



TBMR For Windows

Bare Machine Recovery for IBM Spectrum Protect

User Guide

Version 9.6.1 released April 2024

Copyright © 2008-2024 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 Avam ar are tradem arks 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.
- Am azon Web Services (AWS) and Am azon Elastic Compute Cloud (EC2) are trademarks of Am azon. com, Inc.
- Cohesity DataProtect is a trademark of Cohesity Inc.
- Rubrik is a tradem ark of Rubrik Inc.
- CloneManager® is a registered tradem ark 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 Website: https://www.cristie.com



3

Contents

1	Document Conventions	5
2	Overview	6
	2.1 Prerequisites	
	2.2 Backup Process	
	2.3 Recovery Process	
3	Create The Bootable Recovery	
	Environment	8
4	The TBMR Create Configuration	
-	Tool	9
	11 Creating the Configuration Information	0
	4.1 Creating the Configuration Information	
	4.2 Backup of Boot and SystemState Files	
	4.3 Creating a TBMRcfg Pre-Schedule	
5	Using a IBM Spectrum Protect	
•	Backup for Disaster Recovery	13
	5.1 Encrypted Backups	13
	5.2 Image Backups	15
	5.3 Backupsets	15
	5.4 Transitional Nodes	
6	Restoring your System	16
	6.1 Booting the WinPE5, WinPE10 or WinPE11 DR Environment	16
	6.2 WinPE5, WinPE10 or WinPE11 Based TBMR Recovery Environment	17
	6.2.1 TBMR Recovery Environment Main Menu	
	6.2.2 Begin the Restore Process	21
	Logfile Sav e Path	
	Select Restore Type	
	Restore from Node	
	Specify Certificate File	
	Specify IBM Spectrum Protect Details and Recovery	
	Date/Time	
	Storage Pools Confirm Volume Layout	
	Select Filespaces To Restore	
	Clone Settings	
	Dissimilar Hardware	
	Restore from Backupset	
	Disk Recovery Sequence	
	Disk Scaling	
	6.2.3 Tools	48



4

7

8

Dissimilar Hardware Wizard	
Load a Driv er	
Copy log files to remov able media or network location	
6.2.4 View Logs	
6.2.5 Configure Network	59
Configure NIC Parameters	
Assign Static or DHCP IP Settings	
Map a Network Driv e	
Unmap a Network Driv e	
Setup DNS Serv ers	
Setup Network Identification	
6.2.6 Configure Routing	69
IPv 4 Routes	
IPv 6 Routes	
Diagnostics	
6.2.7 Reboot	
6.3 Active Directory Recoveries	
Appendices	76
7.1 Storage Pool support	
7.2 UEFI and MBR BIOS support	
Cristie Technical Support	83



1 Document Conventions

The following typographical conventions are used throughout this guide:

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



2 Overview

6

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.



TBMR User Guide

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



8

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.



TBMR User Guide

9

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.

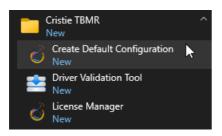
The Cristie tool that provides this function is called **TBMRCfg.exe** which is located in the TBMR installation folder (normally **Program Files\Cristie\TBMR**). This is a command line only tool which is licensed for use for a 30 initial day trial period. A full license is required to use the program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

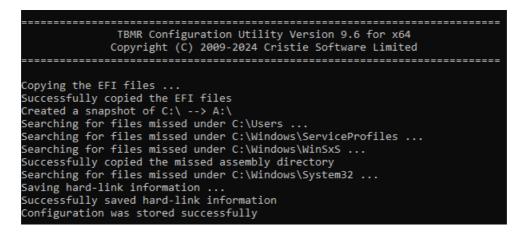
The next sections discuss this process in more detail.

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.



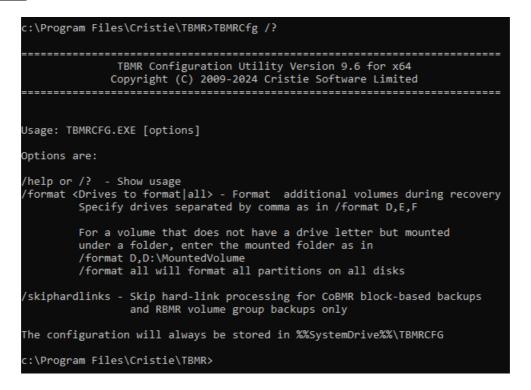
This will create a new configuration using the default settings.



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 <code>TBMRCfg.exe /?</code>, this will display the command line options available.





The command line options are very simple:

/help or /?

10

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

TBMR User Guide

11

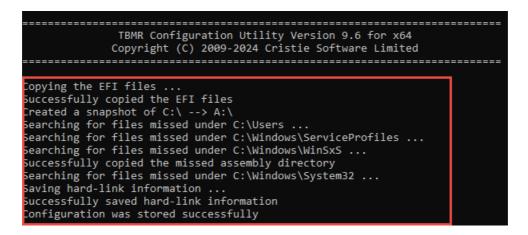
TBMRCfg stores the configuration in %SystemDrive%\TBMRCFG folder (%SystemDrive% is the drive associated with the Windows folder, usually C:\). This location cannot be changed.

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:



Enter File Encryption Key Password	<
Enter File Encryption Key Password	
File name: \\\Boot	
Encryption Key password:	
Confirm Key password:	
OK Cancel Help	

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:

_	TBMR Recovery Status	
Formatt	Restore Status - 20 % Completed.	^
Preparir Creating Created Formatti Created	Filespace Details Name : \\win-16d52g9home\c\$ Type : NTFS Drive : C:	
Created Created	Password Request	
Created Created Formatti Formatti Formatti Formatti Creating Creating Making	Data is encrypted using a password. Enter the correct password and press [OK] to proceed. Pressing [Cancel] will abort the operation.	ļ
Stoppin	Time Taken : UU:15:30 Hate : 7488.8 KB7Sec	
Succes	Restored Files (47 %)	
Restore Backup	Restored Bytes (20 %)	
F	Close Abort	*
	Close Abor	t

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.



TBMR User Guide

15

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 <u>Create the</u> <u>bootable cloning environment</u> 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.

- 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.

Press any key to boot from CD or DVD._

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 <u>Load a Driver</u> 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.



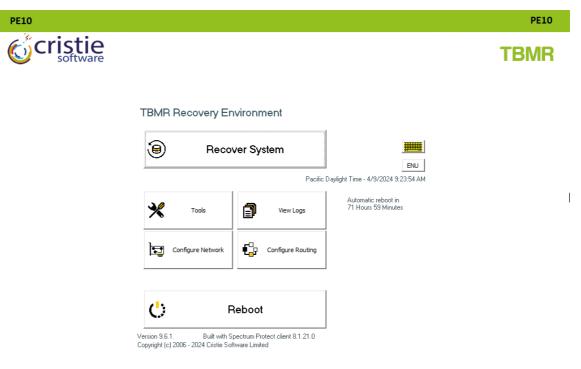
When this sequence completes, the TBMR Recovery Environment will be shown.



