



TBMR For Linux

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 Avamar are trademarks of the Dell EMC Corporation.*
- *vSphere, vCenter and vCloud are trademarks of VMware Inc.*
- *Hyper-V is a trademark of Microsoft Corporation.*
- *Azure is a trademark of Microsoft Corporation.*
- *Amazon Web Services (AWS) and Amazon Elastic Compute Cloud (EC2) are trademarks of Amazon.com, Inc.*
- *Cohesity DataProtect is a trademark of Cohesity Inc.*
- *Rubrik is a trademark of Rubrik Inc.*
- *CloneManager® is a registered trademark of Cristie Software Ltd.*
- *SysBack is a registered trademark of Cristie Software Ltd.*

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

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

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



Contents

1	Document Conventions	4
2	Introduction	5
	2.1 Limitations	5
	2.2 Further Information	5
3	System Requirements	6
4	Supported Filesystems	7
5	uEFI and MBR BIOS Support	8
6	Using TBMR For Disaster Recovery	9
	6.1 Saving the System Configuration	9
	6.2 TBMRcfg	9
	6.3 Creating a TBMRcfg Pre-Schedule	11
	6.4 Transitional Nodes	12
7	Spectrum Protect Client Backup	13
	7.1 Housekeeping	13
8	Performing a Recovery	14
	8.1 Build Custom ISO	26
	8.2 Command Line Recoveries	29
9	Post Recovery Options	31
	9.1 Show Log Files	31
	9.2 Copy Log Files	31
10	Cristie Technical Support	35



1 Document Conventions

The following typographical conventions are used throughout this guide:

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



2 Introduction

Bare Machine Recovery for IBM Spectrum Protect provides disaster recovery capability for Spectrum Protect protected Linux Intel hosts.

It is possible to recover the original system to the same or dissimilar hardware. To protect a system, backups can be taken periodically, along with configuration information, which includes details of hard disks, network interfaces, etc.

This Guide shows the user how to save system configuration information, backup and recover a Linux Intel machine using TBMR. More detailed information is available from `man` pages for the TBMR components. The `man` pages are available after installation of TBMR.

This guide relates to TBMR for Linux Intel version 9.6.1 only.

Note: TBMR can only be used in conjunction with IBM Spectrum Protect.

This guide describes how to:

- *Save Configuration data using `tbmrcfg`*
- *Configure and run your IBM Spectrum Protect Client backup*
- *Perform a Disaster Recovery*

2.1 Limitations

There are limits to what this version of TBMR for Linux Intel will support. It will NOT support:

- *Platforms other than Intel 64-bit only.*
- *Multi-boot operating systems*
- *Recovery of files that are being written to at the time of backup.*

2.2 Further Information

Further information and advice on using TBMR may be found in the **Cristie Knowledge Base** (<https://kb.cristie.com>) or the **Cristie Forum** (<https://forum.cristie.com>).



3 System Requirements

TBMR for Linux Intel can only be installed on a x86_64 Linux Intel (i.e. 64-bit) machine.

TBMR requires that Spectrum Protect BA client version 7.1 or later is already installed.

A minimum memory of **6 GB RAM** is required for booting the recovery environment and running a recovery.

Please refer to this web page <https://www.cristie.com/support/matrix/> to determine the latest OS and IBM Spectrum Protect client/server support for TBMR Version 9.6.1.

Before TBMR can be used it must also be correctly licensed. Cristie provides a 30 day trial license with the product.



4 Supported Filesystems

Please refer to this web page <https://www.cristie.com/support/matrix/> to determine the latest file system support for TBMR Version 9.6.1.



5 uEFI and MBR BIOS Support

Note: recovery support is provided for conversion from uEFI to MBR BIOS. Conversion from legacy MBR BIOS to uEFI is not currently supported.

The recovery ISO is configured for both MBR (legacy) and uEFI boot. It can therefore boot into either environment. There are no special considerations that need to be made by the customer for uEFI machines. If your machine boots with elilo, prior to performing a backup please run:-

```
tbmrcfg -b elilo
```

All Cristie Bare Metal Recovery software handles the recreation of the uEFI partitions during the recovery of the machine, this is transparent to the user.

When recovering an uEFI enabled OS you must recover to uEFI capable hardware.

When recovery is to a different machine, you may need to manually configure the uEFI boot stanza in order to boot the recovered uEFI OS. Please refer to the Cristie Knowledgebase for further information on editing the boot stanza.

Note: when recovering an uEFI enabled OS, it is recommended that the recovery environment is booted in uEFI mode.



6 Using TBMR For Disaster Recovery

This section describes the steps involved in using Spectrum Protect in conjunction with TBMR for disaster recovery.

This description assumes that the Spectrum Protect client software has already been installed and configured correctly.

To ensure your system is protected observe the following steps:

1. *Install TBMR on the system you wish to protect.*
2. *Use the `tbmr cfg` program to capture and store the configuration of the system.*
3. *Use the Spectrum Protect Backup/Archive Client to backup the system to your IBM Spectrum Protect server as usual.*

6.1 Saving the System Configuration

Configuration is always saved to **/TBMR CFG** - it can't be saved anywhere else. This guarantees it is always stored in the backup.

When saving the configuration information to the backup location, this must be done **before** the backup is run.

To save the configuration information for each machine, the supplied command line program `tbmr cfg` is used. It is recommended that this is run prior to running each backup to ensure the configuration is up to date.

6.2 TBMRcfg

To use the command line configuration saving program, type `tbmr cfg`. The configuration will automatically detect the machine boot loader and boot partition, however, if either are incorrectly detected you may specify additional options.

The available options of `tbmr cfg` can be shown using:

```
tbmr cfg --help
```

Some examples are shown here:

To save configuration information from a machine that boots using *grub* installed on `/dev/sda` to the backup location, use:

```
tbmr cfg -b grub -d /dev/sda
```

To save configuration information from a machine that boots using *grub* installed on `/dev/hda`, use:

```
tbmr cfg -b grub -d /dev/hda
```

There is a full manual page for `tbmr cfg` available by typing `man tbmr cfg`.



