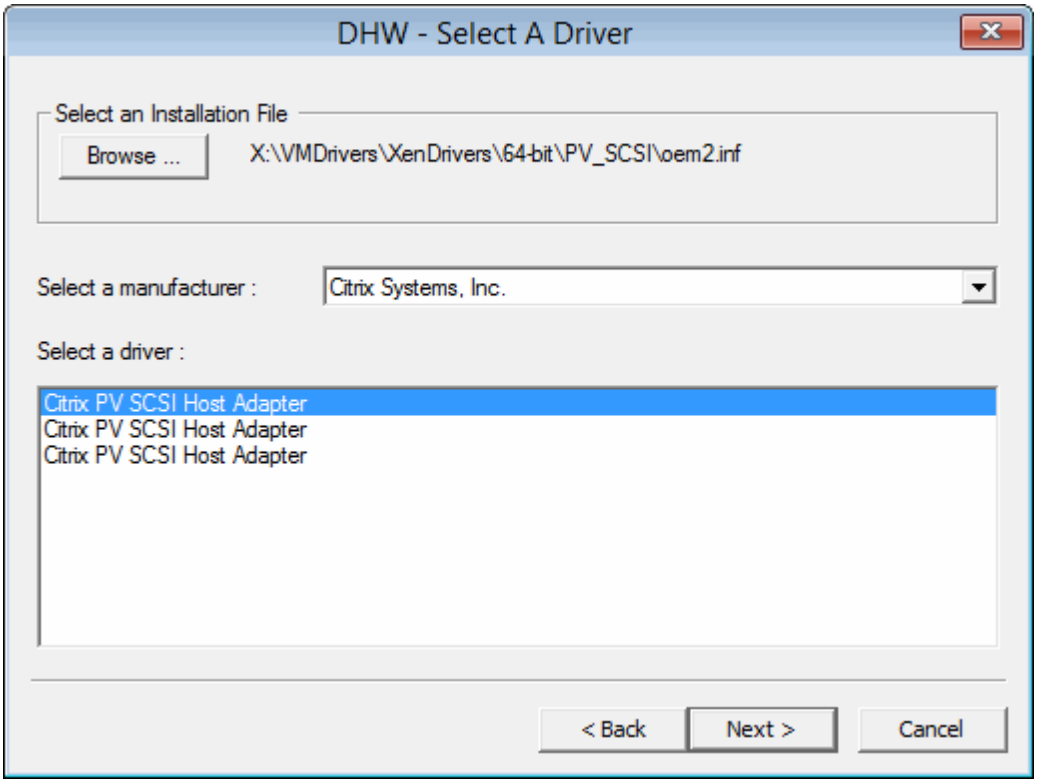
Then select Next>.



Select Browse... to locate the driver or HAL file you need by browsing to the appropriate folder that holds the .inf file. If you need to load the driver from another machine, then you can browse to a share on that machine and then to the appropriate folder.

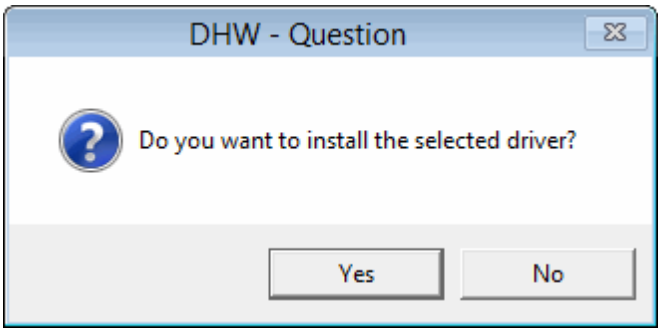


Here we are selecting the Citrix PV SCSI controller driver:



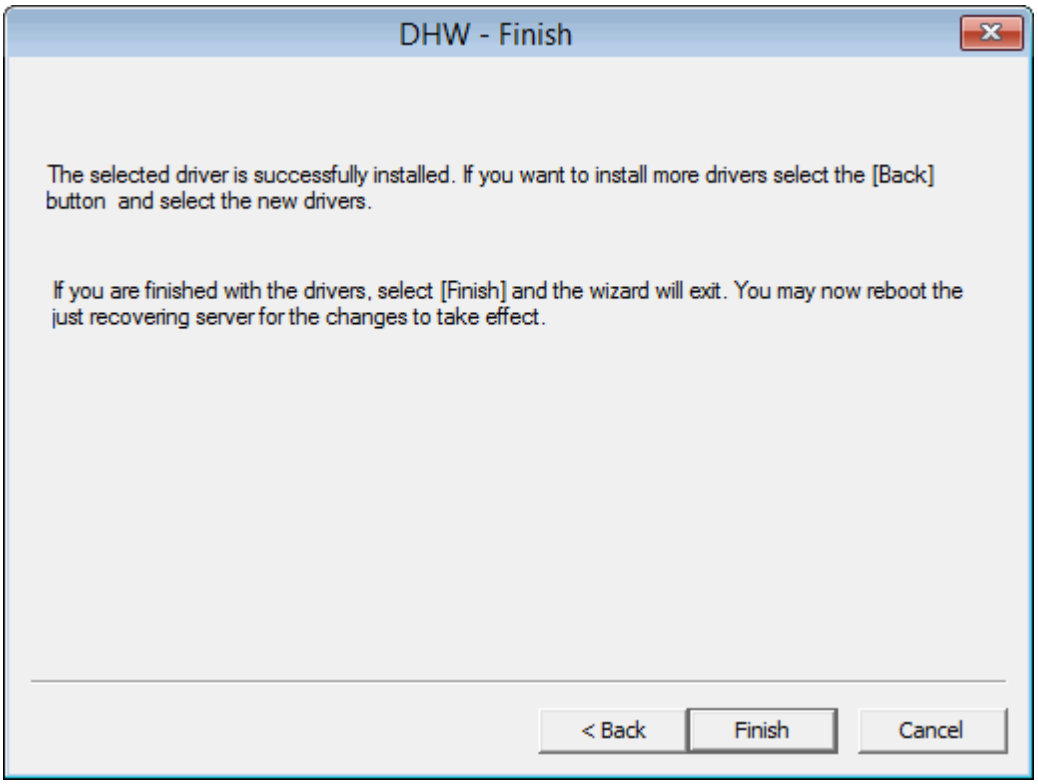
The Wizard allows you to select drivers that are grouped by manufacturer. Select the

actual driver that you wish to install and click Next>.



After you confirm the selection, the Wizard determines which files need to be installed. You are given the opportunity to change the location from which they are loaded if required..

When the drivers have been installed, the Wizard allows you to go back to install another device driver or Finish the process.

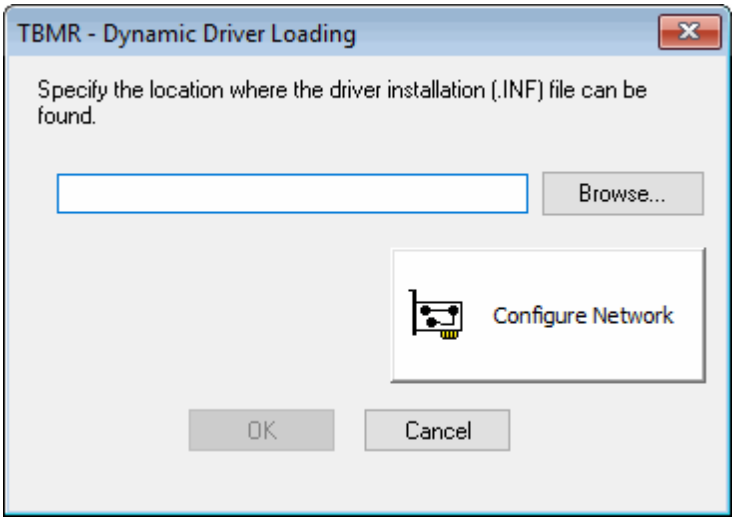


6.2.3.2 Load a Driver

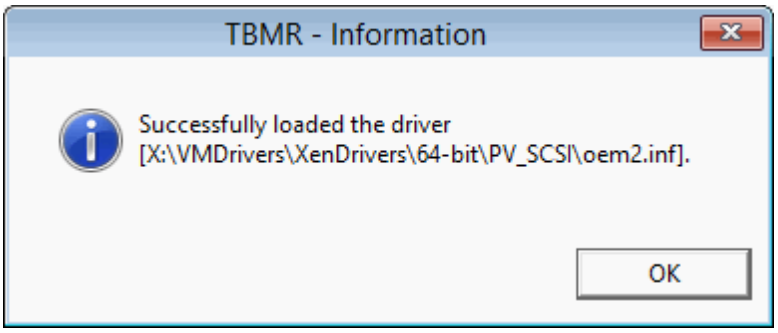
This option allows a new **Mass Storage** or **Network Interface card** driver to be loaded into the WinPE5, WinPE10 or WinPE11 environment. Use this when WinPE5, WinPE10 or WinPE11 does not have a built-in driver for your hardware.

For example, if the DR environment does not show any disks to be recovered, you can inject a new mass storage device driver for the device and retry the DR Wizard.

You will be prompted for the location of the driver INF file. Use the Configure Network button to map a network share if necessary:



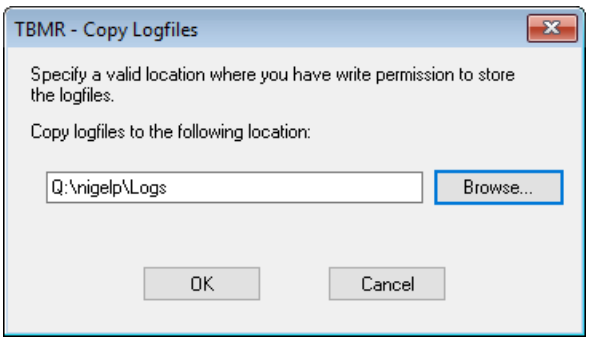
The INF file and other associated driver files (such as the .SYS file) can be located on a CD, USB device or a network share. The following confirmation dialogue is displayed if the driver is loaded successfully:



6.2.3.3 Copy log files to removable media or network location

Since all log and error files generated during the recovery are only transitory (ie. they are lost as soon as the Windows WinPE5, WinPE10 or WinPE11 environment exits), this option allows you to copy the files to a local device or remote network share for permanent record before booting the recovered system.

Use the **Cristie Network Configurator** utility to setup a network share first. All the files are compressed into a single ZIP file so that they can be easily sent to Cristie Support when required.

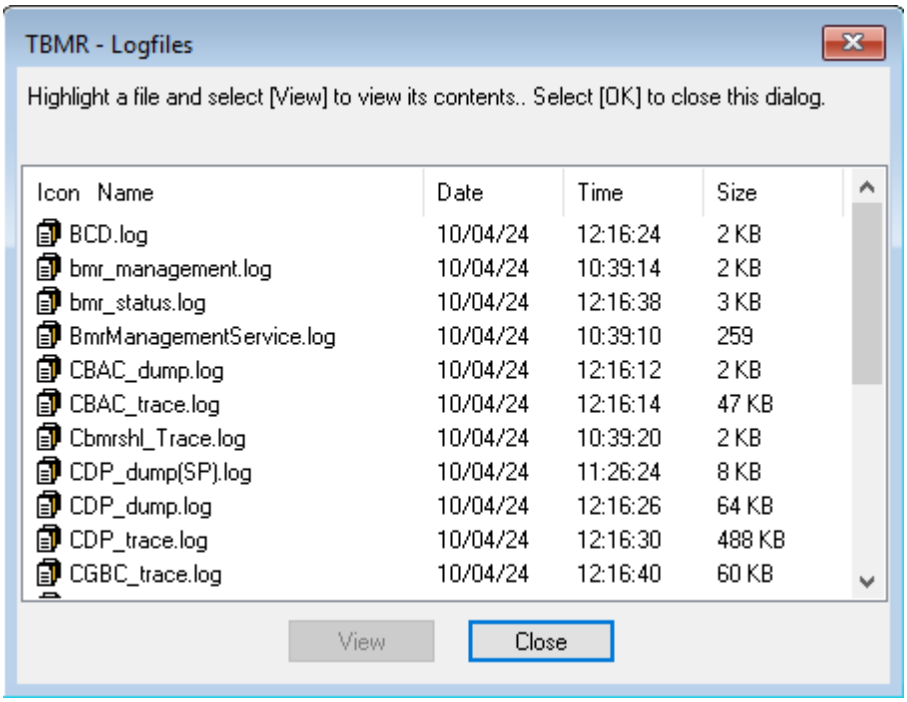


The example shows files being copied to a network share **Q:\nigelp\LOGs**.

Note: the logs are automatically written back to the recovered system after a successful recovery. They are saved to the TBMR installation sub-folder 'Temp'.