6.2.1 TBMR Recovery Environment Main Menu

18

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:



PE10

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



icons to do this.

Automatic reboot in

A reboot countdown clock is shown 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



PE10

	English (UK)
~	English (US)
	Czech
	Danish
	Dutch
	Finnish
	French (France)
	French (Belgium)
	French (Canada)
	French (Swiss)
	German (Germany)
	German (Swiss)
	Hungarian
	Icelandic
	Italian
	Japanese
	Latin American
	Norweigan (Bokmål)
	Polish
	Portuguese (Portugal)
	Portuguese (Brazil)
	Russian
	Slovak
	Slovenian
	Spanish
	Swedish
	Ukranian
	Date, Time and Time Zone
	NTP Resync

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.



💣 Date and Time			
Date and Time Additional Clock	ks Internet Time		
Date: Tuesday, April 9, 2024 Time: 9:29:46 AM Change date and time Time zone (UTC-08:00) Pacific Time (US & Canada)			
	Change time zone		
Daylight Saving Time ends on Sunday, November 3, 2024 at 2:00 AM. The clock is set to go back 1 hour at that time.			
	OK Cancel Apply		

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.



		Restoring your System	21
PE10			PE10
Cristie		1	BMR
	TBMR Recovery Environment Pecial Recover System Pacial Pacial Tools Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system Image: State of the system	ENU ENU ific Daylight Time - 4/9/2024 9:30:55 AM Automatic reboot in 71 Hours 52 Minutes	
	C Reboot		
			- • ×
Esc ~ 、 ! <u>1</u> [@] 2 [#] 3	^{\$} 4 [%] 5 [^] 6 ^{&} 7 [*] 8 ⁽ 9 ⁾) 0 ⁺ = 🕙 Home Pgl	Jp Nav
Tab q w e r	tyu i o p	{ [On Mv Up
Caps a s d	fghjkl:	; ". Enter Insert Pau	ise Mv Dn
Shift z x c	v b n m < , > .	? / ^ Shift PrtScn Scr	Lk Dock
Fn Ctrl 🖷 Alt	Alt Ctr	I < ✓ >	Fade

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.



TBMR - Specify Path To Save Logfiles To At End Of Recovery
Check this box if you do not wish to supply a path to save the log files to
Log Files Path Enter the path to save the log files to either as a share in UNC format or as a drive letter and path.
Browse
Configure Network
< Back Next > Cancel
For example, use the option to first map a network share location of then Browse to select a folder on the share.
Log Files Path
Enter the path to save the log files to either as a share in UNC format or as a drive letter and path.

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

Browse...

Configure Network

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.

V:\nigelp\Logs

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

TBMR User Guide

į

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.

TBMR - Select Restore Type
Please specify the type of restore you wish to perform:
Restore from a Spectrum Protect node
○ Restore from a backupset stored on a Spectrum Protect node
Restore from a backupset stored on a disk or removable media other than tape
< Back Next > Cancel

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.



RMR	R - Specify Certificate Path	
bink specify certificate ratio		
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 >]		
	Configure Network	
	< Back Next > Cancel	

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.



MR - Specify Certificate Path		
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 >]		
Check this box to use a certificate file or a zip file of the client key databa	ase.	
Enter the certificate file or zip file name either as a share in UNC format or as a drive letter and path.		
V: \nigelp\TSM-Certificates\8.1.17\10.10.2.84.arm	Browse	
	Configure Network	
	< Back Next > Cancel	

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.

TBM	R - Spectrum Protect Sett	tings							
	Please enter the Spectrum Protect Server and Client details below and select 'Next>' to continue.								
	Spectrum Protect Server Details								
	Server Name/IP Address:	: 10.10.2.84 Port: 1501							
	Backupset Location;	Browse							
	Spectrum Protect Client D	Details							
	Node Name:	NP-WIN2022							
	User Id*:								
	* Leave blank	ik if you wish to use the default (i.e. the same as the Node Name)							
	Password:	•••••							
	Wednesday, A	PII) restore April 10, 2024 12:30:11 AM							
		< Back Next >	Cancel						
		< DALK NEXT >	Cancel						

Identify Spectrum Protect server using an IPv4 IP address

Or,



TBMR - Spectrum Protect Se	ttings								
Please enter the Spectra below and select 'Next>	Please enter the Spectrum Protect Server and Client details below and select 'Next>' to continue.								
Spectrum Protect Serve	Spectrum Protect Server Details								
Server Name/IP Addres	s: fe80::cb0:2fa2:1883:2ab611 Port: 1501								
Backupset Location	Browse								
Spectrum Protect Client	Spectrum Protect Client Details								
Node Name:	NP-WIN2022								
User Id*:									
* Leave bla	nk if you wish to use the default (i.e. the same as the Node Name)								
Password:	•••••								
Point-in-time	(PIT) restore								
Wednesday,	April 10, 2024 🔍 🔪 12:30:11 AM 🚖								
	< Back Next > Cancel								

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:



TBMR - Spectrum Protect Settings							
Please enter the Spectrum Protect Server and Client details below and select 'Next>' to continue.							
Spectrum Protect Server Details							
Server Name/IP Address: 10.10.2.84 Port: 1501							
Backupset Location: Browse							
Spectrum Protect Client Details							
Node Name: NP-WIN2022							
User Id*:							
* Leave blank if you wish to use the default (i.e. the same as the Node Name)							
Password:							
Point-in-time (PIT) restore							
Wednesday, April 10, 2024 🔍 12:30:11 AM 🚖							
▲ April 2024 ►							
Sun Mon Tue Wed Thu Fri Sat							
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 8 9 10 11 Today: 4/10/2024							
Today; 4/10/2024							
< 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 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:



TBMR Recovery Status										
Formatt	nestore status - 20 /0 Completeu.									
Preparir Creating Created Formatti Created	Filespace Details Name : \\win-l6d52g9homc\c\$ Type : NTFS Drive : C:									
Created Created	Password Request									
Created Created Formatti Formatti Formatti Formatti Formatti Creating Creating Making	Data is encrypted using a password. Enter the correct password and press [DK] to proceed. Pressing [Cancel] will abort the operation.	ļ								
Stoppin	Time Taken : UU:15:30 Rate : 7488.8 KB/Sec									
Succes	Restored Files (47 %)									
Restore Backup	Restored Bytes (20 %)									
	Close Abort	~								
	Close Abo	rt								

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:

Name					Capacity		F	ree (Space	
Pool-A					8.97 GB		e	5.72 (GB	
Pool-B					18.97 GB		1	14.97	7 GB	
To configure, select a Virtual D tored Virtual Disks (1)			-							
Name Pool-A-Disk0	Layout Simple	Provis	ioning	Capac 5.00 (Alloca	ated 00 MB		Volume E:	
Neural District District (1)			D		at and installed	(0)				
tored Physical Disks (1)			Propo	osed Phy	sical Disks	(0)				
Stored Physical Disks (1) Name	Capacity		Propo	osed Phy Usage		(0)	Chassis	5	Media Type	
Stored Physical Disks (1) Name VMware Virtual SATA Hard			-		2	(0)	Chassis sata0		Media Type SSD	

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).