This is a full list of options:

Option	Description
-b<name>, --bootloader=<name>	Set boot loader to <name> (default is grub)
-d<name>, --bootdevice=<name>	Set boot device name to <name>
-l<file>, --logfile=<file>	Set log file (default is cbmrcfg.log)
-o<file>, --output=<file>	Set output file (default is disrec.ini)
-p<permissions>	Set output file permissions (default 0600)
-v, --verbose	Verbose mode
--autorelabel=<n>	Automatically relabel SELinux if <n> != 0
--cobmr_boot_backup	CoBMR only. Intended to be used where the system is backed up using Cohesity's block based backup. Cohesity only snapshots LVM partitions and in most cases '/boot' will be on a standalone partition and be missed. This switch will perform a simple TAR based backup of '/boot' and put it in '/COBMRCFG' so it's included in the backup.
Note: It should never be on for standard file based backups	
--disk_pattern=<pattern>	Only include disks matching <pattern>
--disk_regex=<regex>	Only include disks matching <regex>
--disk_skip=<pattern>	Don't include disks matching <pattern>
--disk_skip_regex=<regex>	Don't include disks matching <regex>
--disshw=<n>	Use dissimilar hardware support if <n> != 0
--filedev_mount_options=<string>	Set file device mount options
--filedev_mount_target=<string>	Set file device mount target
--format_pattern=<pattern>	Only format devices matching <pattern>
--format_regex=<regex>	Only format devices matching <regex>
--format_skip=<pattern>	Don't format devices matching <pattern>
--format_skip_regex=<regex>	Don't format devices matching <regex>
--mpath=<n>	Don't scan for mpath devices if <n> = 0
--partition_pattern=<pattern>	Only partition devices matching <pattern>
--partition_regex=<regex>	Only partition devices matching <regex>
--partition_skip=<pattern>	Don't partition devices matching <pattern>
--partition_skip_regex=<regex>	Don't partition devices matching <regex>
--local_fs	Don't include remote filesystems
--local_disks	Don't include remote disks, e.g. iscsi
--rc=<n>	Set return code to <n>
--rescale_pattern=<pattern>	Only rescale devices matching <pattern>
--rescale_regex=<regex>	Only rescale devices matching <regex>
--rescale_skip=<pattern>	Don't rescale devices matching <pattern>
--rescale_skip_regex=<regex>	Don't rescale devices matching <regex>
--save_mpath_list	Save mpath details
--vg_pattern=<pattern>	Only create VGs matching <pattern>



<code>--vg_regex=<regex></code>	Only create VGs matching <regex>
<code>--vg_skip=<pattern></code>	Don't create VGs matching <pattern>
<code>--vg_skip_regex=<regex></code>	Don't create VGs matching <regex>
<code>--help, --usage</code>	Print this message and exit
<code>--version</code>	Print the version and exit

6.3 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` as a pre-schedule command for your Linux Spectrum Protect TSM incremental backups, you need to add a line to your `dsm.sys`, and create the script on the system you are protecting.

Please make sure your Spectrum Protect TSM backups are being run as a user with Root access.

Create a script called `tbmrcfg.sh` and copy it to `/etc/cbmr/` with the content below:

```
SHELL=/bin/bash
PATH=/usr/local/bin:/usr/local/sbin:/usr/bin:/usr/sbin:/bin:/sbin:/root/bin:
tbmrcfg
```

Modify `/opt/tivoli/tsm/client/ba/bin/dsm.sys`: and add the content below

```
PRESCHEDULECMD '/etc/cristie/tbmrcfg.sh'
```

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

To find the `PATH` variable of your Linux system run the below in a terminal

```
$PATH
```

e.g.

```
-bash-4.2# $PATH
-bash: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin: No such file or directory
-bash-4.2#
```

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



6.4 Transitional Nodes

If you backup to a node located on a Spectrum Protect Server version 7.1.8 or 8.1.2 and above, using a Spectrum Protect client 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 than 8.1.2 that enforces TLS communication. This will prevent older Spectrum Protect clients from accessing the node after the client has enabled TLS on the node.

You can change the Session Security by updating the node with the command:

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



7 Spectrum Protect Client Backup

If the backup is to be written using Spectrum Protect BA client, the `dsm.sys` file should be configured.

The default location for the Spectrum Protect BA client option file is:

```
/opt/tivoli/tsm/client/ba/bin/dsm.sys
```

This file should be edited to point to the Spectrum Protect server to be used:

```
SErvername server_a
      COMMmethod      TCPip
      TCPPort          1500
      TCPServeraddress 10.2.1.20
```

The Spectrum Protect BA client should be configured to backup all files which are required for OS recovery.

For **btrfs** file system support only, it is recommended to add the following line to `dsm.sys` to exclude the snapshot directories (unless they are required):

```
exclude.dir /.snapshots/*/snapshot
```

7.1 Housekeeping

In order to ensure that you can recover to the latest version of the operating system that was installed on your Linux Intel machine, you must ensure that a Spectrum Protect incremental backup is performed every time the operating system files change.

This is not always possible, so **Cristie Software Ltd.** recommends that the Spectrum Protect incremental backup be performed regularly. However, you should choose a period which reflects the rate of change of data in your own organisation. Although the configuration data will change less frequently than the operating system, it is a wise precaution to update this regularly. For example, this can be achieved by creating a cron job for your schedule or using the Spectrum Protect Scheduler.



8 Performing a Recovery

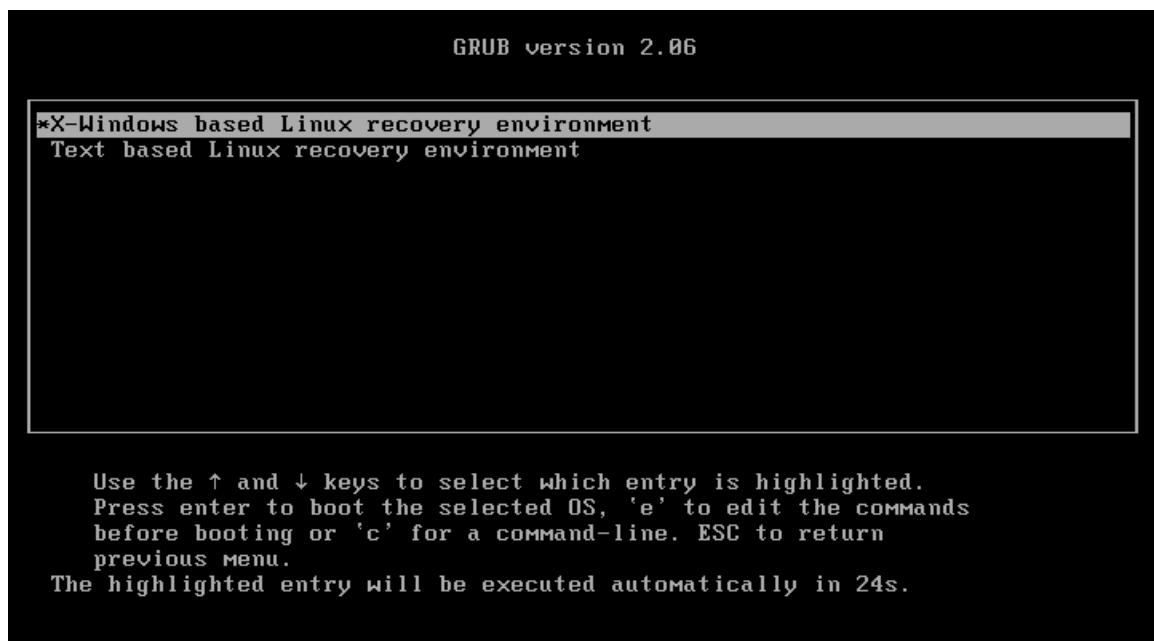
When a machine has failed, it can be recovered using the XBMR bootable product CD/DVD-ROM or DR ISO (if your host supports this capability). XBMR is a separate product to TBMR. It is a generic Recovery Environment for all Cristie Linux BMR products.