6.2.4 View Logs

This main menu option allows the log files produced during the recovery to be viewed using Notepad. Normally, viewing this information is only required to diagnose a problem with the recovery.



The important files are (this is not an exhaustive list):

bmr_management.log - remote VA management log, Used by Cristie Support.
bmr_status.log - restored disk and registry configuration log, eg. disks/partitions created summary etc.
BmrManagementService.log - remote VA management log, Used by Cristie Support.
cbac_dump.log - contains a summary of the TSM client/server versions and node details.
cbac_trace.log - contains a detailed summary of the TSM client/server communications. Used by Cristie Support for diagnosing TSM interface problems.
cbmrshl_trace.log - contains a summary of the main menu shell operations. Used by Cristie Support for diagnosing shell operations.
cdp_dump.log - contains general information regarding the system BIOS, disk configuration and timezone details of the original and target system.
cdp_trace.log - contains a detailed summary of how the partitions were restored. Used by Cristie Support for diagnosing disk configuration problems.
CGBC_trace.log - Cristie Generic Backup Client log file.
cnm_trace.log - contains network library information. Used by Cristie Support.
crm_trace.log - contains the Recovery Manager log. Used by Cristie Support.**dhw_log.log** - contains a summary of Dissimilar Hardware Wizard activities. Used by Cristie Support for diagnosing new driver problems.
CRMWizard_trace.log - contains the Recovery Manager log. Used by Cristie Support.
dhw_log.log - contains a summary of Dissimilar Hardware Wizard activities. Used by Cristie Support for diagnosing new driver problems.
discovery_main.log - contains a summary of network discovery activities. Used by Cristie

Support for diagnosing network problems.
dsmerror.log - TSM interface log information
network.log - contains NIC hardware summary, current network configuration (eg. IP address, gateway IP address etc) and routing table.
PeNetCfg_trace.log - Configure network tool log.
PeRouteCfg_trace.log - Network Routing tool log.
setupapi.log - contains a summary of the Plug and Play devices detected by WinPE5, WinPE10 or WinPE11 as it boots. Used by Cristie Support for diagnosing WinPE5, WinPE10 or WinPE11 driver problems.
Version.log - Used by Cristie Support to determine version of Cristie TBMR software and DLLs deployed.

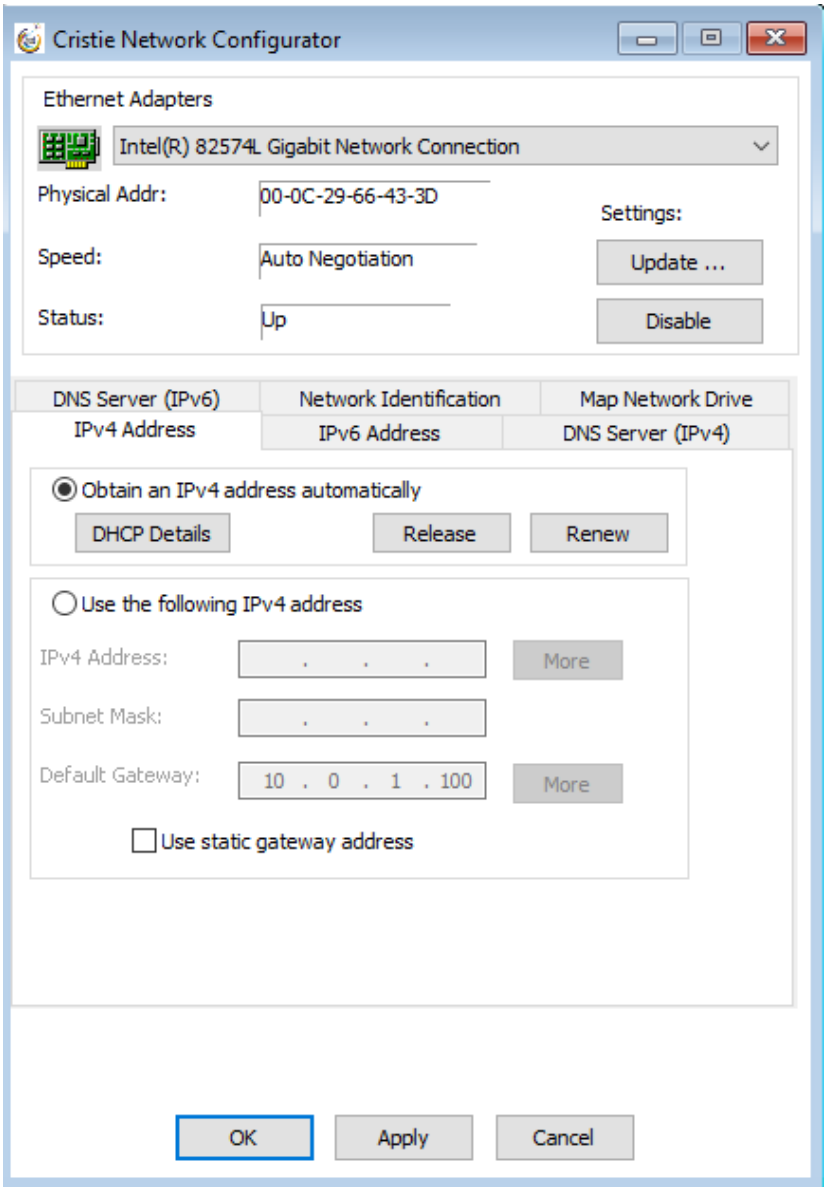
6.2.5 Configure Network

The **Cristie Network Configurator** tool provides extensive facilities to configure the network during the recovery process. It offers the following features:

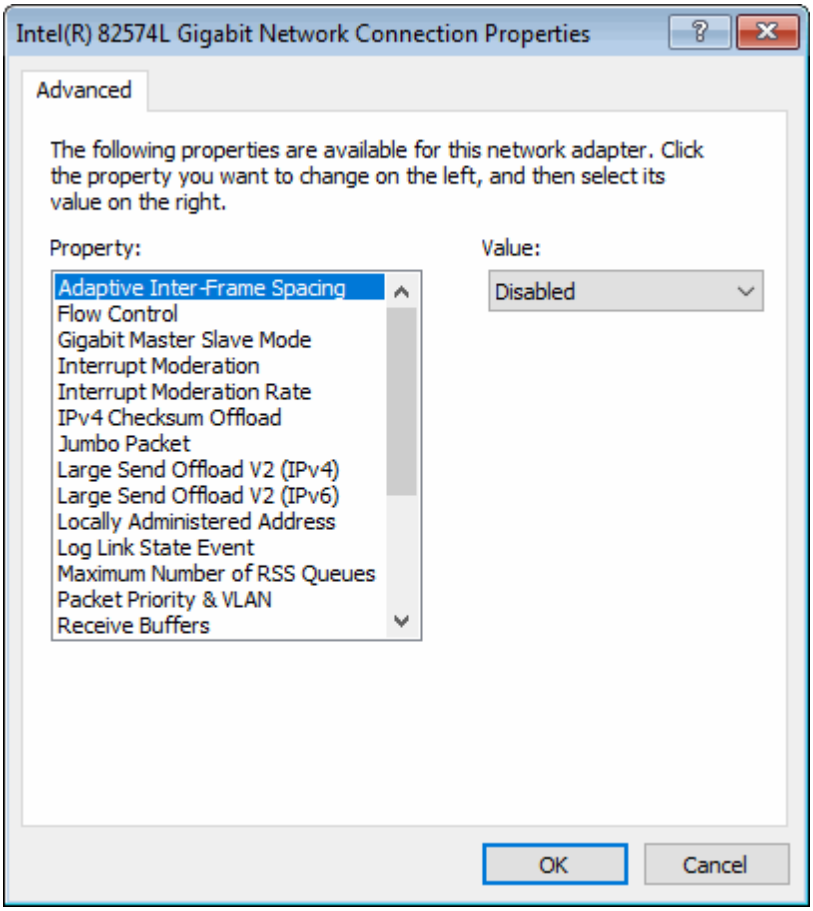
- supports multiple NICs
- configure individual NIC parameters for duplex mode and link speed
- the ability to select DHCP allocated or static IPv4 and IPv6 IP addresses
- the ability to setup DNS server IPv4 and IPv6 IP addresses
- the ability to setup the Network Identification of the recovering system
- allow file shares to be set on the recovering system (using IPv4 and IPv6 IP addresses)
- map/unmap network drives

6.2.5.1 Configure NIC Parameters

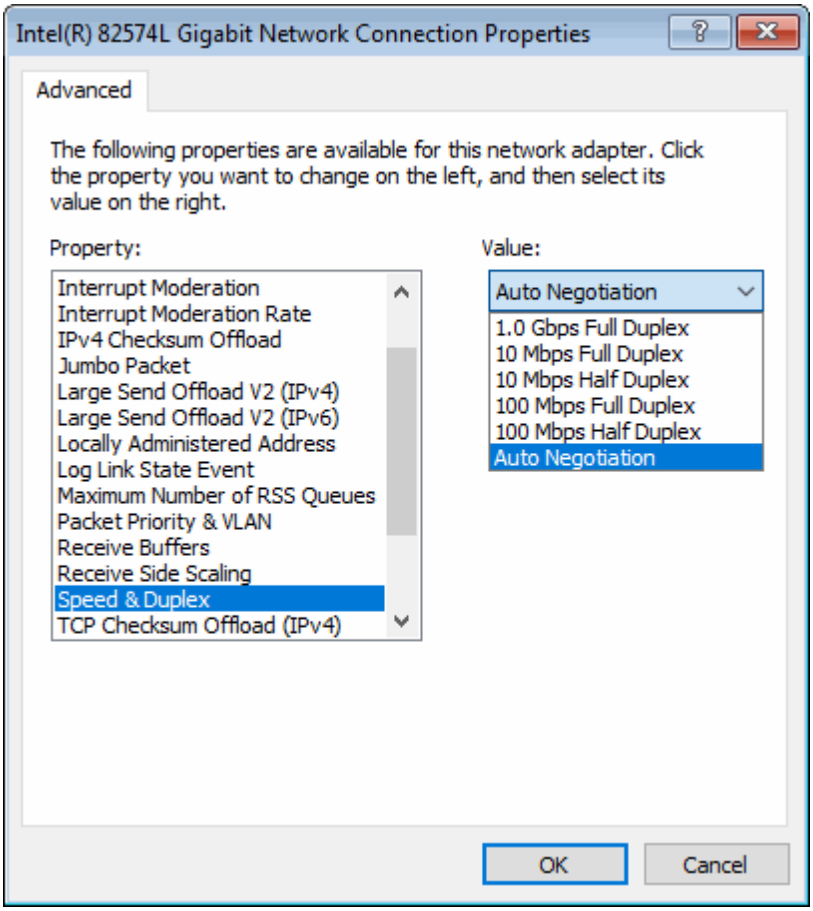
It is possible to change both the link speed and duplex mode for any NIC detected on the recovering target system. Select the desired NIC (there could be more than one) from the drop down box and then select Update....



The resulting display offers numerous NIC properties that can be changed. This property list is dependent upon the NIC - ie. not all properties will be available for all NICs.



To change the NIC speed or duplex setting, select the corresponding Property from the dialogue and then select the required value from the Value drop down box as shown below:



Again, note that the speed/duplex settings available are NIC dependent. Auto Negotiation is generally the NIC default setting. Other NIC properties may be changed as required.