TBMR User Guide

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**.

Storage Pool Virtu	ual Disk						
Name	Pool-A-Dis	k0					
Layout	Simple						
Provisioning Thin							
Capacity 5.00 GB							
Allocated 768.00 MB						1	
Volume	E:						
/Mware Virtual S.							
	Disks (2)						
oposed Physical	Disks (2)	Capacity	Bus	Usage	Chassis	Media Type	^
oposed Physical		Capacity 10.00 GB	SAS	Usage Automatic	Chassis	SSD	^
oposed Physical Name PhysicalDisk1 PhysicalDisk2		10.00 GB 10.00 GB	SAS	Automatic Automatic	Chassis	SSD SSD	^
oposed Physical Name] PhysicalDisk1		10.00 GB	SAS	Automatic	Chassis	SSD	^

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:



Name			Capacit	у	Free Space
Pool-A			8.97 GB	1	6.72 GB
Pool-B			18.97 G	В	14.97 GB
To configure, select a Virtual i tored Virtual Disks (2)	Disk from the tab	ole below and right	-click to assign tar	get Physical Disl	ks to it.
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)		Prop	osed Physical Disk	s (2)	
Name	Capacity	Bus	Usage	Chase	sis Media Type
VMware, VMware Virtual S	10.00 GB	SAS	Automatic	SCSI	D SSD

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.



CBMR - Storage Pools	
CBMR_DP.DLL 9.3 (build 43373) Cristie Disk Partitioner (CDP) created on Aug 12 Creating Storage Pool S Creating Virtual Disk 'Pool-A-Disk0' Creating Virtual Disk 'Pool-B-Disk0' Creating Virtual Disk 'Pool-B-Disk1' Loading configuration information Restoring Microsoft Windows Server 2019 (1809) Nov 2018, 64-bit (build 17763)	
OK	< Back Next > Cancel

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

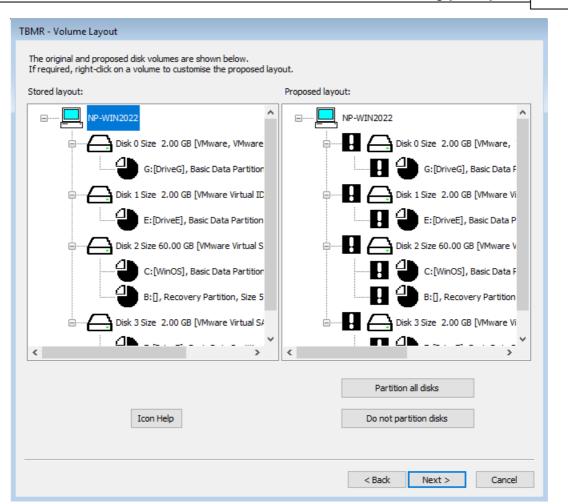
The next step in the **Automatic recovery** shows a list of the disks and partitions to be recovered.

TBMR - Volume Layout							
The original and proposed disk volumes are shown below. If required, right-click on a volume to customise the proposed la	yout.						
Stored layout:	Proposed layout:						
	□ □ NP-WIN2022						
Disk 0 Size 2.00 GB [VMware, VMware Vi	rt Disk 0 Size 2.00 GB [VMware, VMv						
Disk 1 Size 2.00 GB [VMware Virtual IDE	H Disk 1 Size 2.00 GB [VMware Virtua						
Disk 2 Size 60.00 GB [VMware Virtual SAT	A Disk 2 Size 60.00 GB [VMware Virtu						
Disk 3 Size 2.00 GB [VMware Virtual SAT.	A Disk 3 Size 2.00 GB [VMware Virtua						
< >	< >						
	Partition all disks						
Icon Help	Do not partition disks						
	< Back Next > Cancel						

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



TBMR User Guide



The left-hand panel of the dialogue shows the original disk layout and partitions. The righthand 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

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 a placed next to a disk means at least one partition/ volume WILL be partitioned.

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

There are 3 disk types available:

∃ indicates a standard disk



36

indicates a dynamic disk

indicates a Storage Pool virtual disk

Click on the Icon Help button to display a summary of this:

TBMR - Volume Layout The original and proposed disk volumes are shown below. If required, right-click on a volume to customise the proposed la	ayout.
Stored layout:	Proposed layout:
Icon Help Disk Level Disk WILL be partitioned Image: Disk WILL NOT be partitioned Image: Disk WILL NOT be partition. At least one Partition. Volume WILL be formatted Disk WILL be ignored in the recovery	VMv Partition/Volume Level Virtue Partition/Volume WILL be formatted Virtue Partition/Volume WILL NOT be formatted Disk Type Disk Disk Dynamic Disk
< Icon Help	Storage Pool Virtual Disk K Do not partition disks

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.



TBMR User Guide

TBMR - Volume Layout	
The original and proposed disk volumes are shown below. If required, right-dick on a volume to customise the proposed layout.	
Stored layout: Proposed layout:	
□ □ , NP-WIN2022	
Disk 0 Size 2.00 GB [VMware, VMware Virt Disk 0 Size 2.0	0 GB [VMware, VMv
Disk 1 Size 2.00 GB [VMware Virtual IDE H	0 GB [VMware Virtua
TBMR - Disk Partitioning	, Basic Data Parti
	GB [VMware Virtu
CAUTION: You will lose all the data on this disk!	GB [VMware Virtua
○ No, do not partition this disk. Existing data may be safe.	
OK Cancel	
	>
Partition all disks	
Icon Help Do not partition disks	
< Back Next >	Cancel

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

TBMR - Volume	e Layout	
	d proposed disk volumes are shown below. If required, right-click on a volum proposed layout.	e to
Stored layout:	Proposed layout:	
	NP-WIN2008R2	^
±	TBMR - Error	e 40.00 Gi
.	_	≥ 1.00 GE
±	Couldn't change whether disk should be partitioned	≥ 10.00 Gi
±		≥ 5.00 GE
*	ОК	≡ 5.00 GE ¥
		Icon Help
	< <u>B</u> ack <u>N</u> ext >	Cancel