You should ensure your machine's BIOS is set up to boot from CD/DVD-ROM or ISO as appropriate.

The process encompasses the following stages:

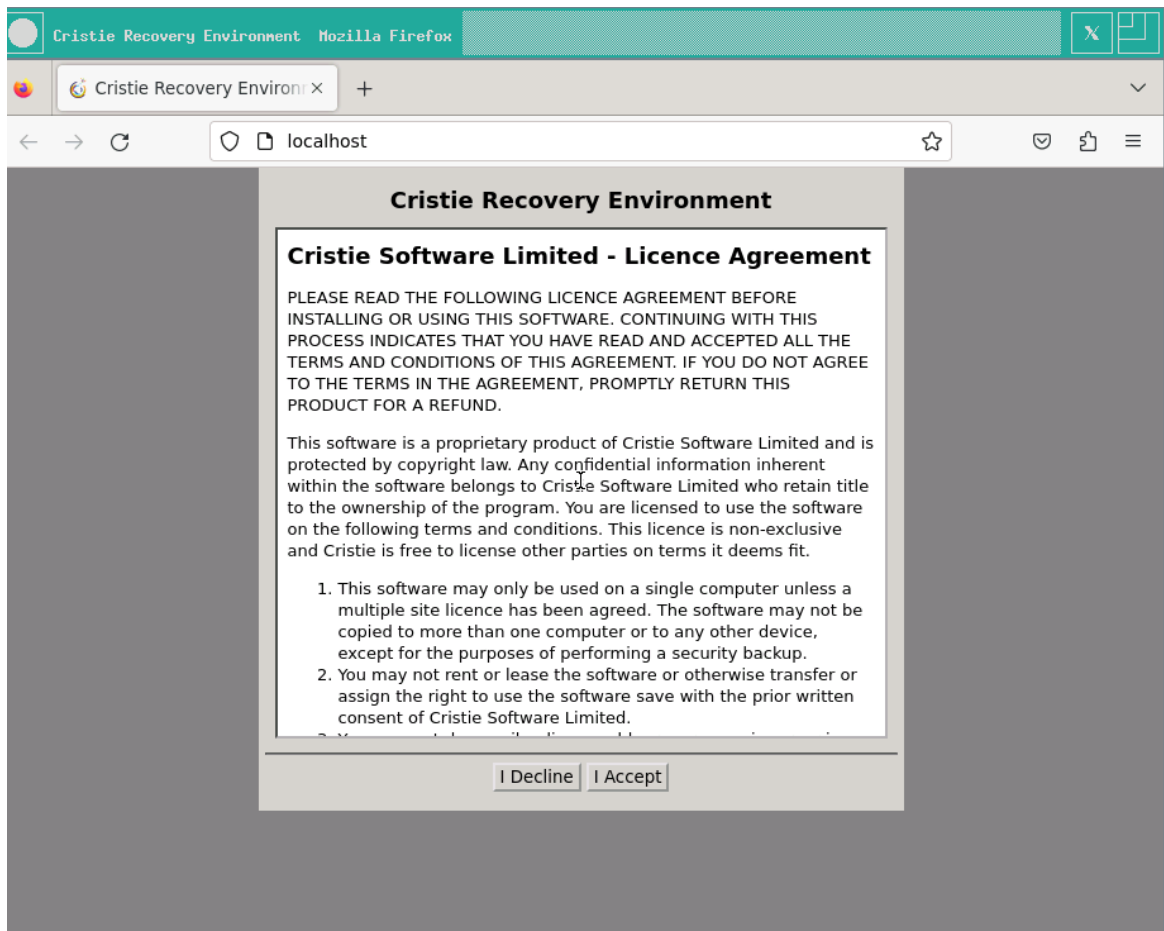
- **Boot** into XBMR Recovery Environment and configure as required
- **Read** Configuration Data from your backup
- **Restore** Files from your backup
- **Load** additional drivers (if necessary)
- **Reboot** into recovered OS

Boot the machine using the **XBMR** bootable CD ROM or ISO. You will then be presented with the screen below:



Cristie recommends that you choose the graphical X-Windows recovery environment mode which loads the **Cristie Recovery Environment**. You will be presented with the **license** screen. Click **Accept** if you agree with the licencing terms.





The Product Selection drop-down menu will then be shown. Now select the Cristie product used during the backup - TBMR in this case.



Click **OK**. You will then see the **TBMR Recovery Environment** main menu.





Cristie recommends selecting the **Automatic Recovery Wizard** option from the **Recovery Environment** main menu. This will then display the **Setup TBMR Location** dialogue box, where you can specify the IBM Spectrum Protect Server information.

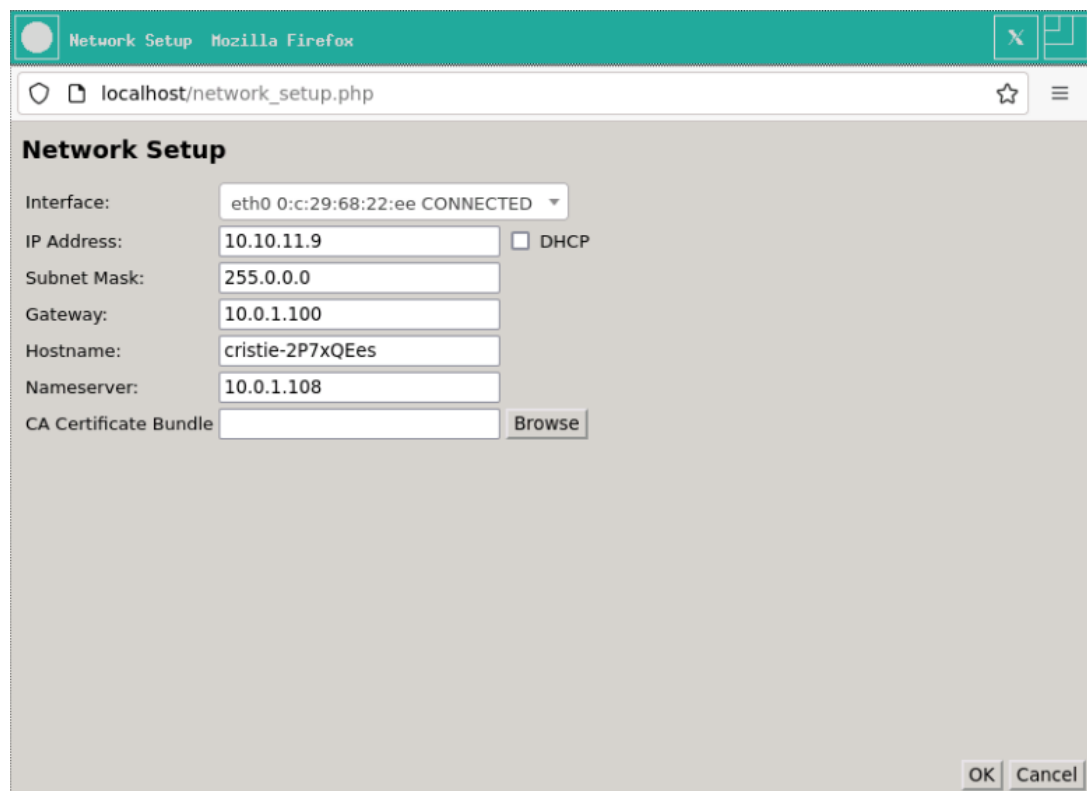
The screenshot shows a web browser window titled 'Mozilla Firefox' with the address 'localhost/tbmr_setup_location.php'. The page is titled 'Setup TBMR Location' and includes a star icon. Below the title, it says 'Provide TSM Server information.' and 'This wizard will take you through the steps to fully recover your system from a backup.' The form contains several input fields: 'Server Address*' with the value '10.10.2.84', 'Port*' with the value '1501', 'Certificate' with the value '/mnt/certificate/nigelp/TSM-Ce' and a 'Browse' button, 'Node Name*' with the value 'np-rhel9' and a 'Browse' button, and 'Password*' with masked characters and an 'Encryption Keys' button. There is also a 'Network Setup' button. At the bottom right, there are 'Next >' and 'Cancel' buttons.