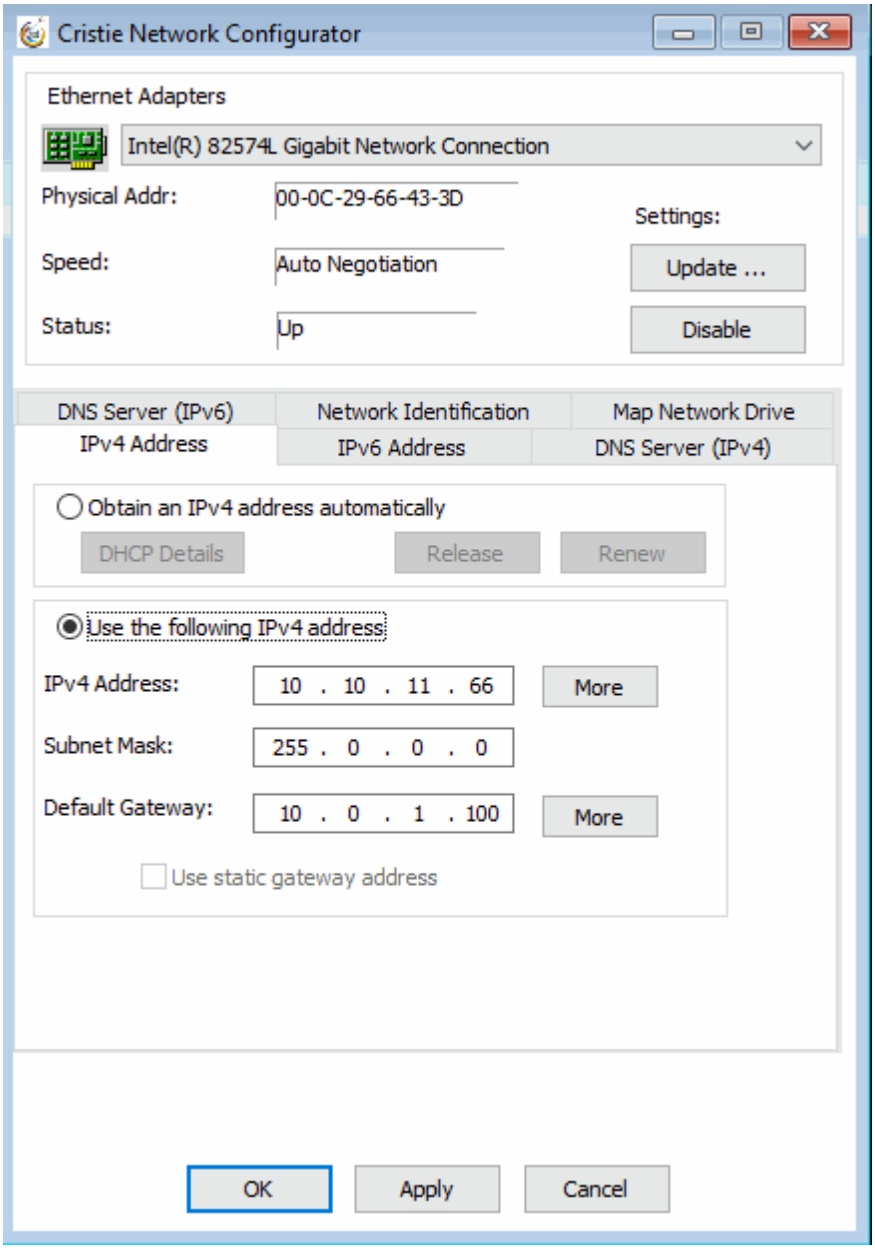
If the NIC is currently connected to the network then the *Status* will be shown as **Operational**. Otherwise the NIC is considered to be **Non-Operational.**

6.2.5.2 Assign Static or DHCP IP Settings

Normally the WinPE5, WinPE10 or WinPE11 DR environment will start with DHCP enabled and active. However, if a static IP is required, use the 'Use the following IP address' option to manually configure.

First ensure the desired network adapter is selected from the drop down list. If a static IP address is to be applied, select the 'Use the following IP address' button. This will automatically deselect the default DHCP option and allow the static IP parameters to be defined.

Different tabs are provided for configuring IPv4 or IPv6 IP addresses.

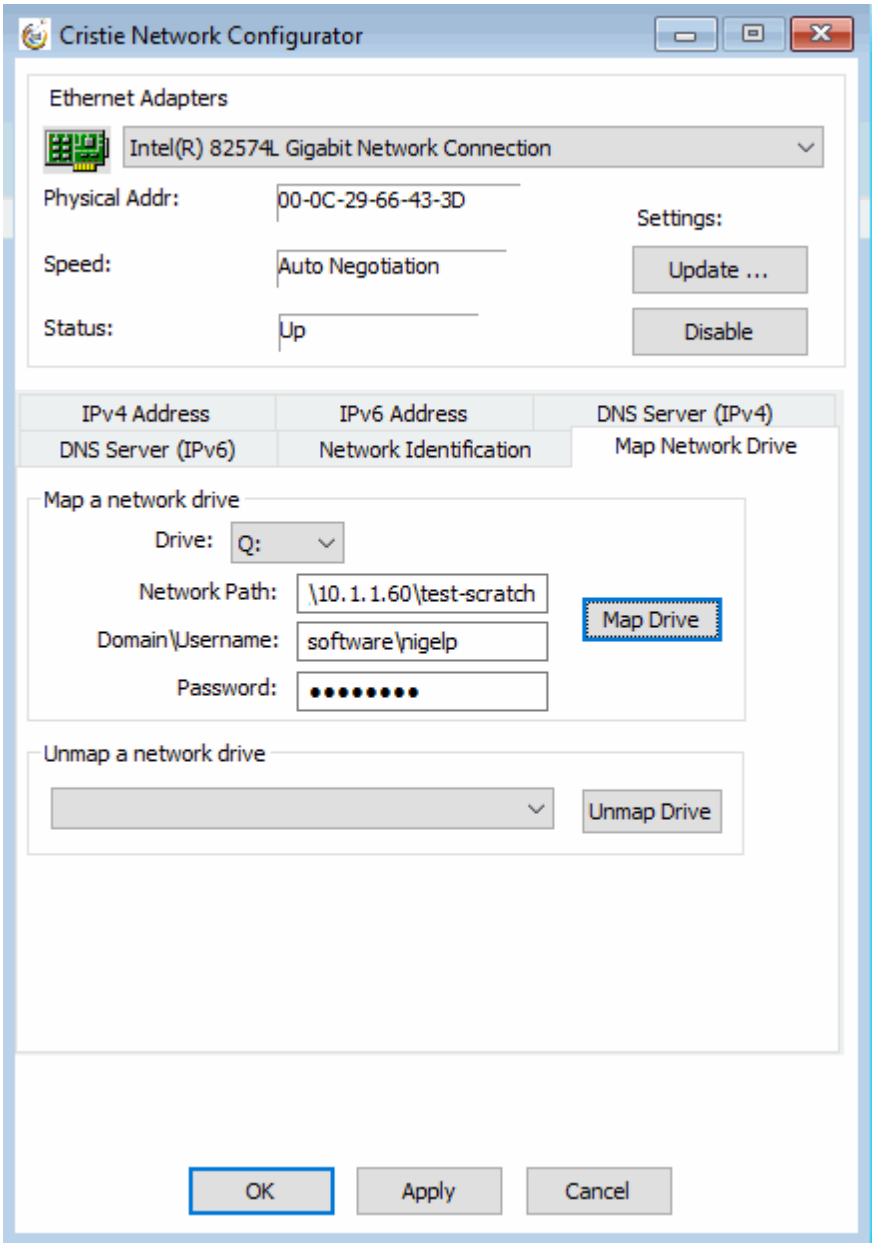


Set the new IP address, subnet mask and gateway IP address. The More button will allow the system to have more than one static IP address. Click on Apply to confirm the settings for the selected adapter.

This feature will also allow the DHCP lease to be released or renewed, as required.

6.2.5.3 Map a Network Drive

In order to simplify access to network resources, the Network Configurator allows you to map a network drive to a network share. Start the Cristie Network Configurator from the **Tools** menu and select the **Map Network Drive** tab.



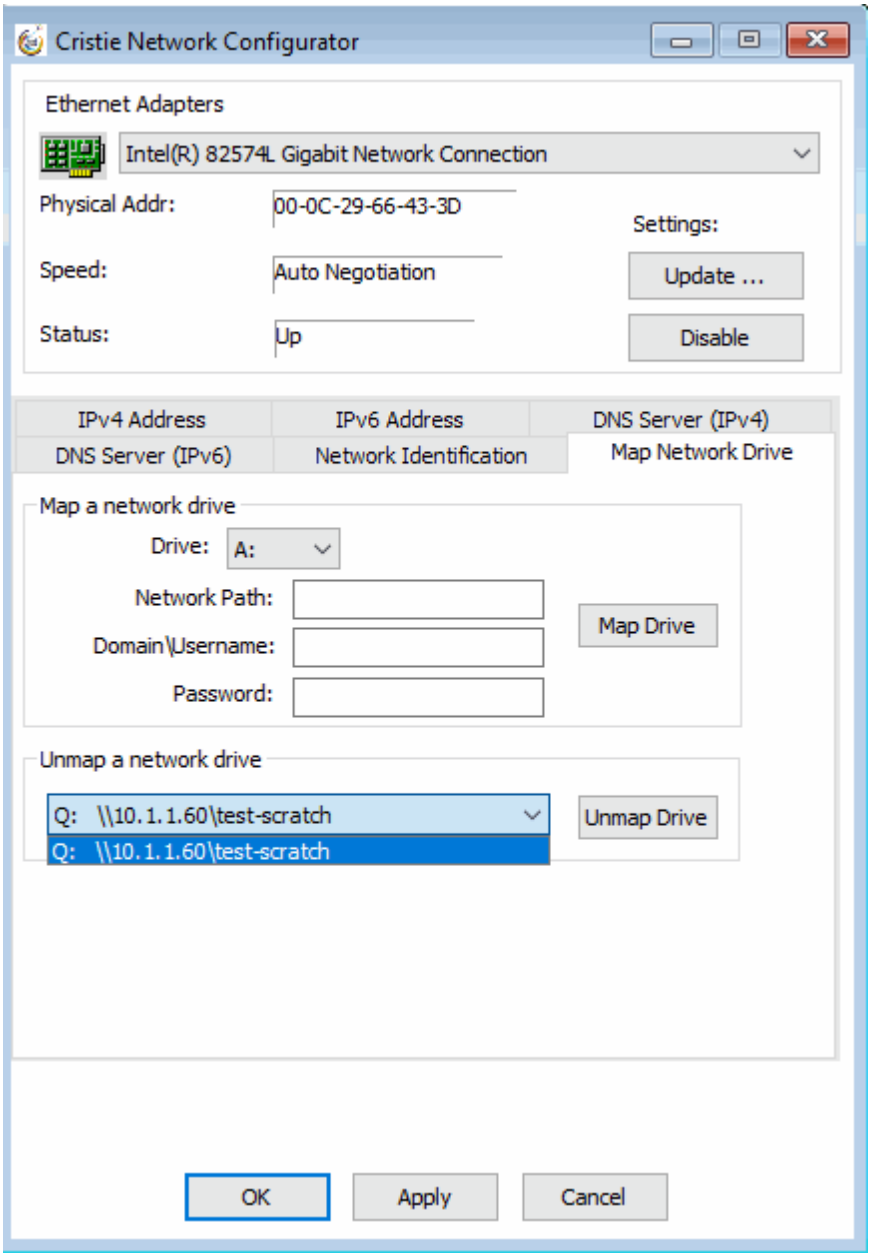
Select the drive letter that you wish to allocate from the **Drive** drop-down box and type in the share name that you wish to associate with it. Also specify the network credentials to be used to access the share.

Note: The network path may be specified either by hostname, IPv4 or IPv6 address.

Press Map Drive to confirm the share operation. If successful, the share will be added to the **Unmap a network drive** drop down list.

6.2.5.4 Unmap a Network Drive

If you need to disconnect a mapped drive for any reason, this option allows you to do this. Just select the drive that you wish to disconnect from the Unmap a network drive drop down list and then click Unmap Drive.



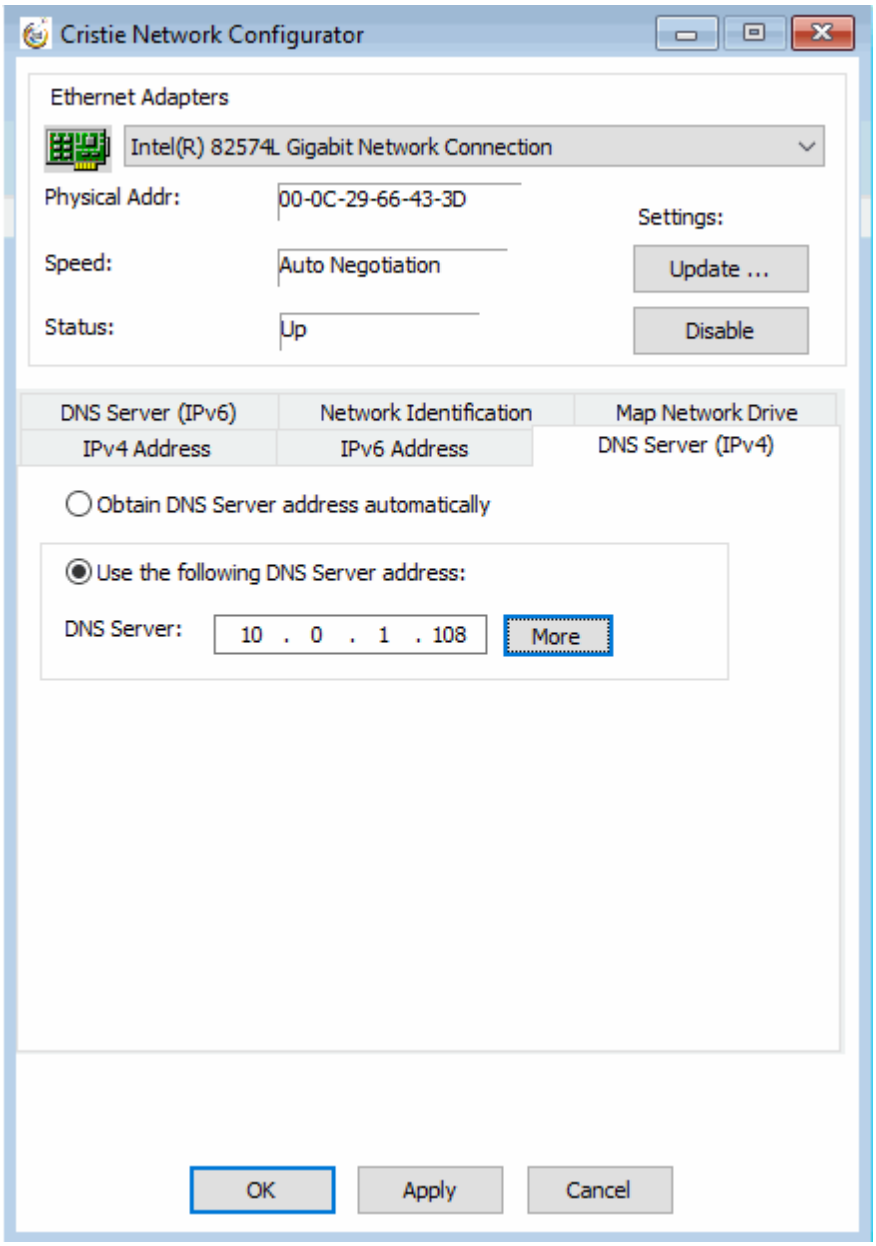
The mapped drive is removed from the list to confirm the operation.