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



TBMR - Volume Layout			
	d disk volumes are shown below. a volume to customise the proposed layout.		
Stored layout:	Pro	oposed layout:	
	022	□····· □ NP-WIN2022	
∎ ⊕ °	sk 0 Size 2.00 GB [VMware, VMware Virt		2.00 GB [VMware, VMv
÷ A	Volume / Partition Details	•	2.00 GB [VMware Virtua
. <u> </u>	Type: Partition File System: NTFS	p	riveE], Basic Data Parti
	-	Max (MB): 2031 6	i0.00 GB [VMware Virtu
	Label: DriveE		2.00 GB [VMware Virtua
	Mount Details:		
	Drive Letter: $_{\sf E}$ \sim		
	Sormat		
<	ОК	Cancel	>
		Partition all disks	
	Icon Help	Do not partition disk	S
		< Back Next	> Cancel

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

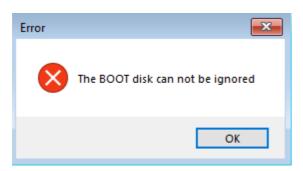
- size in MB (only if disk is shown with a 🕒)
- label
- format (yes/no)

The screenshot below shows an example:

ĺ	Volume / Partition Deta	ils			×
	Туре:	Partition			
	File System:	NTFS		\sim	
	Size in MB:	1556	Max (MB): 2031		
	Label:	NewDriveE			
	Mount Details:				
	Drive Letter:	$E=-\!$			
		🗹 Format			
		IK]	Cancel		

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**:

тві	TBMR - Select Filespaces to Restore						
	At least one System and one Boot partition must be selected in order to recover your machine. This may be the same partition. You can select additional drives to be restored by ticking the check box next to the drive.						
	Drive Letter	Boot	System	Name		File System	
	С:	Yes		\\np-win2022\c\$		NTES	
	E :			\\np-win2022\e\$		NTFS	
	F :			\\np-win2022\f\$		NTFS	
	G :			\\np-win2022\g\$		NTFS	
	Select All Deselect	All					
_							
					< Back Next	> Cancel	

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.

R - Clone Settings					
Do not cha	nge any settings on this	page unless you wish	to change the	e identity	
	overed machine. For exa				
Change the comp	uter's NetBIOS name on	reboot.			
NP-WIN2022	>	NewNetBIOS			
Change the comp	uter's host name on reb	oot.			
NP-Win2022	>	NewHostname			
,	>				
Change the IP ad	dress of this adapter on	reboot.			
Physical Addres	s: 00-0C-29-66	5-43-3D			
Intel(R) 82574	L Gigabit Network Conne	ction (Up)		~	
ancelycycecor	Use DHCP		DHCP		
IP Address:	10 . 10 . 11 .		. 10 . 11	. 80	
			. 0 . 0		
Netmask:	255.0.0.				
Gateway:	10 . 0 . 1 .	100> 10	. 0 . 1	. 100	

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 "<mark>Next ></mark>" the button will change to "<mark>Finish</mark>", 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.

TBMR - Dissimilar Hardware
The Plug-and-Play manager found new devices in the recovering machine.
View List
Default driver search path: x:\vmdrivers
Enter the path(s) where the drivers can be found:
X:\VMDrivers\VMwareDrivers\64-bit Browse
Separate multiple paths with a semicolon (;) Configure Network
Note: it is generally only necessary to inject drivers for mass storage and some network devices. Drivers for other device types (such as chipset, CPU type etc.) can be safely ignored and left for standard Windows Plug-and-Play processing on reboot. However if you wish to load all types of PCI device, tick the following box.
load all types of drivers
< Back Finish Cancel

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

configure Network

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.



42

			Found New Devices	
P	CI CI	Class Storage Network	Description Standard SATA AHCI Controller [PCI\VEN_15AD& 82574L Gigabit Network Connection [PCI\VEN_80	
			Exit	

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:



TBMR - Backupset Selec	tion	
Please select the bac	kupset to restore.	
Select backupset:		
Description:	win2022	
		< Back Next > Cancel

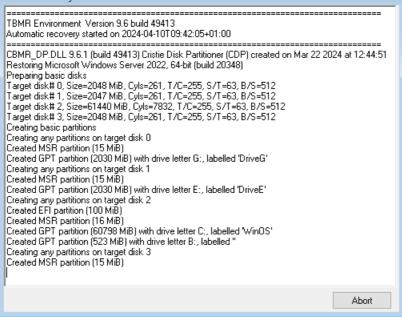
The rest of the restore sequence runs as described in the section Restore from Node.



Disk Recovery Sequence

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

TBMR Recovery Status



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**,



Restore Statu	ıs - 81 % Con	npleted.				
- Filespace I	Filespace Details					
Name:	C:					
Туре:	NTFS					
Drive:	C:					
Date:	09/04/2024	17:20:26				
Current File						
Name:	\Microso	oft-Windows-Identity	Server	-Proxy-Package~31bf3856a		
Size:	3.19 KB					
Status:						
Progress						
File	s Done:	50,769	of	119,804		
Byte	s Done:	5.75 GB	of	7.08 GB		
Time	Taken:	00:15:04		Rate: 7494.7 KB/s		
		Rest <mark>ored Files (4</mark>	2 %)			
		Restored Bytes (8	31 %)			
		Abort				

followed by SystemState (after a file count):

Restore State	us - 82 % Com	npleted.		
Filespace	Details			
	VSS SYSTE	M STATE		
Type:	NTFS			
Drive:				
Date:	09/04/2024	17:20:26		
Current Fil	e			
Name:				
Size:	1.49 MB			
Status:				
Progress				
File	s Done:	115,687	of	122,564
Byte	s Done:	6.98 GB	of	8.44 GB
Time	: Taken:	00:48:22		Rate: 6247.2 KB/s
		Restored Files (9	4 %)	
		Restored Bytes (32 %)	
		Abort		

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

TBMR Recovery Status	
Formatted partition with drive letter E:, labelled 'DriveE' Formatted partition with drive letter H:, labelled " Formatted partition with drive letter C:, labelled 'WinOS' Formatted partition with drive letter B:, labelled " Formatted partition with drive letter F:, labelled 'DriveF' Creating partition mount points Creating volume mount points Making bootable volumes active Stopping access to Diskpart Successfully performed disk operations.	~
Restore will start shortly in a separate window. Backup images were restored successfully. The system files were restored successfully.	
Updating the target registry Copying boot files Success Sanity check passed Copying DisRec.ini to the Windows driveSuccess	
Starting Dissimilar Hardware. Searching for new hardware devices in the recovering system. No new devices were found in your system.	
Recovery Environment finished successfully on 2024-04-10T10:33:34+01:00	
	¥
Finish	

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 subfolder '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.