Now enter the Server details (of the IBM Spectrum Protect Server where the backup resides). Enter the Server IP address and port (1500 is the default). For IBM Spectrum Protect server version 8.1.2 you may need to set a TLS encryption certificate. Otherwise leave that field blank. Finally enter the Node name and password. If required, it is possible to view the nodes on the server by clicking the [Browse](#) button next to the **Node Name**.

Note: You need to enter the administrative details for the Spectrum Protect Server into the Node Name and Password fields to achieve this.

Contact your IBM Spectrum Protect administrator if you are unsure of any of the settings.

If it is required to configure the local network settings (i.e. the XBMR Recovery Environment), click the [Network Setup](#) button. Now enter your new network settings.

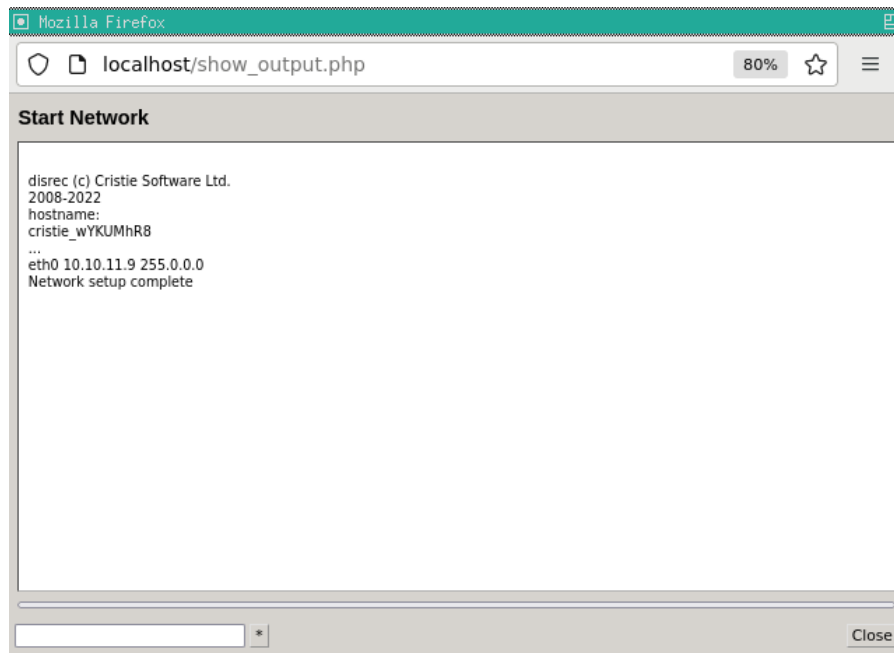


The screenshot shows a web browser window titled "Network Setup Mozilla Firefox" with the address bar displaying "localhost/network_setup.php". The main content area is titled "Network Setup" and contains the following fields and controls:

- Interface: A dropdown menu showing "eth0 0:c:29:68:22:ee CONNECTED".
- IP Address: A text input field containing "10.10.11.9".
- Subnet Mask: A text input field containing "255.0.0.0".
- Gateway: A text input field containing "10.0.1.100".
- Hostname: A text input field containing "cristie-2P7xQEes".
- Nameserver: A text input field containing "10.0.1.108".
- CA Certificate Bundle: A text input field with a "Browse" button next to it.
- A checkbox labeled "DHCP" is located to the right of the IP Address field.
- At the bottom right, there are "OK" and "Cancel" buttons.

Select [OK](#) to save your changes. The Start Network screen will then display the network changes being implemented.





Click **Close** to return to the **Setup TBMR Location Wizard**. Now click **Next >** and the **Get Configuration** dialogue will be shown. Entering a recovery date and time will restore an available backup nearest (but earlier) to the specified date/time.

A screenshot of a Mozilla Firefox browser window showing the 'Get Configuration' page. The address bar shows 'localhost/tbmr_restore_configuration.php'. The page title is 'Get Configuration'. Below the title, it says 'Specify the restore settings here.' There are four input fields: 'Recovery Date' with a placeholder '(mm/dd/yyyy)', 'Recovery Time' with a placeholder '(HH:MM:SS)', 'DSMC Options', and 'Logging' with a dropdown menu set to 'Normal'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

If you wish to recover a backup other than the latest (the default) select a particular date/time - a Point-in-Time (PIT). Click the Date field and a calendar will pop-up like this:



Get Configuration

Specify the restore settings here.