6.2.5.5 Setup DNS Servers

DNS server IP addresses are automatically set when the WinPE5, WinPE10 or WinPE11 DR environment boots. However, options are provided to allow DNS server IP addresses to be manually set if required.

Different tabs are provided for configuring IPv4 or IPv6 IP addresses.

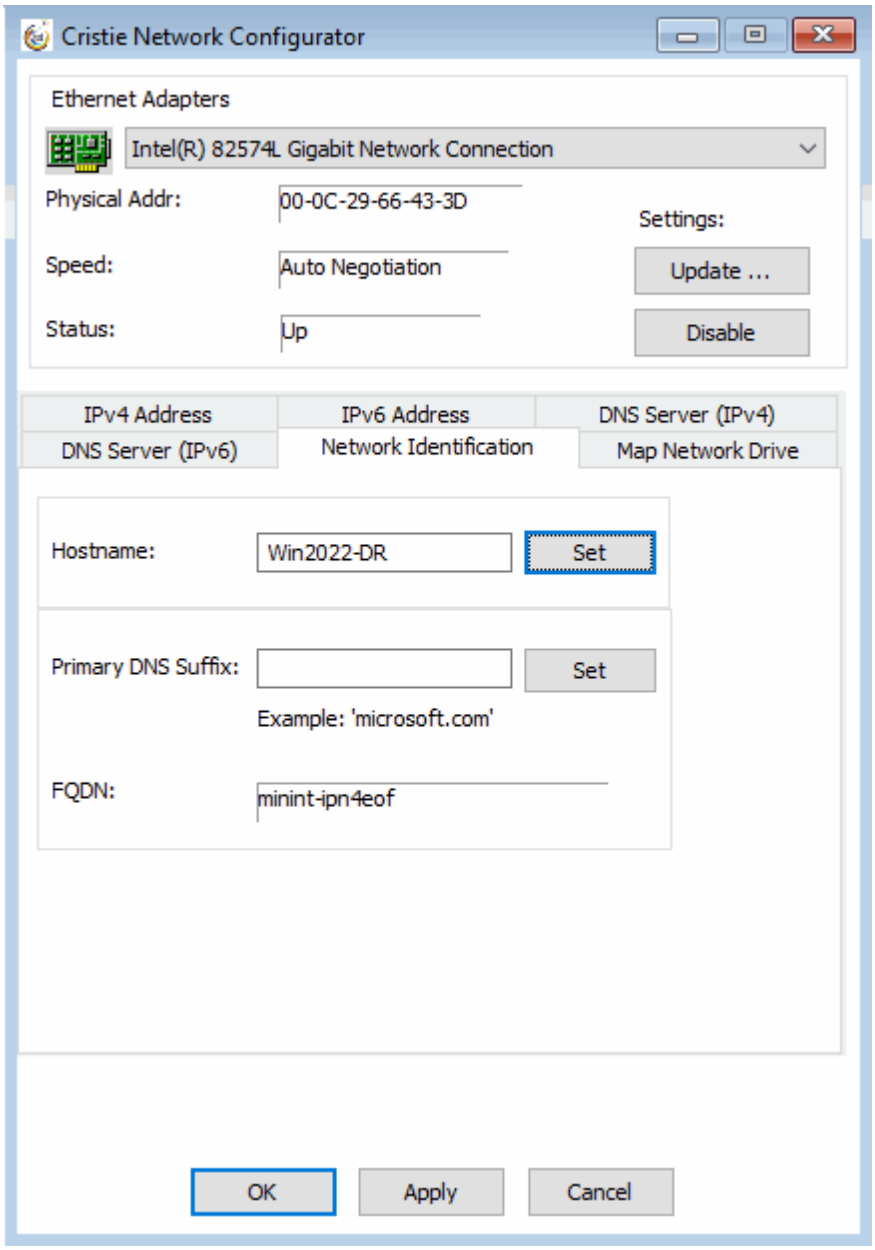
Note: WINS servers are not currently supported by this tool.



Select the **'Use the following DNS Server address'** radio button and enter the new DNS IP server address. If required, select the More button to add several DNS IP addresses. Press Apply to activate the new address.

6.2.5.6 Setup Network Identification

Click the **Network Identification** tab to setup a new hostname for the recovering system. This allows the WinPE5, WinPE10 or WinPE11 hostname and Primary DNS suffix to be changed during a DR session if required. These details are transient and only apply only while the WinPE5, WinPE10 or WinPE11 DR session is running. They are not applied to the recovered system when it reboots after the DR session.



Enter the new Computer Hostname and press Set to confirm the change.

6.2.6 Configure Routing

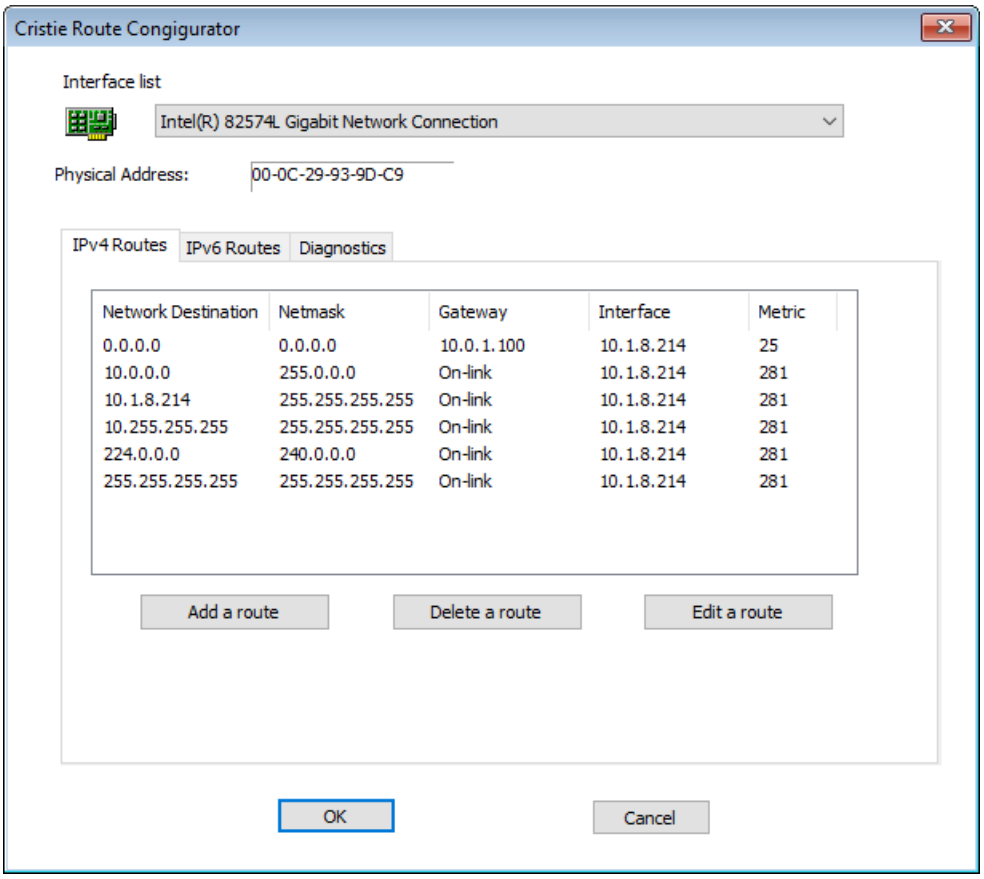
The **Cristie Route Configurator** tool provides extensive facilities to configure the network routes during the recovery process.

It offers the following features:

- supports multiple NICs
- provides the ability to add/modify/delete a route
- supports IPv4 and IPv6 routes
- allows IPv4 and IPv6 ping/tracert diagnostics to be run on a target hostname or IP address

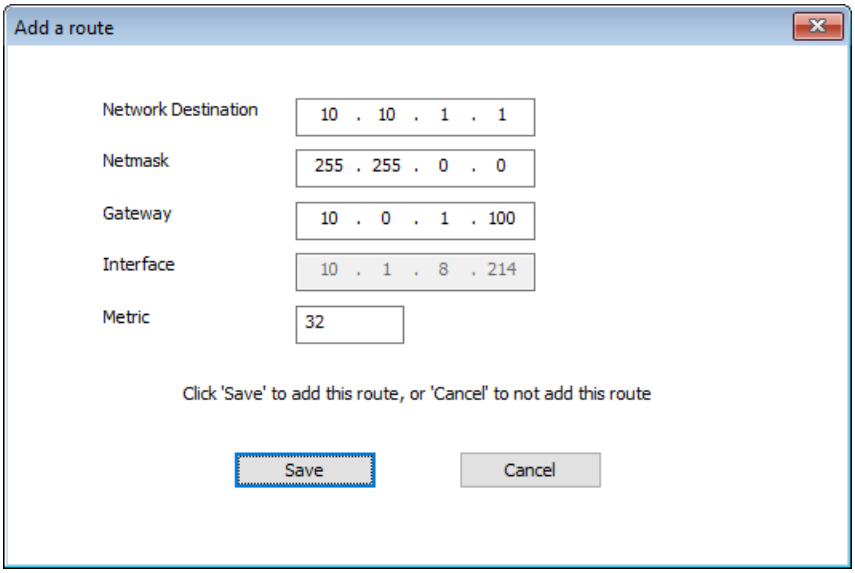
6.2.6.1 IPv4 Routes

Click the IPv4 Routes tab if not already selected. First select the required interface from the drop-down list.

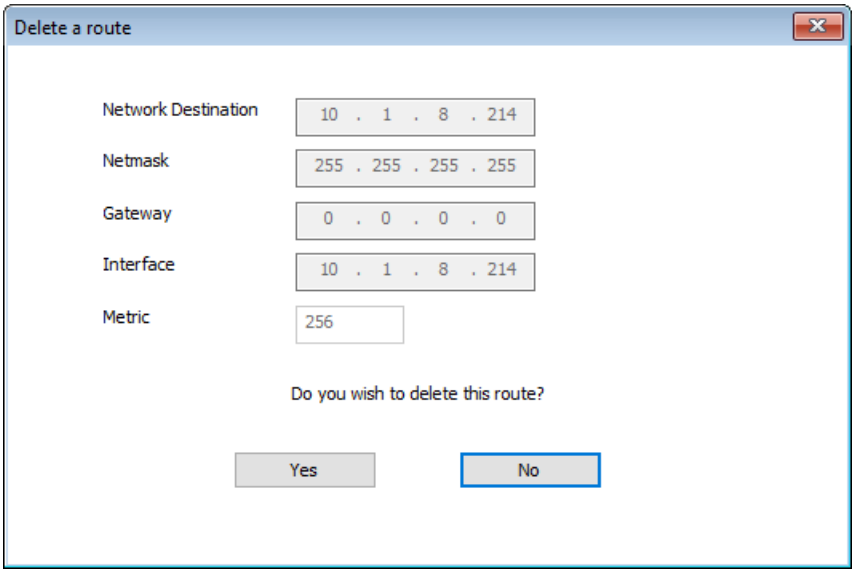


You may then add a new route, delete or edit an existing route.