TBMR - Volume Layout			
The original and proposed d If required, right-click on a v			
Stored layout:		Proposed layout:	
	R2 ^		
Disk 0	Size 1023 MB [VMwa	Disk 0 Size 15.00 GB [٧N
Disk 1	Size 5.00 GB [VMwa		
Disk 2	Size 4.00 GB [VMwa		
Disk 3	Size 40.00 GB [VMw		
Disk 4	Size 1.00 GB [VMwa		
Disk 5	Size 10.00 GB [VMw		
Disk 6	Size 5.00 GB [VMwa 🗸		
<	>	<	>
		Icon Help	
		< Back Next > Cancel	

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

48

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

Tools	X
✻	 Load a driver Dissimilar hardware wizard Start VNC Set trace levels Advanced options
	 Start iSCSI initiator Copy Logfiles
	OK Close

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:

CAVC Trace Level	3	~	CNWC Trace Level	3
Avamar Trace Level			NetWorker Trace Level	
CBAC Trace Level DSMC Trace Level	3	~	CRAC Trace Level	3
CBMC Trace Level CRC Trace Level	3	~	CDP Trace Level	3 ~
CCHC Trace Level	3	~	CMI Trace Level	3 ~
CCSC Trace Level Simpana Trace Level	3	~	SM Trace Level SDS_FTP Trace Level SDS_TSM Trace Level	0 ~ 0 ~
CLCC Trace Level CLC Trace Level	3	~		

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.

Advanced options	×
WARNING: Do not change these settings unless directed to do so by Cristie support.	
Map disks automatically	
Update boot.ini	
Disable Compaq/HP services	
Edit Configuration	
Edit Dsm.Opt	
🗌 Skip Automatic Dissimilar Hardware	
Preserve Disk Signatures	
Restore local disks only	
OK Cancel	

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

50

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>.



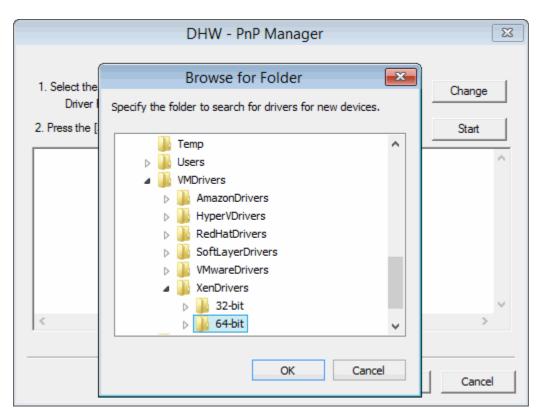
Select the 'Install Drivers using Plug-and-Play' option:



DHW - Select An Option	×
Select one of the following options and select [Next]	
Install Drivers using Plug-and-Play	
C Manually Install Drivers	
C Advanced Options	
< Back Next > Car	icel

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.



DHW - PnP Manager	×
 Select the folder where you have stored your Windows drivers Driver Path : X:\VMDrivers\XenDrivers\64-bit Press the [Start] button to start scanning. 	Change Start
	^
	~
<	>
< Back Finish	Cancel

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:

🔆 Found a new hardware!				
CBMR found a new hardware in your system.				
A matching driver "X:\VMDRIVERS\32-BIT\LSI_SCSI.INF" is found install this driver. Selecting [Install All] will install the matching drivers devices without prompting.				
Driver Path : X:\VMDRIVERS\32-BIT	Stop Searching Change Driver Path Search Again			
Install Install <u>A</u> ll <u>S</u> kip	Cancel			

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.

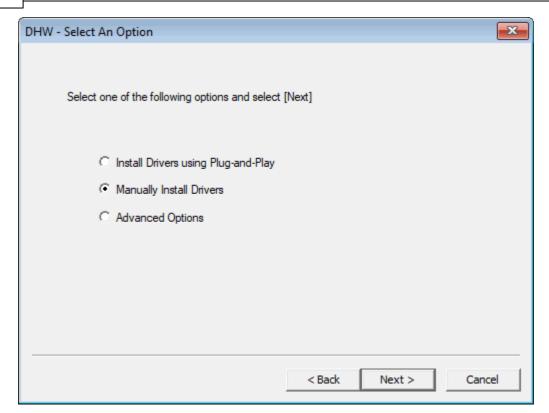
Once all of the drivers of the detected devices have been processed, the Wizard will indicate that the installation has finished. Click on Finish to proceed.

HW - PnP Manager	×
 Select the folder where you have stored your Windows drivers Driver Path : X:\VMDRIVERS\32-BIT Press the [Start] button to start scanning. 	Change Start
The following devices were found by the PnP manager:	<u>_</u>
Bus Class Description	
PCI SCSIAdapter SCSI Controller PCI Net Intel(R) PRO/1000 MT Network Connection	
Installing drivers for the newly found devices Installing driver for [SCSI Controller] Installed Installing driver for [Intel(R) PRO/1000 MT Network Connection] Skipped Finished installing drivers for the newly found devices.	×
< Back Finish	Cancel

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>.

DHW - Select A Driver			
Select an Installation File — Browse			
Select a manufacturer :			Ŧ
Select a driver :			
	< Back	Next >	Cancel

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.

TBMR User Guide

Ş

		Select a driver file			×
Organize 🔻	New folder			== +	
	Name	*		Date modified	Туре
	PV_SC	CSI		11/18/2014 2:36 AM	File folder
	<				>
	File name:		~	Driver installation files	~
				Open Ca	ncel

Here we are selecting the Citrix PV SCSI controller driver:

-	DHW - Select A Driver	×
Select an Installation File – Browse X:\VM	Drivers\XenDrivers\64-bit\PV_SCSI\oem2.inf	
Select a manufacturer :	Citrix Systems, Inc.	•
Select a driver :		
Citrix PV SCSI Host Adapter Citrix PV SCSI Host Adapter Citrix PV SCSI Host Adapter		
	< Back Next > Can	cel

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

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

DHW - Question 🛛 🕅
Do you want to install the selected driver?
Yes No

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.

DHW - Finish	x
The selected driver is successfully installed. If you want to install more drivers select the [Back] button and select the new drivers.	
If you are finished with the drivers, select [Finish] and the wizard will exit. You may now reboot th just recovering server for the changes to take effect.	e
< Back Finish Cance	el

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:

TBMR - Dynamic	Driver Loading	9		×
Specify the local found.	tion where the dr	iver instal	ation (.If	NF) file can be
				Browse
		ŀ	_ Ca	onfigure Network
	OK	Car	ncel	

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:

	TBMR - Information	×
i	Successfully loaded the driver [X:\VMDrivers\XenDrivers\64-bit\PV_SCSI\oem2.inf].	
	OK	

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.

TBMR - Copy Logfiles		— ×-
Specify a valid location where you ha the logfiles.	ave write permissio	on to store
Copy logfiles to the following location	c	
Q:\nigelp\Logs		Browse
OK	Cancel]

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.