Recovery Date (mm/dd/yyyy)

Recovery Time H:MM:SS

DSMC Options

Su	Mo	Tu	We	Th	Fr	Sa
			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				

< Back Next > Cancel

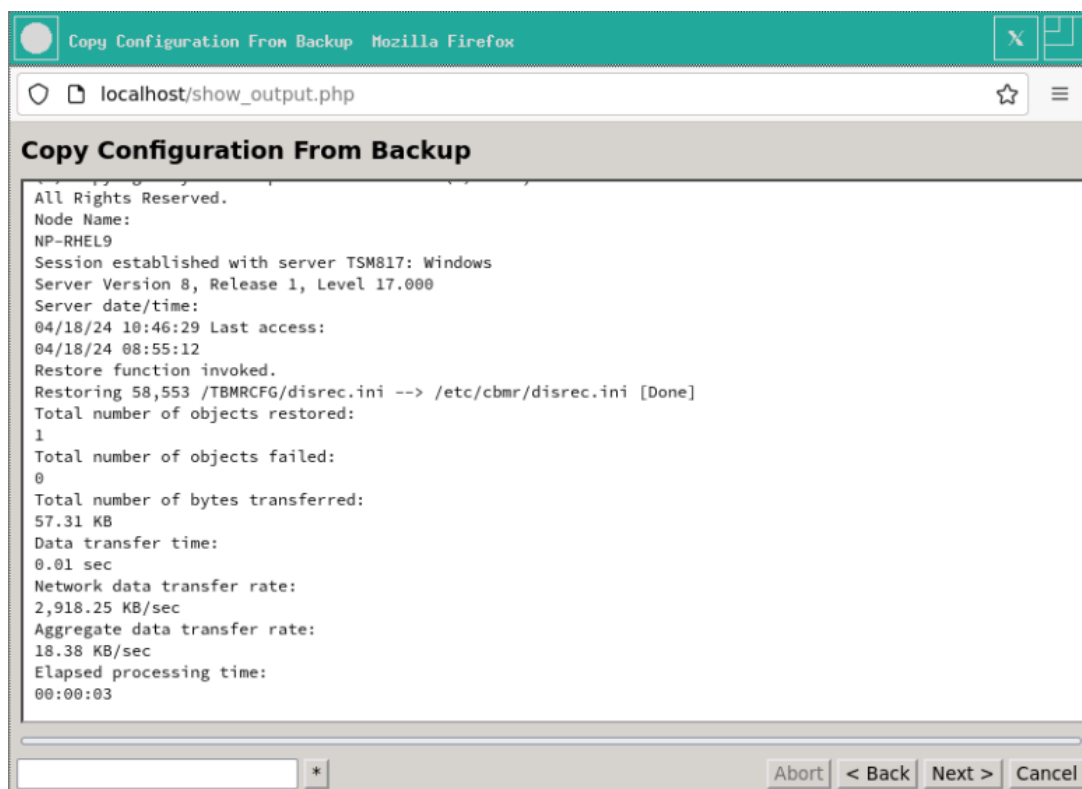
In this example this would recover a backup closest to 28 February 2023 00:00am. Note IBM Spectrum Protect will find the closest incremental backup looking backwards in time.

Normally, nothing needs to be entered under **Spectrum Protect (DSMC) recover options**. If you do need to enter any parameters, it will probably be standard IBM Spectrum Protect options. Any parameters entered will be passed to the IBM Spectrum Protect server unchanged, but they must be prefixed with a '-'. For example **-resourceutilization=2**. Please consult your IBM Spectrum Protect User Manual for full details.

Note: for a list of these parameters and how to use them you should consult the relevant IBM Spectrum Protect User Guide.

Click **Next >** to continue. This will then restore the configuration from the backup.





Click **Next >** to continue to the **Start Recovery** phase. You will then be presented with the Start Recovery options. Here you can change the configuration of the system being restored.

Start Recovery Mozilla Firefox

localhost/tbmr_start_recovery.php?dsmc_pit_date=&dsmc_pit_time=&dsmc_opts=&verbosity

Start Recovery

Specify the restore settings here.

Recovery Date (mm/dd/yyyy)

Recovery Time (HH:MM:SS)

DSMC Options

Target Machine Dissimilar hardware support ☒ New boot stanza ☐

SELinux Relabel ☒

Logging

Sync ☐ Sync existing files

Multipath Support ☐

Local Disks Only ☒ Ignore SAN disks

Recovery Options

Disrec options

Next > Cancel

Select the **Sync** tick-box if you wish to sync existing files. This option will then run a recovery

sequence of everything from the restore phase onwards - so a file restore, then a dissimilar hardware step and finally a make bootable step. If the client supports incremental restores, this will save a lot of time.

For the target machine tick [Dissimilar hardware support](#) if you want the recovery to automatically inject drivers for any new devices detected at the end of the recovery. This is the default.

If you are recovering Multipath/PowerPath disks, you must check the tick-box for **Multipath/PowerPath Support**. Not doing so will cause the disks to be treated as non-Multipath/PowerPath disks. You can then select and customise your Multipath/PowerPath disk layout by clicking on the [Multipath Options](#) or [PowerPath Options](#) button. Note this option is only enabled if multipath disks are set in the configuration.

Recover	Original device	New device
<input checked="" type="checkbox"/>	boot 3600c0ff000d70ba1a95c0c5a01000000 20G /dev/sda, /dev/sdc	3600c0ff000d70ba16c7d0c5a01000000 20G /dev/sda, /dev/sdd
<input checked="" type="checkbox"/>	mpathb 3600c0ff000d70ba1c4dc435a01000000 17G /dev/sdb, /dev/sdd	3600c0ff000d70ba1a95c0c5a01000000 20G /dev/sdb, /dev/sdc

If you wish, you may customise your disk layout, volume group or filesystem selection by clicking on the [Recovery Options](#) button.



Recovery Options Mozilla Firefox

localhost/recovery_options.php

Recovery Options

Boot Options

Auto Override the default bootloader

Map Disks

The original and new disks are shown below. If required, drag a new disk to a different row to customise the proposed layout. Dragging a new disk onto a row which already has a new disk will swap those entries.

uncheck all

Recover	Original disk	New disk
<input checked="" type="checkbox"/>	/dev/sda 50GB	/dev/sda 50GB mptspi

Volume Groups

uncheck all

☒ rhel (/dev/sda2)

Filesystems

uncheck all

☒ / (/dev/mapper/rhel-root xfs)

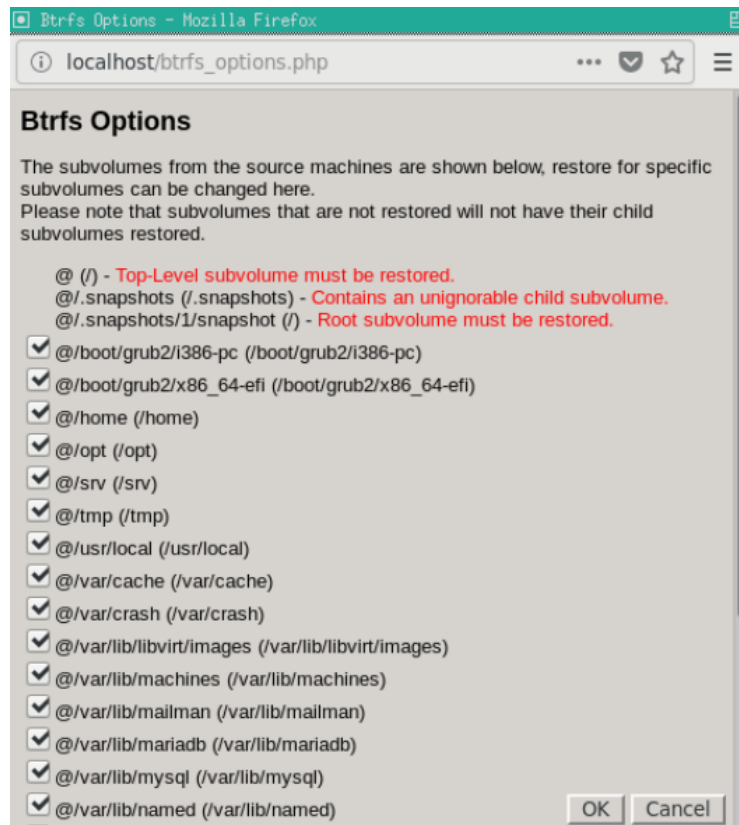
☒ /boot (/dev/sda1 xfs)

OK Cancel

Note: disks that have been configured in the Multipath/PowerPath Options menu will not be visible on the Recovery Options menu.