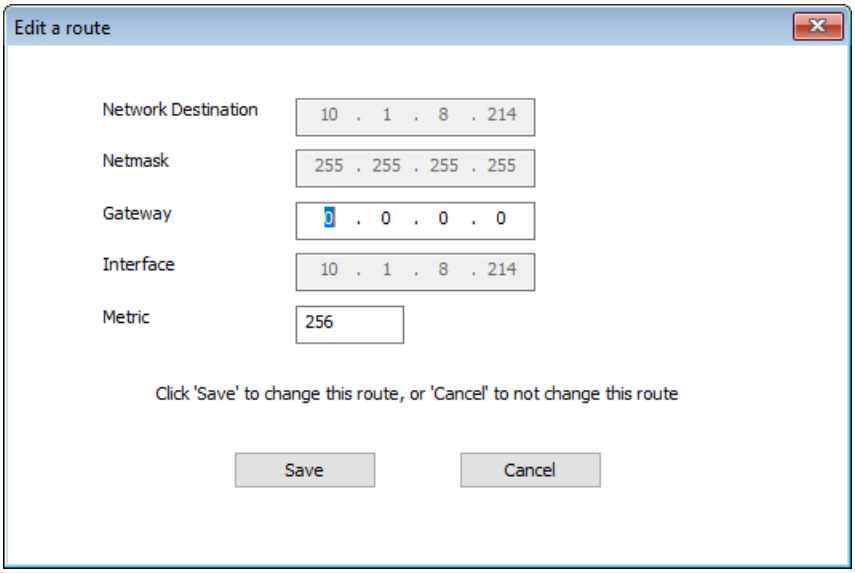
To add a new route, click Add a route. A data entry dialogue is displayed. To add a route identify the new route network, the route netmask, gateway and route metric. Click Save to add the new route or Cancel to cancel the creation of the new route.



To delete an existing route, highlight the desired route in the displayed list and click Delete a route. A confirmation dialogue is displayed. To delete click Yes to confirm or No to cancel the delete operation.

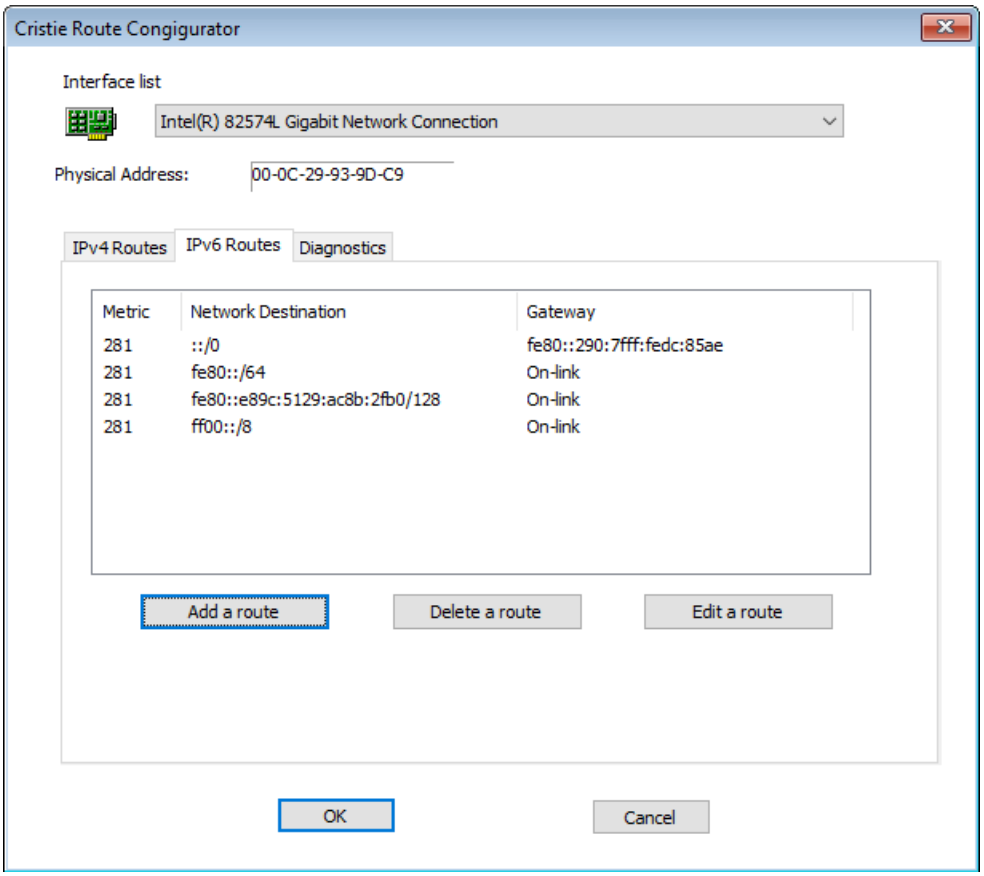


To edit an existing route, highlight the desired route from the displayed list and click Edit a route. A data entry dialogue is displayed. Only the network gateway and metric can be changed however. Click Save to make the changes or Cancel to abandon the changes.



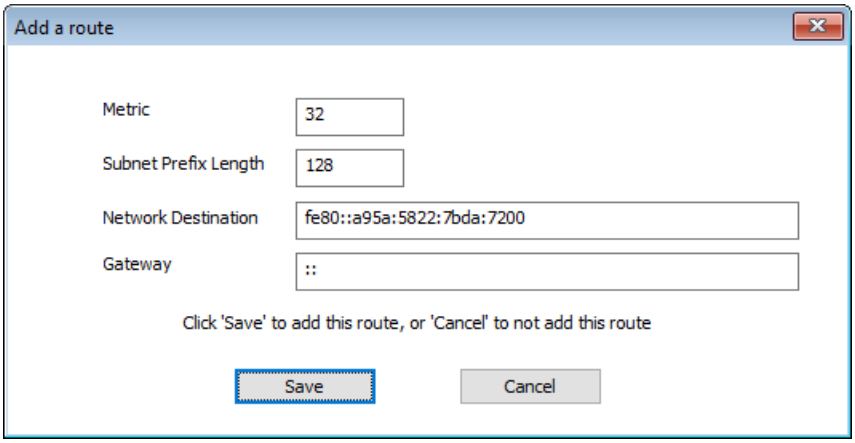
6.2.6.2 IPv6 Routes

Click the IPv6 Routes tab if not already selected. First select the required interface from the drop-down list.

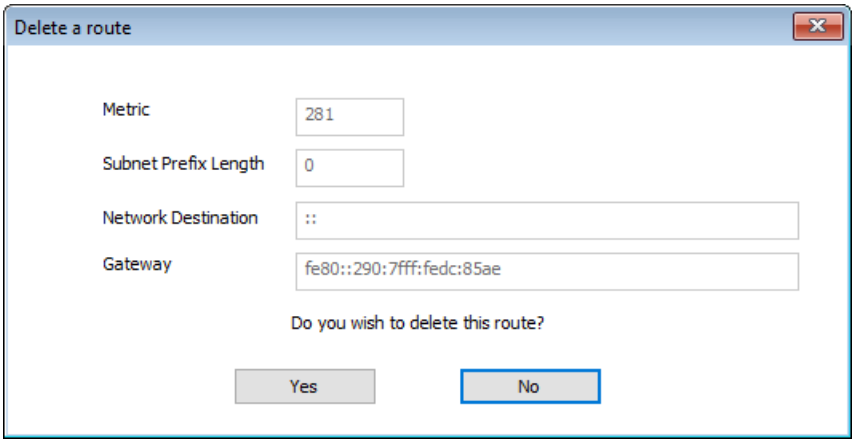


You may then add a new route, delete or edit an existing route.

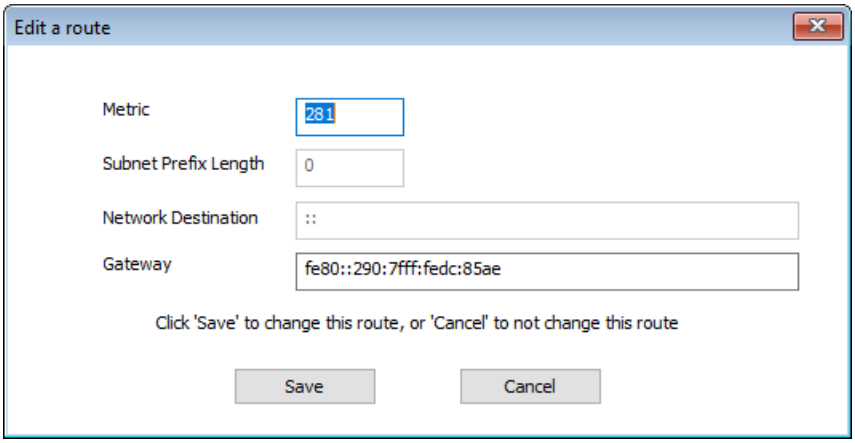
To add a new route, click Add a route. A data entry dialogue is displayed. To add a route identify the new route network, subnet prefix length, gateway and route metric. Click Save to add the new route or Cancel to cancel the creation of the new route.



To delete an existing route, highlight the desired route in the displayed list and click Delete a route. A confirmation dialogue is displayed. To delete click Yes to confirm or No to cancel the delete operation.

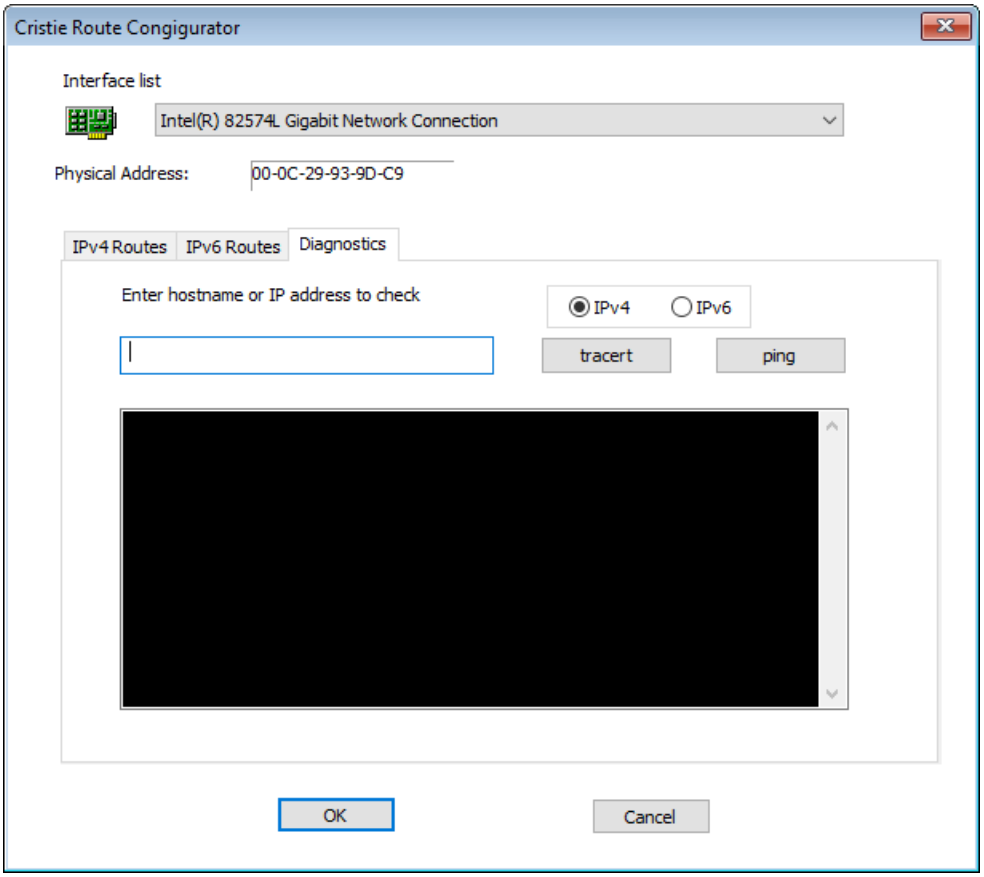


To edit an existing route, highlight the desired route from the displayed list and click Edit a route. A data entry dialogue is displayed. Only the network gateway and metric can be changed however. Click Save to make the changes or Cancel to abandon the changes.