IBMR - Logfiles				x
Highlight a file and select [View] to vie	wits contents., Se	elect [OK] to cl	ose this dialog	l.
Icon Name	Date	Time	Size	^
🗊 BCD.log	10/04/24	12:16:24	2 KB	
🗊 bmr_management.log	10/04/24	10:39:14	2 KB	
🗊 bmr_status.log	10/04/24	12:16:38	3 KB	
🗊 BmrManagementService.log	10/04/24	10:39:10	259	
🗊 CBAC_dump.log	10/04/24	12:16:12	2 KB	
🗊 CBAC_trace.log	10/04/24	12:16:14	47 KB	
🗊 Cbmrshl_Trace.log	10/04/24	10:39:20	2 KB	
🗊 CDP_dump(SP).log	10/04/24	11:26:24	8 KB	
🗊 CDP_dump.log	10/04/24	12:16:26	64 KB	
🗊 CDP_trace.log	10/04/24	12:16:30	488 KB	
CGBC_trace.log	10/04/24	12:16:40	60 KB	~
				_
View	Clos	e		

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

58

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

60

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....

🍯 Cristie Network Cor	nfigurator	- • •
Ethernet Adapters		
Intel(R) 8257	4L Gigabit Network Connection	· ~
Physical Addr:	00-0C-29-66-43-3D	Settings:
Speed:	Auto Negotiation	Update
Status:	Up	Disable
DNS Server (IPv6)	Network Identification	Map Network Drive
IPv4 Address	IPv6 Address	DNS Server (IPv4)
Obtain an IPv4 ad	dress automatically	
DHCP Details	Release	Renew
O Use the following	IPv4 address	
IPv4 Address: [More
Subnet Mask: [
Default Gateway: [10 . 0 . 1 . 100	More
Use statio	c gateway address	
0	K Apply	Cancel

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.



· · · · · · · · · · · · · · · · · · ·			
Intel(R) 82574L Gigabit Network Co	nnectio	n Properties	? 🗙
Advanced			
The following properties are available the property you want to change of value on the right. Property:			lick
Adaptive Inter-Frame Spacing Flow Control Gigabit Master Slave Mode Interrupt Moderation Interrupt Moderation Rate IPv4 Checksum Offload Jumbo Packet Large Send Offload V2 (IPv4) Large Send Offload V2 (IPv6) Locally Administered Address Log Link State Event Maximum Number of RSS Queues Packet Priority & VLAN Receive Buffers	~	Disabled	~
		ОК	Cancel

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:



Intel(R) 82574L Gigabit Network Co	nnection l	Properties 🔹 🔹
Advanced		
The following properties are availal the property you want to change of value on the right. Property:	on the left,	
Interrupt Moderation	<u>^</u>	Auto Negotiation V
Interrupt Moderation Rate IPv4 Checksum Offload Jumbo Packet Large Send Offload V2 (IPv4) Large Send Offload V2 (IPv6) Locally Administered Address Log Link State Event Maximum Number of RSS Queues Packet Priority & VLAN Receive Buffers Receive Side Scaling Speed & Duplex		1.0 Gbps Full Duplex 10 Mbps Full Duplex 10 Mbps Half Duplex 100 Mbps Full Duplex 100 Mbps Half Duplex Auto Negotiation
TCP Checksum Offload (IPv4)	<u> </u>	OK Cancel

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.

🍯 Cristie Network Co	nfigurator	- • •
Ethernet Adapters		
Intel(R) 8257	4L Gigabit Network Connection	~
Physical Addr:	00-0C-29-66-43-3D	Settings:
Speed:	Auto Negotiation	Update
Status:	Up	Disable
DNS Server (IPv6)	Network Identification	Map Network Drive
IPv4 Address	IPv6 Address	DNS Server (IPv4)
Obtain an IPv4 ad	dress automatically	
DHCP Details	Release	Renew
OUse the following	IPv4 address	
IPv4 Address:	10 . 10 . 11 . 66	More
Subnet Mask:	255.0.0.0	
Default Gateway:	10 . 0 . 1 . 100	More
Use stati	c gateway address	
0	K Apply	Cancel

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.

🍯 Cristie Network Conf	ligurator	- • •
Ethernet Adapters		
Intel(R) 82574L	. Gigabit Network Connection	n v
Physical Addr:	00-0C-29-66-43-3D	Settings:
Speed:	Auto Negotiation	Update
Status:	Up	Disable
IPv4 Address	IPv6 Address	DNS Server (IPv4)
DNS Server (IPv6)	Network Identification	Map Network Drive
Map a network drive Drive: Q: Network Path: Domain\Username: Password:	software \nigelp	Map Drive
Unmap a network drive	~	Unmap Drive
OK	Apply	Cancel

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

66

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.

🍯 Cristie Network Cont	figurator	
Ethernet Adapters		
Intel(R) 82574	Gigabit Network Connection	n ~
Physical Addr:	00-0C-29-66-43-3D	Settings:
Speed:	Auto Negotiation	Update
Status:	Up	Disable
IPv4 Address	IPv6 Address	DNS Server (IPv4)
DNS Server (IPv6)	Network Identification	Map Network Drive
Map a network drive Drive: A: Network Path: Domain\Username Password:	:	Map Drive
Unmap a network drive Q: \\10.1.1.60\test-s Q: \\10.1.1.60\test-s		Unmap Drive
ОК	Apply	Cancel

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.

Ethernet Adapters	-	
	574L Gigabit Network Connection	~
Physical Addr:		
Priysical Addr:	00-0C-29-66-43-3D	Settings:
Speed:	Auto Negotiation	Update
Status:	Up	Disable
DNS Server (IPv6)	Network Identification	Map Network Drive
IPv4 Address	IPv6 Address	DNS Server (IPv4)
DNS Server:		

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

68

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.

🍯 Cristie Network Co	nfigurator					
Ethernet Adapters						
Intel(R) 8257	4L Gigabit Network Connection	~				
Physical Addr:	00-0C-29-66-43-3D	Settings:				
Speed:	Auto Negotiation	Update				
Status:	Up	Disable				
IPv4 Address	IPv6 Address	DNS Server (IPv4)				
DNS Server (IPv6)	Network Identification	Map Network Drive				
Hostname:	Win2022-DR	Set				
E	Example: 'microsoft.com' ninint-ipn4eof					
0	K Apply	Cancel				

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.

Cristi	stie Route Congigurator										
	Interface list										
Intel(R) 82574L Gigabit Network Connection											
F	- hysi	ical Addres	s: 00)-0C-29-93-9D-C	9						
	IP۱	/4 Routes	IPv6 Route	es Diagnostics							
		Network I	Destination	Netmask	Gateway	Interfa	ace Metric				
		0.0.0.0		0.0.0.0	10.0.1.100						
		10.0.0.0		255.0.0.0	On-link	10.1.8					
		10.1.8.2		255.255.255.2		10.1.8					
			55.255			10.1.8					
		224.0.0.0		240.0.0.0 255.255.255.2	On-link	10.1.8 10.1.8					
		20012001	200.200	2001200120012		101110					
			Add a rout	e	Delete a rout	te	Edit a route				
				ОК		Car	ncel				

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.