Note: de-selecting a filesystem will disable filesystem creation and file restore.

If the system to be recovered contains BTRFS subvolumes you may configure whether they are recreated during recovery. Click the [Btrfs Options](#) button to bring up the menu (note this option is only displayed if BTRFS volumes are present).



De-selecting a checkbox will prevent the recovery from recreating the subvolume. Click [OK](#) to save and continue.

Note: Some subvolumes can not be de-selected due to a child subvolume dependency or if it is a root subvolume.

If you wish to change the Network Settings in advance of recovery, select **Post Recovery Network**. This option is only available for SLES 11 or later, and Red Hat 6 or later.



Post Recovery Network

This dialog allows the post recovery network settings to be changed. Each interface may be given a static IP address and subnet mask, or allocated a DHCP address. The hostname, default gateway and nameserver may also be changed. Empty fields will be left unchanged on the recovered system. If network information is tied to the original hardware addresses, details should be added here for each interface required after recovery, even if the network details are not to be changed.

Enabled Interface	MAC Address	IP Address	Subnet Mask	DHCP
<input checked="" type="checkbox"/> eth0	00:0c:29:ec:93:a2	10.10.11.9	255.0.0.0	<input type="checkbox"/>

Post Recovery Script

Hostname

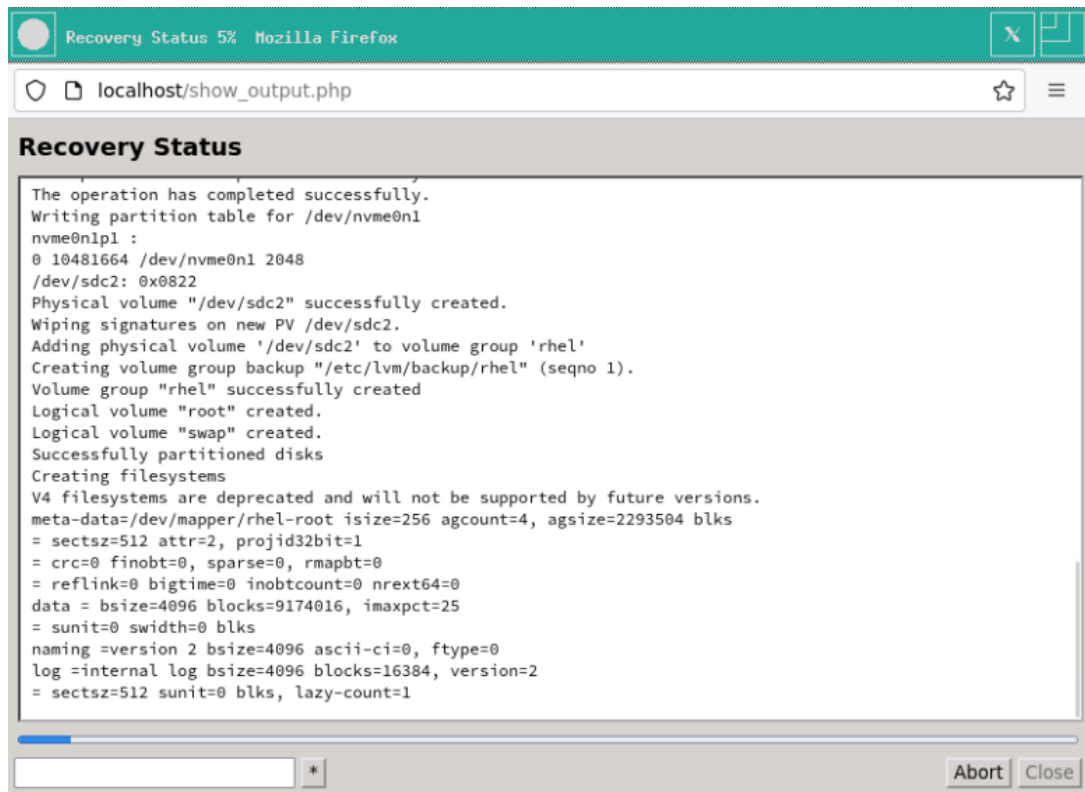
Gateway

Nameserver (1)

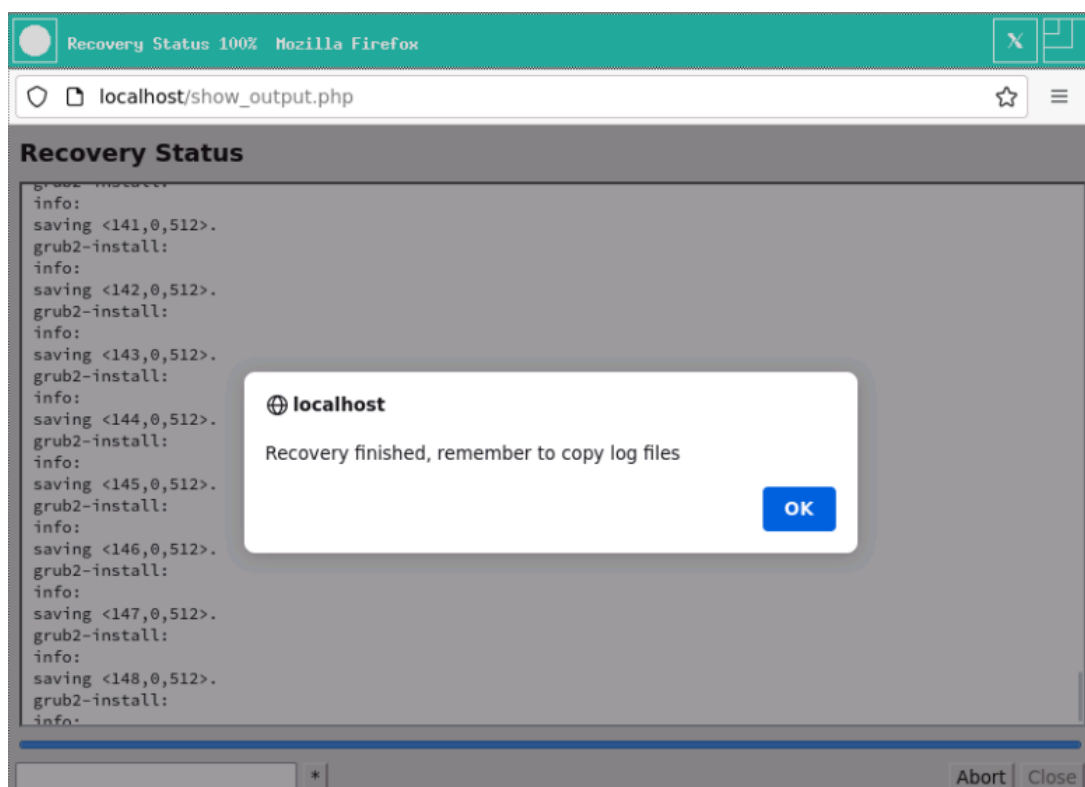
When you are satisfied that all options are correct, click **OK** to confirm.