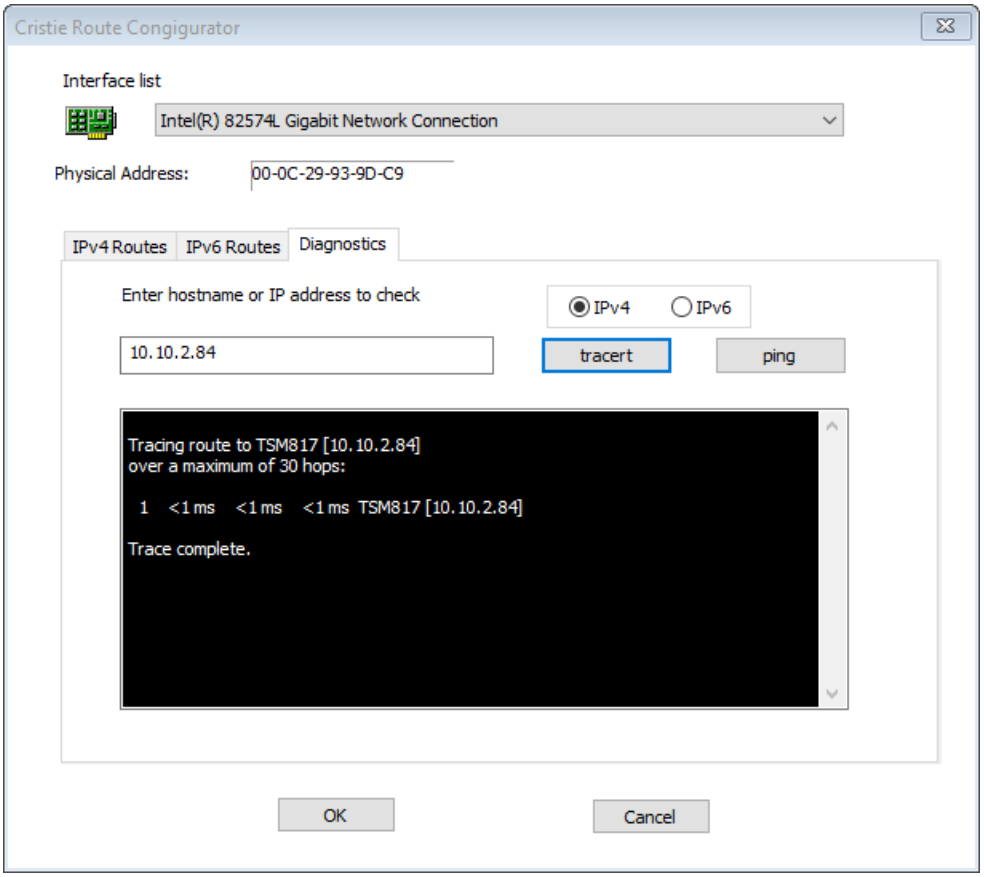


6.2.6.3 Diagnostics

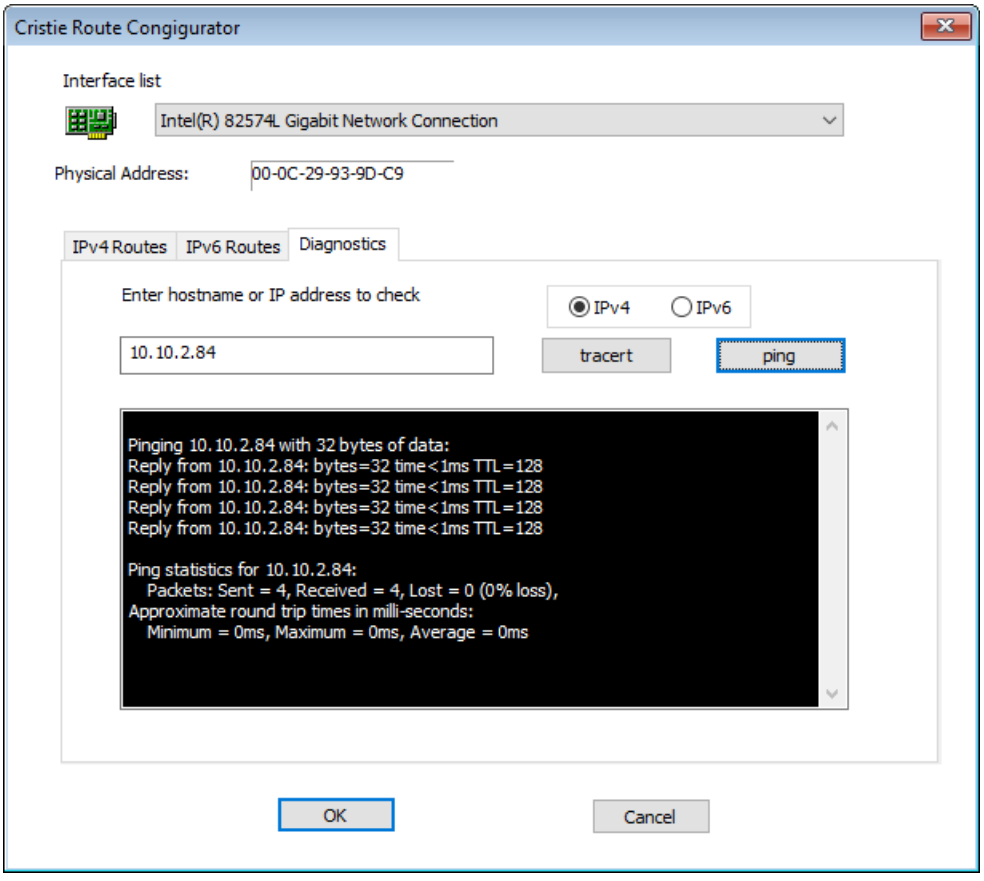
Click the diagnostics tab if not already selected. First select the required interface from the drop-down list.



Enter either the hostname or IPv4/IPv6 IP address of the network target. Click tracert to examine the route to the selected target.



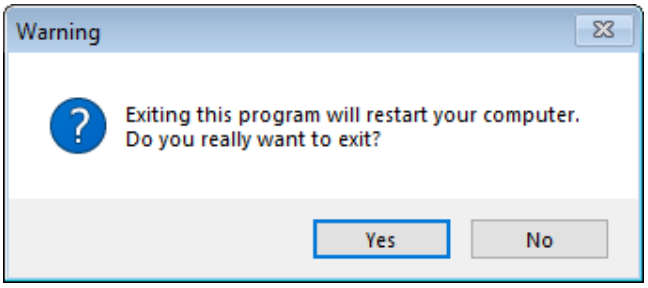
Click ping to check connectivity to the selected host. Click OK to exit the dialogue.



6.2.7 Reboot

After a successful recovery, select Reboot to exit the WinPE5, WinPE10 or WinPE11 environment and boot the recovered system. Note you may need to change the default boot device to be the OS boot disk since it may still be configured to boot from the TBMR DR boot environment.

Click Yes on the confirmation dialogue to restart or No to continue running the DR console:



6.3 Active Directory Recoveries

To perform an **Active Directory (AD)** restore on a DC no additional user actions are required during the restore phase.

For *block* or *image* based restores the **SystemState** is implicitly restored. For file based restore the SystemState is only explicitly restored if it has been backed up separately otherwise it is implicitly restored along with all the other files. In either case changes are made to SystemState to account for differences in hardware between the source and target machines and minor changes to the boot files if necessary.

After completing the restore the post-recovery phase does differ slightly. On first boot after recovery the system will boot into **Directory Services Repair Mode (DSRM)**. It will then perform some cleanup (required to reintroduce the DC back into its forest) and then reboot again to finalise this. Once this second reboot has taken place the DC should come back up OK.

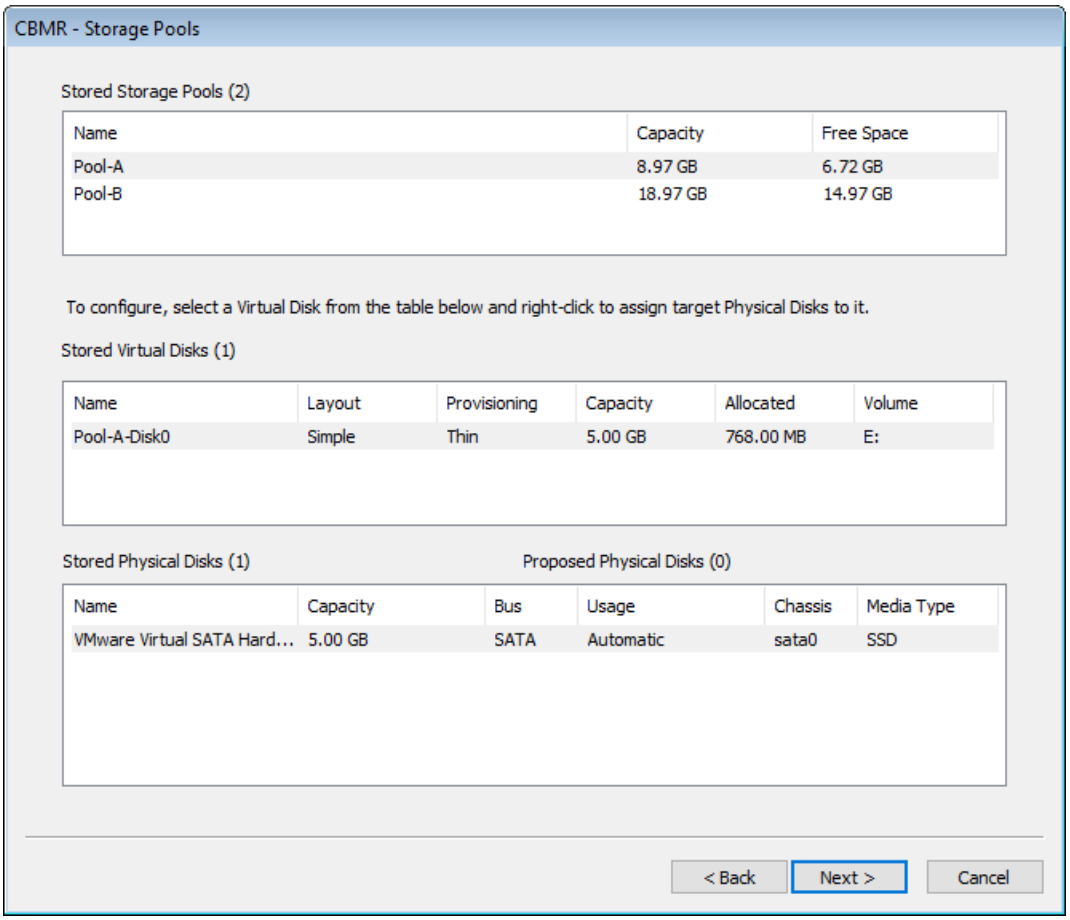
> ***Note: This entire phase is automated - the Microsoft online documentation states that a user must "login" to DSRM using a special username and password and run some steps. For TBMR AD recoveries this is not necessary and can cause issues. So the DC should be left alone until the second reboot takes place.***

7 Appendices

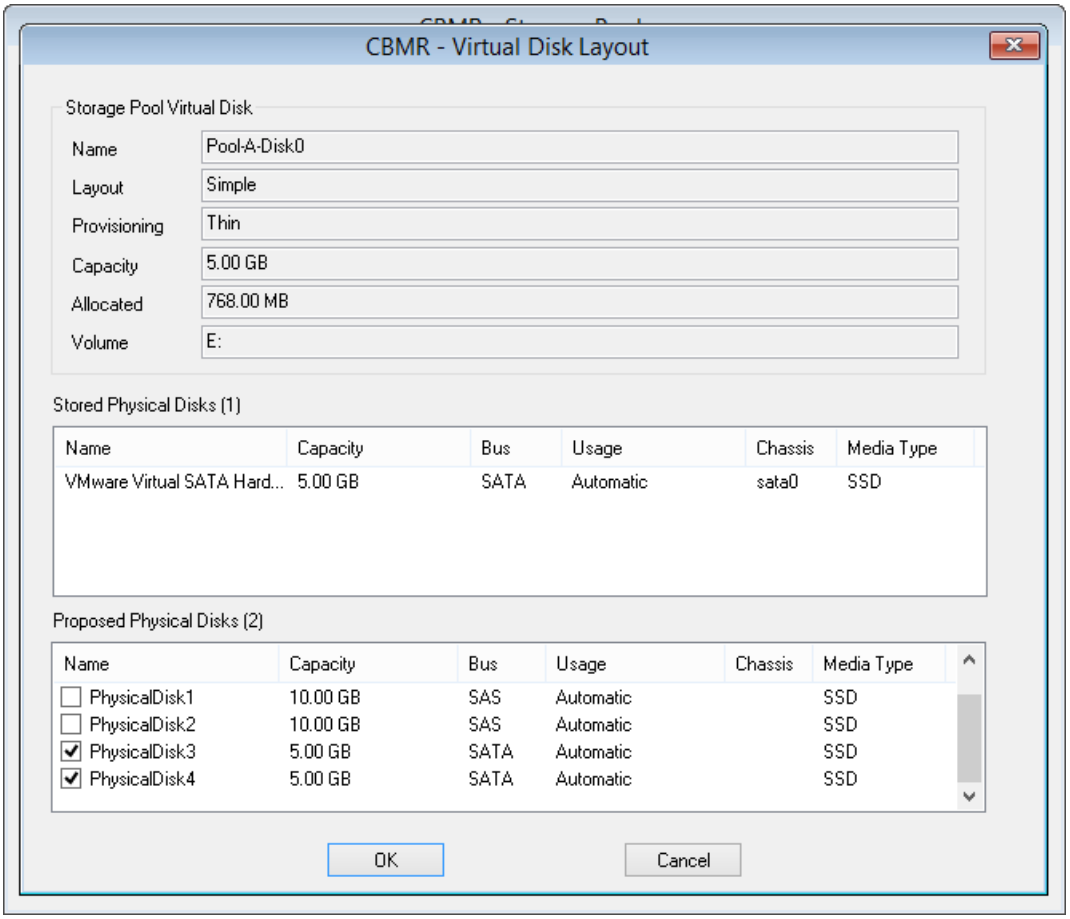
7.1 Storage Pool support

Windows **Storage Pools/Spaces** are now supported for Windows Server 2012 R2, 2016, 2019, 2022 and Desktop 10 and 11.