70	Bare Machine Recovery for IBM Spectrum Protect
----	--

Add a route					×
Network Destination	10 . 10).	1	. 1	
Netmask	255 . 25	5.	0	. 0	
Gateway	10 . 0	•	1	. 100	
Interface	10 . 1		8	. 214	ł
Metric	32	7			_
		_			
Click 'Save' to	add this route	e, or	'Car	ncel' to	not add this route
s	ave			C	ancel

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.

Delete a route	
Network Destination	10 . 1 . 8 . 214
Netmask	255 . 255 . 255 . 255
Gateway	0.0.0.0
Interface	10 . 1 . 8 . 214
Metric	256
	Do you wish to delete this route?
	Yes No

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.



Edit a route		×
Network Destination	10 . 1 . 8 . 214	
Netmask	255 . 255 . 255 . 255	
Gateway	0.0.0	
Interface	10 . 1 . 8 . 214	
Metric	256	
Click 'Save' to cha	nge this route, or 'Cancel' to not change this route	
S	Save Cancel	

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.

Cristie	e Route Cong	igurator					-X			
	Interface list									
	Intel(R) 82574L Gigabit Network Connection									
F	Physical Addres	s: 00-0	C-29-93-9D-0	.9						
		I								
	IPv4 Routes	IPv6 Routes	Diagnostics							
	Metric	Network Des	tination		Gateway					
	281	::/0	anadon		fe80::290:7fff	:fedc:85ae				
	281	fe80::/64			On-link					
	281 281		5129:ac8b:2ft	0/128	On-link On-link					
	281	ff00::/8			UnHink					
		Add a route		Delete a r	oute	Edit a route				
	L	,		Delete di						
		L	OK	1	Ca	ancel				

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.

Add a route		×
Metric	32	
Subnet Prefix Length	128	
Network Destination	fe80::a95a:5822:7bda:7200]
Gateway	::]
Click 'Save' to	add this route, or 'Cancel' to not add this route	
	Cancel	

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.

Delete a route		×
Metric	281	
Subnet Prefix Length	0	
Network Destination	::	
Gateway	fe80::290:7fff:fedc:85ae	
	Do you wish to delete this route?	
	Yes No	

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.

Edit a route		×
Metric	281	
Subnet Prefix Length	0	
Network Destination	::	
Gateway	fe80::290:7fff:fedc:85ae	
Click 'Save' to cha	ange this route, or 'Cancel' to not change this route	
	Save Cancel	

6.2.6.3 Diagnostics

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

Cristie Route Congigurator	— X
Interface list	
Intel(R) 82574L Gigabit Network Connection	
Physical Address: 00-0C-29-93-9D-C9	
IPv4 Routes IPv6 Routes Diagnostics	
Enter hostname or IP address to check IPv6	
l tracert ping	
~	
OK	

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



Cristie Route Co	ngigurator	X
Interface lis	st	
田田	Intel(R) 82574L Gigabit Network Connection	~
Physical Add	dress: 00-0C-29-93-9D-C9	
IPv4 Rout	tes IPv6 Routes Diagnostics	
Ent	er hostname or IP address to check IPv4 IPv6	
10	. 10.2.84 tracert ping	
1	acing route to TSM817 [10.10.2.84] er a maximum of 30 hops: . <1 ms <1 ms <1 ms TSM817 [10.10.2.84] ace complete.	<hr/>
	OK Cancel	

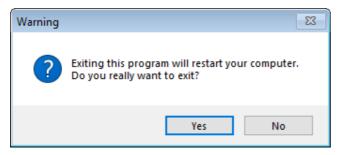
Click ping to check connectivity to the selected host. Click OK to exit the dialogue.

Interface list Intel(R) 82574L Gigabit Network Connection Physical Address: 00-0C-29-93-9D-C9 IPv4 Routes IPv6 Routes Diagnostics Enter hostname or IP address to check Inter hostname or IP address to check Pinging 10.10.2.84 with 32 bytes of data: Reply from 10.10.2.84: bytes=32 time < Ims TTL = 128 Reply from 10.10.2.84: bytes=32 time < Ims TTL = 128 Reply from 10.10.2.84: bytes=32 time < Ims TTL = 128 Reply from 10.10.2.84: bytes=32 time < Ims TTL = 128 Ping statistics for 10.10.2.84: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Intel(R) 82574L Gigabit Network Connection Physical Address: 00-0C-29-93-9D-C9 IPv4 Routes IPv6 Routes Diagnostics Enter hostname or IP address to check I0.10.2.84 With 32 bytes of data: Reply from 10.10.2.84: bytes=32 time<1ms TTL=128
Physical Address: 00-0C-29-93-9D-C9 IPv4 Routes IPv6 Routes Enter hostname or IP address to check IPv4 O IPv6 10.10.2.84 tracert Pinging 10.10.2.84 with 32 bytes of data: Reply from 10.10.2.84: bytes=32 time < Ims TTL=128
IPv4 Routes IPv6 Routes Diagnostics Enter hostname or IP address to check IPv4 IPv6 10.10.2.84 tracert ping Pinging 10.10.2.84 with 32 bytes of data: Reply from 10.10.2.84: bytes=32 time < Ims TTL=128 Reply from 10.10.2.84: bytes=32 time < Ims TTL=128 Ping statistics for 10.10.2.84: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Enter hostname or IP address to check Inter hostname or IP address to check address
10.10.2.84 ● IPv4 ○ IPv6 10.10.2.84 tracert pinging 10.10.2.84 with 32 bytes of data: Reply from 10.10.2.84: bytes=32 time<1ms TTL=128
Pinging 10. 10.2.84 with 32 bytes of data: Reply from 10. 10.2.84: bytes=32 time<1ms TTL=128
Reply from 10.10.2.84: bytes=32 time<1ms TTL=128 Reply from 10.10.2.84: bytes=32 time<1ms TTL=128 Reply from 10.10.2.84: bytes=32 time<1ms TTL=128 Reply from 10.10.2.84: bytes=32 time<1ms TTL=128 Ping statistics for 10.10.2.84: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Reply from 10.10.2.84: bytes=32 time<1ms TTL=128 Reply from 10.10.2.84: bytes=32 time<1ms TTL=128 Reply from 10.10.2.84: bytes=32 time<1ms TTL=128 Reply from 10.10.2.84: bytes=32 time<1ms TTL=128 Ping statistics for 10.10.2.84: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Reply from 10.10.2.84: bytes=32 time<1ms TTL=128 Ping statistics for 10.10.2.84: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
↓
OK Cancel

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

76

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:

News					Constitut		-	
Name					Capacity			e Space
Pool-A					8.97 GB			72 GB
Pool-B					18.97 GB		14	.97 GB
tored Virtual Disks (1) Name	Layout	Provi	sioning	Сарас	tity	Allocate	d	Volume
Pool-A-Disk0	Simple	Thin	sioning	5.00 (768.00	-	E:
tored Physical Disks (1)			Propo	osed Phy	sical Disks ((0)		
	Capacity		Bus	Usage	2	c	hassis	Media Type
Name								SSD
Name VMware Virtual SATA Hard	5.00 GB		SATA	Auton	nauc	S	ata0	000

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



77

Storage Pool Virtu	ual Disk —						
Name	Pool-A-Dis	k0					
Layout	Simple						
Provisioning	Thin						
Capacity	5.00 GB						7
Allocated	768.00 MB	}					=
Volume	E:						5
VMware Virtual S/	ATA Hard	5.00 GB	SATA	Automatic	sata0	SSD	
		5.00 GB	SATA	Automatic	sataO	SSD	
oposed Physical	Disks (2)						
oposed Physical Name	Disks (2)	5.00 GB Capacity 10.00 GB	SATA Bus SAS	Automatic Usage Automatic	sata0	SSD Media Type SSD	^
VMware Virtual S/ oposed Physical Name] PhysicalDisk1] PhysicalDisk2	Disks (2)	Capacity	Bus	Usage		Media Type	
oposed Physical Name] PhysicalDisk1	Disks (2)	Capacity 10.00 GB	Bus SAS	Usage Automatic		Media Type SSD	^

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.

Boot Manager	
Boot normally EFI UMware Virtual SCSI Hard Drive (0.0) EFI UMware Virtual SATA CDROM Drive (1.0) EFI Network EFI Internal Shell (Unsupported option) Enter setup Reset the system Shut down the system	Continue to boot using the default boot order.
↑↓=Move Highlight <enter>=Select Entry Default EFIbios</enter>	



79

Boot Manager	
Boot normally EFI UMware Virtual SCSI Hard Drive (0.0) EFI UMware Virtual SATA CDROM Drive (1.0) EFI Network EFI Internal Shell (Unsupported option) Enter setup Reset the system Shut down the system	Configure the firmware boot environment and options.
↑↓=Move Highlight <enter>=Select Entry</enter>	

Select Enter Setup option

	Boot Maintenance Manag	ler
Configure boot options Configure drivers Boot from a file		Manipulate the list of installed OSes and bootable devices
Configure screen size		
Exit the Boot Maintena	nce Manager	
†∔=Move Highlight	<enter>=Select Entry</enter>	Esc=Exit

Select Configure boot options



80

	Configure boot opt	ions
Add boot option Delete boot option Enable or disable boot o Change boot order Go back to Boot Maintena		Add EFI application or removable media as boot option
†↓=Move Highlight	<enter>=Select Entry</enter>	

Select add boot option

NO UOLUME LABEL, [PciRoot(0x0)/Pci(0x15,0x0)/Pci(0x0,0x0)/Scsi(0x0, 0x0)/HD(1,GPT,571AEA8F-B441-4ECD-9FA1-8F1BCB892D) C8,0x800,0x32000)1 Load File [PciRoot(0x0)/Pci(0x16,0x0)/Pci(0x0,0x0)/MAC(000C) 296DC12E,0x0)/IPu4(0.0.0.0,0x0,DHCP,0.0.0.0,0.0.0,0.0) 0,0.0.0.0] Load File [PciRoot(0x0)/Pci(0x16,0x0)/Pci(0x0,0x0)/MAC(000C) 296DC12E,0x0)] Load File [PciRoot(0x0)/Pci(0x16,0x0)/Pci(0x0,0x0)/MAC(000C) 296DC12E,0x0)] Load File [PciRoot(0x0)/Pci(0x16,0x0)/Pci(0x0,0x0)/MAC(000C) 296DC12E,0x0)/IPu6(0000:0000:0000:0000:0000:0000:0000): 0000:0000,0x0,Static,0000:0000:0000:0000:0000:0000 0:0000:0000,0x40,0000:0000:0000:0000:000
Load File IPciRoot(0x0)/Pci(0x16,0x0)/Pci(0x0,0x0)/MAC(000C 296DC12E,0x0)/IPv4(0.0.0,0x0,DHCP,0.0.0.0,0.0.0 .0,0.0.0.0] Load File IPciRoot(0x0)/Pci(0x16,0x0)/Pci(0x0,0x0)/MAC(000C 296DC12E,0x0)] Load File IPciRoot(0x0)/Pci(0x16,0x0)/Pci(0x0,0x0)/MAC(000C 296DC12E,0x0)/IPv6(0000:0000:0000:0000:0000:0000 296DC12E,0x0)/IPv6(0000:0000:0000:0000:0000:0000 0000:0000,0x0,Static,0000:0000:0000:0000:0000 0:0000:0000,0x40,0000:0000:0000:0000:000
0:0000:0000,0x40,0000:0000:0000:0000:000

Select boot partition in File Explorer



81

	File Explorer	
1	(more) 1	
<nb-no></nb-no>		
<nl-nl></nl-nl>		
<pl-pl></pl-pl>		
<pt-br></pt-br>		
<pt-pt></pt-pt>		
<pre><qps-ploc></qps-ploc></pre>		
<ro-ro></ro-ro>		
<ru-ru></ru-ru>		
<sk-sk></sk-sk>		
<sl-si></sl-si>		
<pre><sr-latn-cs></sr-latn-cs></pre>		
<pre><sr-latn-rs></sr-latn-rs></pre>		
<su-se></su-se>		
<tr-tr></tr-tr>		
<ur><uk-ua></uk-ua></ur>		
<zh-cn></zh-cn>		
<zh-hk></zh-hk>		
<zh-t₩></zh-t₩>		
bootmgfw.efi		
bootmgr.efi		
memtest.efi		
†∔=Move Highlight	<enter>=Select Entry</enter>	Esc=Exit

Select EFI boot image

	Modify Boot Option Des	cription
bootmgfw.efi		Commit changes and exit
Input the description Input optional data		
Commit changes and ex Discard changes and ex		
†↓=Move Highlight	<enter>=Select Entry</enter>	Esc=Exit

Modify boot option description and commit



82

Boot Manager	
Boot normally EFI UMware Virtual SCSI Hard Drive (0.0) EFI UMware Virtual SATA CDROM Drive (1.0) EFI Network EFI Internal Shell (Unsupported option) Boot0004 Enter setup Reset the system Shut down the system	Device Path: PciRoot(0x0)/Pci(0x15,0x 0)/Pci(0x0,0x0)/Scsi(0x0 ,0x0)/HD(1,GPT,571AEA8F- B441-4ECD-9FA1-8F1BCB892 DC8,0x800,0x32000)/\EFI\ Microsoft\Boot\bootmgfw. efi
↑↓=Move Highlight <enter>=Select Entry</enter>	
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	<u>sales@cristie.com</u>
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 <u>www.cristie.com/support/</u>

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.