Note: The Post Recovery Network button will only be displayed if the functionality of this feature can actually be performed on the restored system.

When you are satisfied that all options are correct, click **OK** to confirm and return to the **Start Recovery** dialogue. Finally select **Next >** to start the recovery, which will begin with a dialog like this:



The completion of the recovery is signified with a pop-up box like this:



Cristie recommends that the log files are always saved. If the machine fails to boot after the restore Cristie Support will require copies of the log files to diagnose any problems. Details on how to save log files are described in the section [Copy Log Files](#).



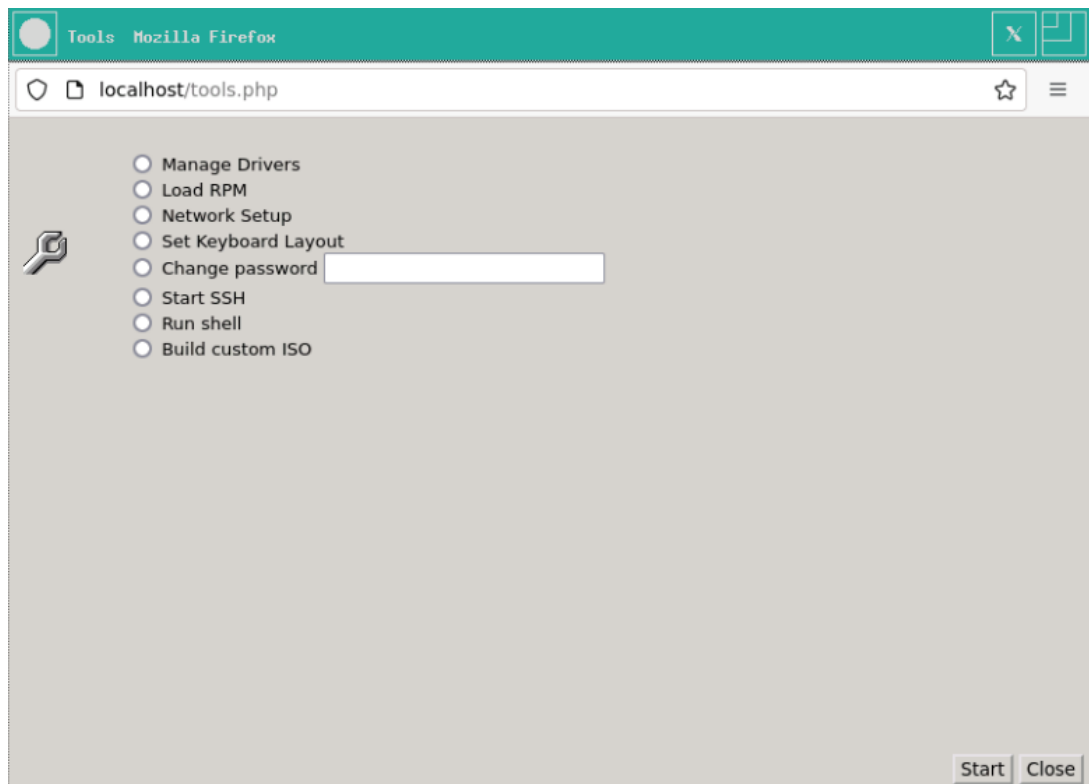
Note: if you are recovering to dissimilar hardware: TBMR will find the required module(s) automatically. Normally this will happen with no further user intervention.

Click **OK** to close the pop-up box, followed by the **Close** button to return to the Main Menu.

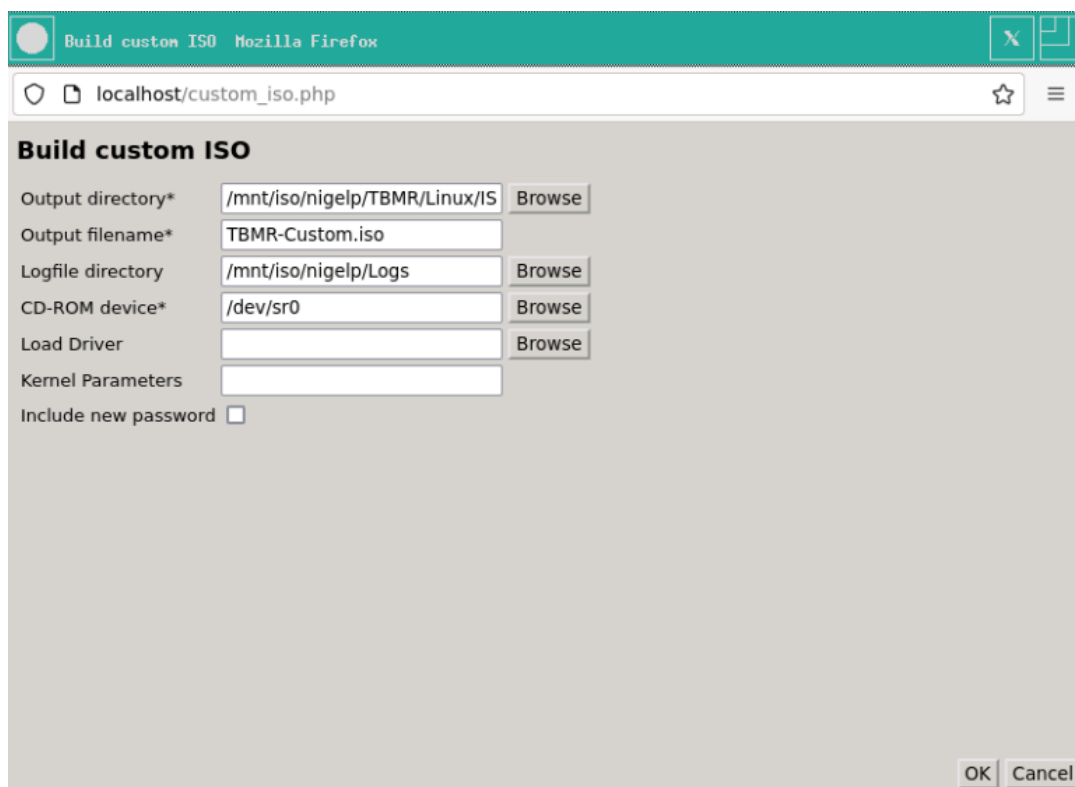
Finally select **Reboot** from the Main Menu to boot the restored machine, if post recovery options are not required.