However, it is important you keep a note of your Storage Pool disk configuration since this will need to be manually re-configured during the recovery process. The Storage Pool names, physical and virtual disks will be saved, but not the disk mapping. For example, this is a typical Storage Pool configuration dialogue:



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



Note: nothing special needs to be done during the backup process as long as all the virtual disks in the pools are backed up.

Storage Pools created on iSCSI disks and restored to the same disks will need to be manually attached using the iSCSI initiator tool in the recovery environment **before** beginning the recovery sequence.

Similarly Storage Pools created on USB disks and restored to the same disks must be connected to the target host **before** booting the recovery environment.

Note: For a local USB disk to become part of a Storage Pool, it must be set to 'Not Removable' in the Windows settings Device properties. Otherwise it will not be offered as a candidate disk when setting up the pool.

If recovering a system with Storage Pools to a hypervisor or cloud, any source machine iSCSI or USB disks can be emulated with virtual disks on the target.

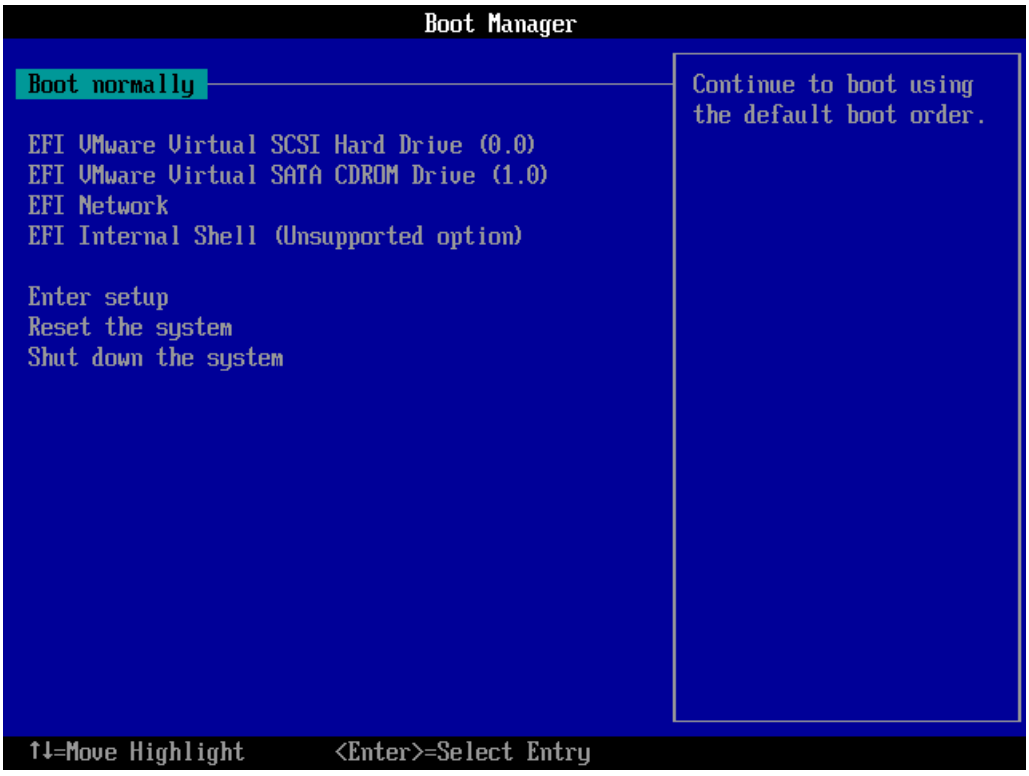
Note: Only the WinPE5 DR environment supports the recovery of storage pools at the moment.

7.2 UEFI and MBR BIOS support

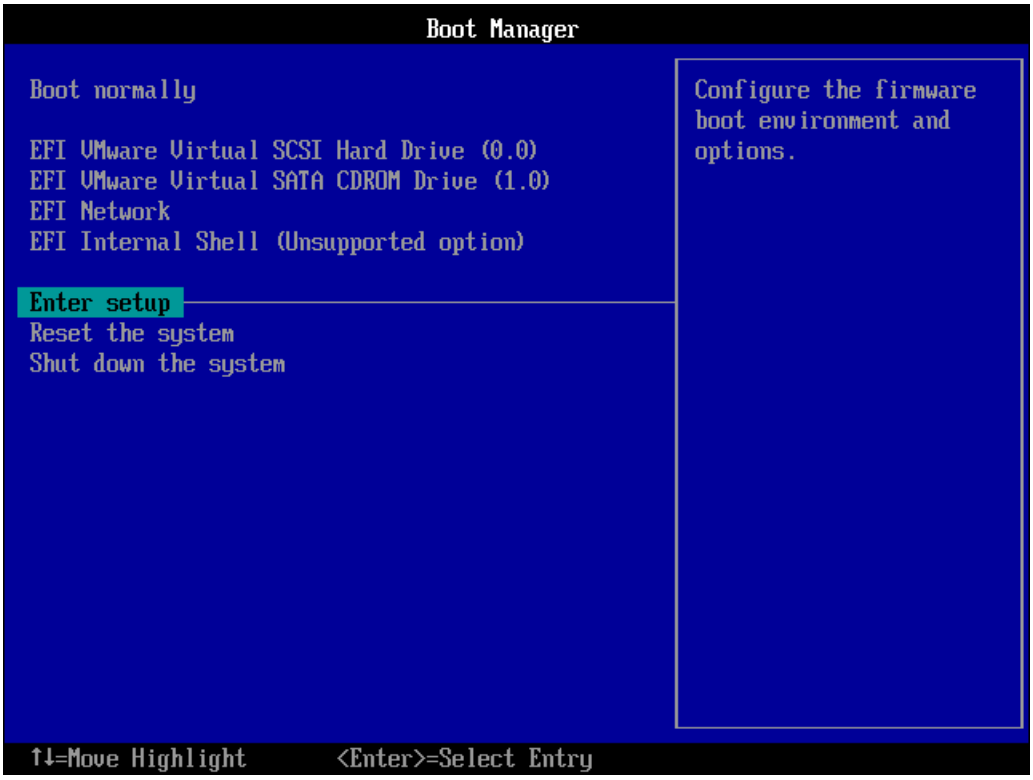
TBMR has the ability to convert a legacy BIOS boot configuration to a more modern EFI based boot configuration during a Windows clone operation. It does this automatically by creating an extra EFI partition on the detected boot disk and adding the requisite boot files to this partition. Regardless of the original boot disk type it will be converted to GPT format in the clone target system.

Note: This EFI BIOS conversion feature is only supported on compatible target environments such as physical machines, VMware Workstation™ and VMware vSphere™.

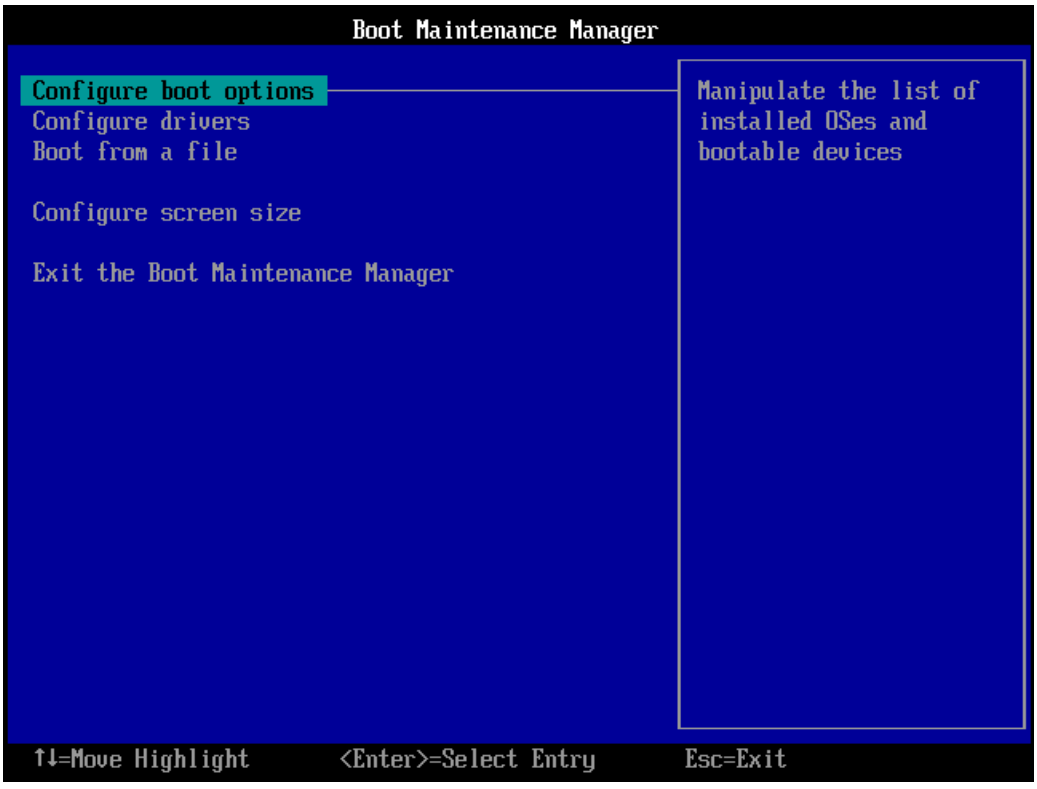
Prior to booting the new EFI clone target manual intervention will be required to configure a new boot option. An example of this obtained from a VMware Workstation™ clone target is shown below. Other virtual environments will be similar.



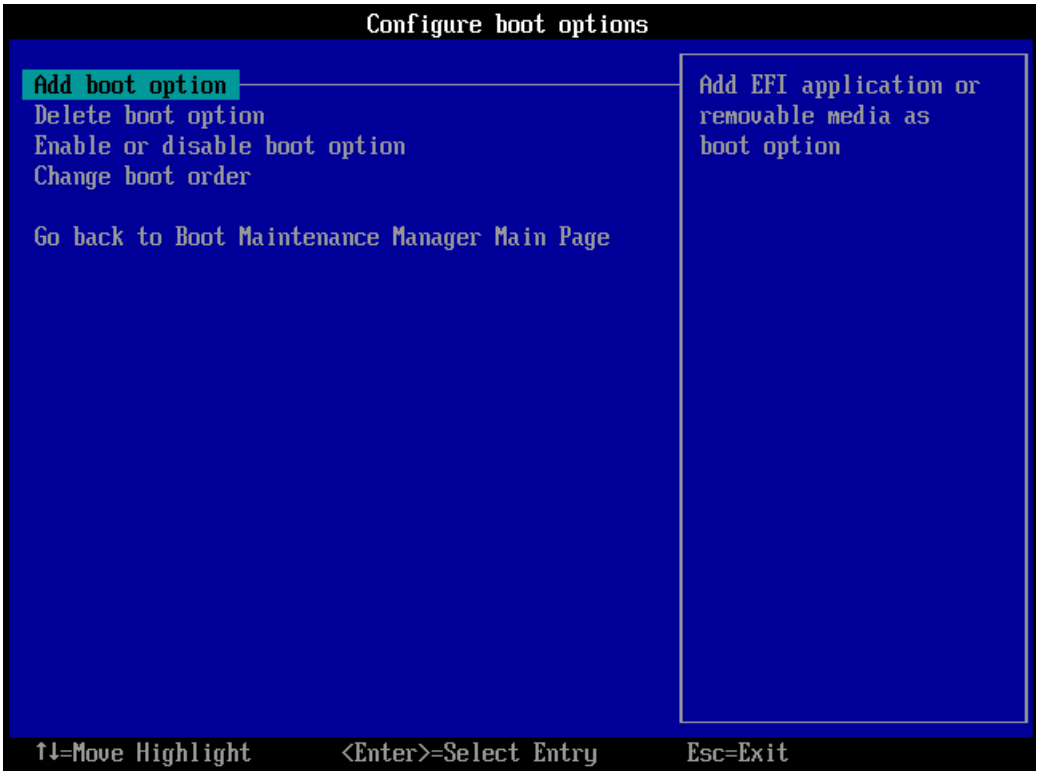
Default EFI bios



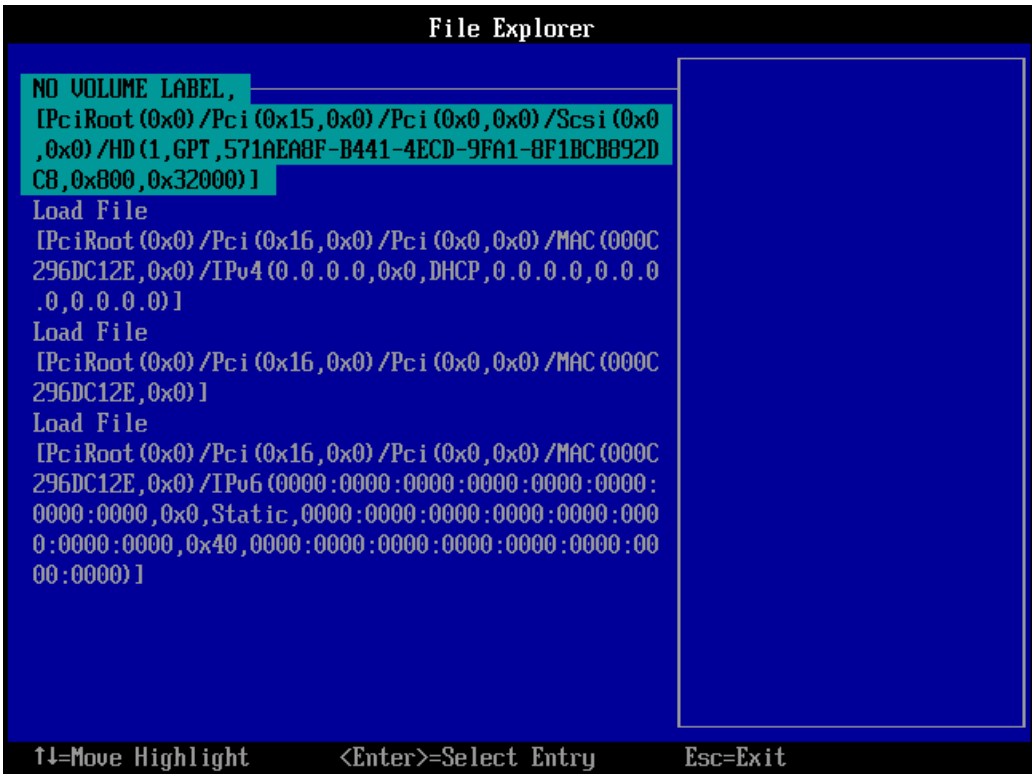
Select Enter Setup option



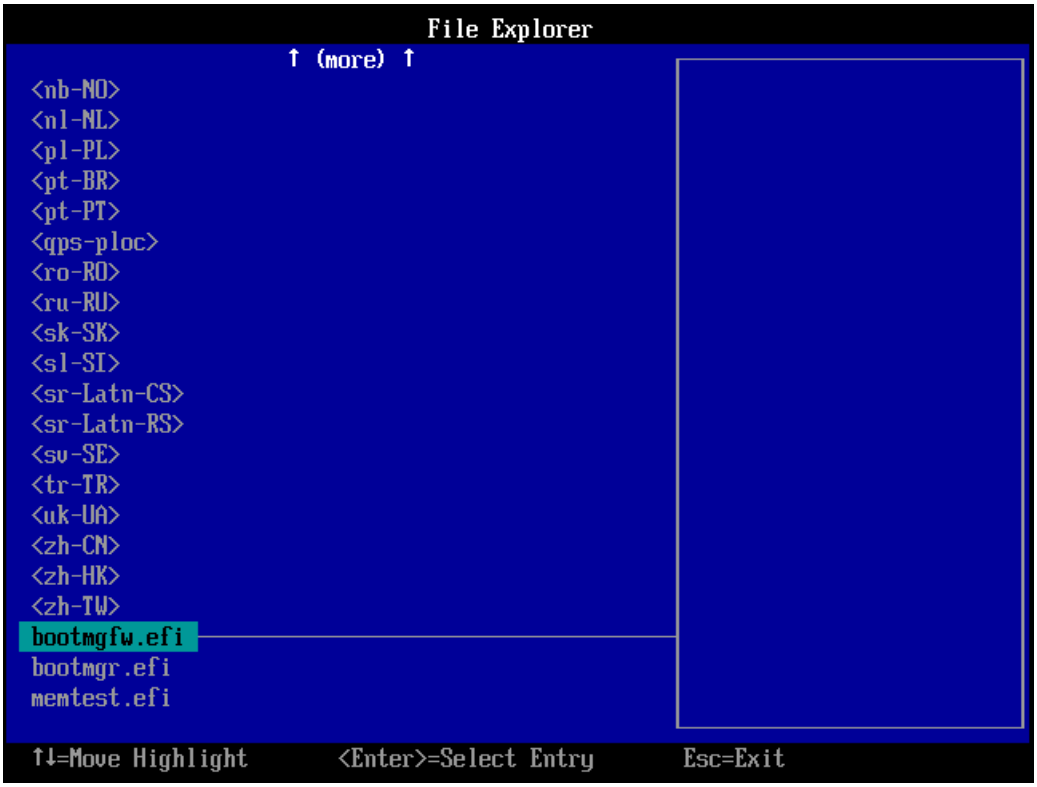
Select Configure boot options



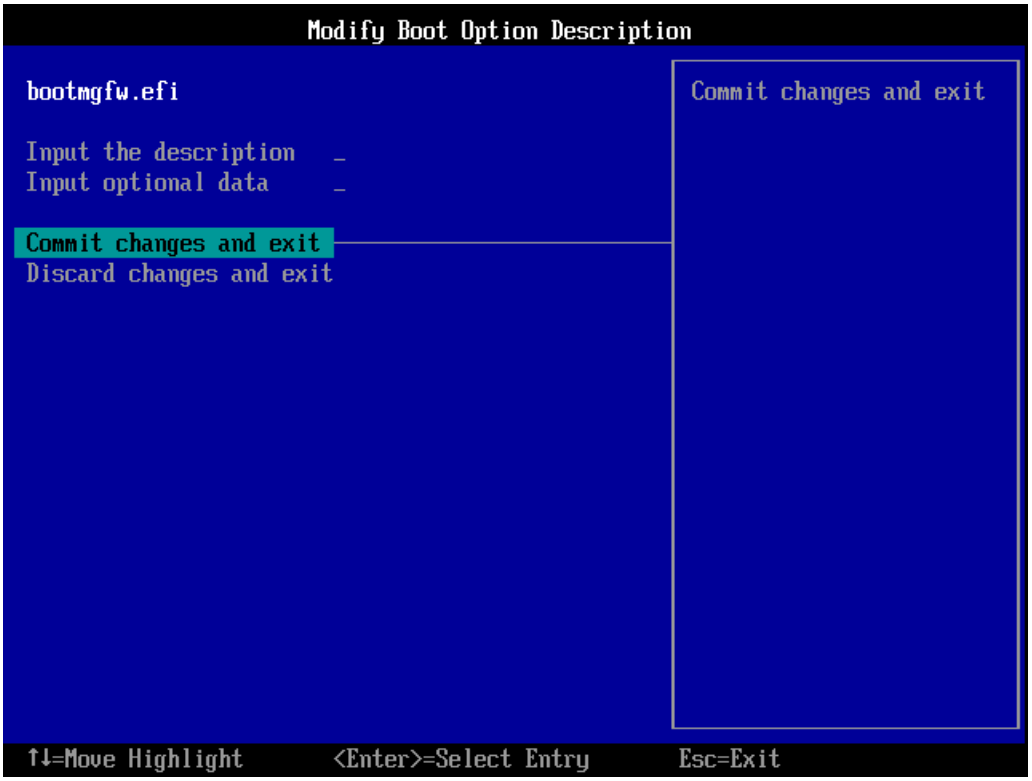
Select add boot option



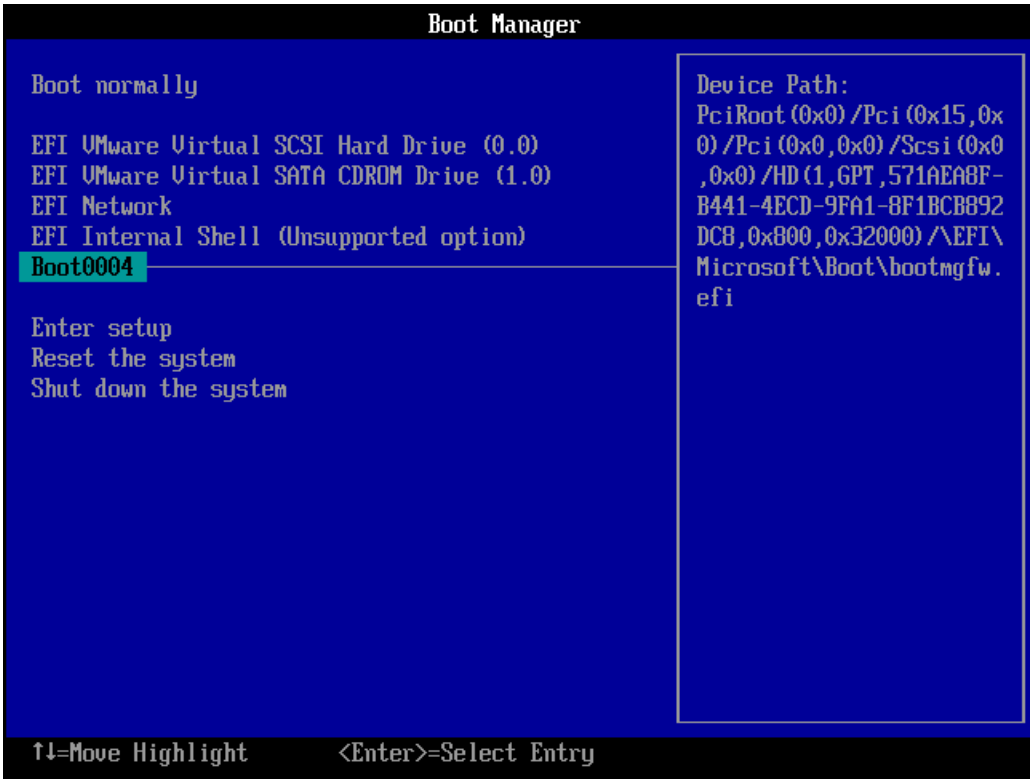
Select boot partition in File Explorer



Select EFI boot image



Modify boot option description and commit



New boot option configured

This feature supports clone source systems with a split boot configuration (i.e. *Boot* and *System* partitions on different disks or different *Boot*/*System* partitions on the same disk). The split boot configuration will be replicated on the clone target subject to the GPT conversion mentioned above.

This feature also supports source systems configured with a Windows dynamic boot volume (e.g. a dynamic mirror).

It is also possible to clone an EFI based source system to a target configured with a legacy BIOS. In this case any GPT based boot disks will be converted to legacy MBR disks and the EFI partition removed.

8 Cristie Technical Support

If you have any queries or problems concerning your Bare Machine Recovery for IBM Spectrum Protect product, please contact Cristie Technical Support. To assist us in helping with your enquiry, make sure you have the following information available for the person dealing with your call:

- TBMR Version Number
- Installed OS type and version
- Any error message information (if appropriate)
- Description of when the error occurs
- All Cristie log files relating to the source or recovery machine. This is very important to help us provide a quick diagnosis of your problem

Contact Numbers - Cristie Software (UK) Limited

Technical Support	+44 (0) 1453 847 009
Toll-Free US Number	1-866-TEC-CBMR (1-866-832-2267)
Knowledgebase	kb.cristie.com
Forum	forum.cristie.com
Sales Enquiries	sales@cristie.com
Email	support@cristie.com
Web	www.cristie.com

Support Hours

05:00 to 17:00 Eastern Standard Time (EST) Monday to Friday

Out-of-Hours support available to customers with a valid Support Agreement - Severity 1 issues* only

UK Bank Holidays** classed as Out-of-Hours - Severity 1 issues only.

*Severity 1 issues are defined as: a production server failure, cannot perform recovery or actual loss of data occurring.
**For details on dates of UK Bank Holidays, please see www.cristie.com/support/

Cristie Software Ltd. are continually expanding their product range in line with the latest technologies. Please contact the Cristie Sales Office for the latest product range.