8.1 Build Custom ISO

To create a custom recovery ISO, firstly boot the supplied XBMR DR ISO on a suitable host system and select the appropriate XBMR product. Then select the **Tools** menu.



Now select **Build custom ISO** and click **Start**. The main build ISO dialogue is shown:

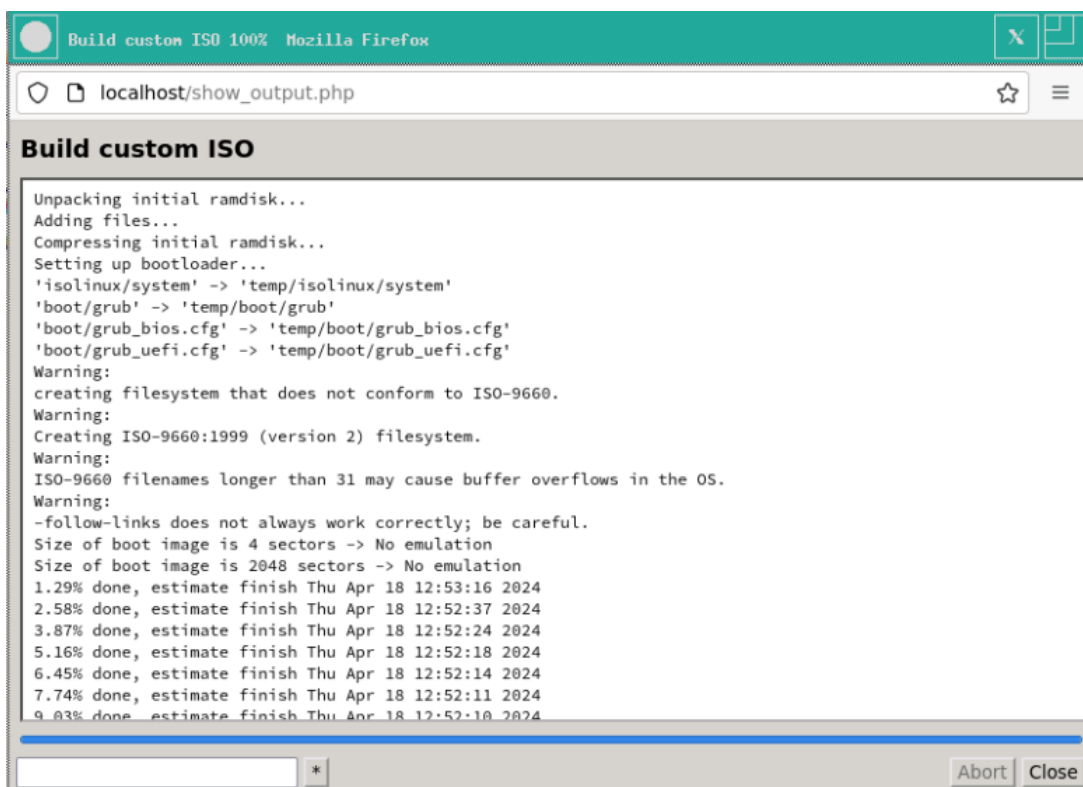


You will need to configure the following fields:

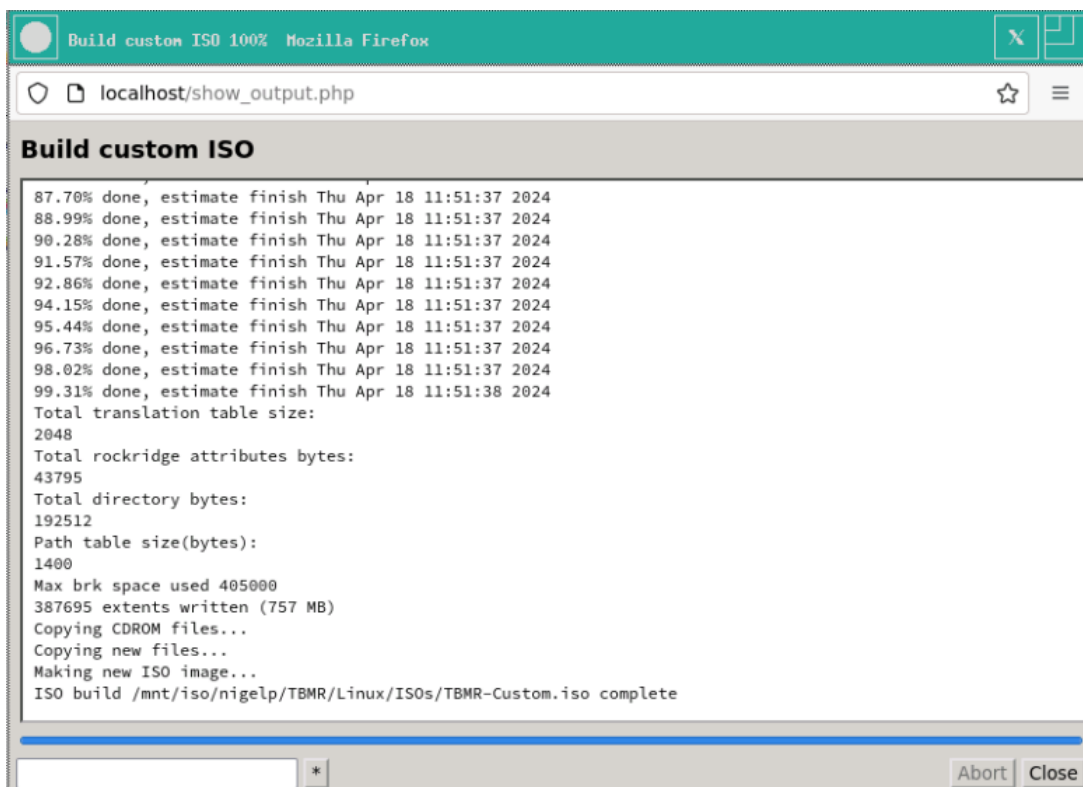
- **Output directory** is a network share (use [Browse](#) to select and mount a share).
- **Output filename** must include the .iso extension.
- **Logfile directory** is a network share (use [Browse](#) to select and mount a share).
- **CD-ROM device** (use [Browse](#) to select a CD/DVD-ROM device from /dev).
- **Load Driver** select the path to an optional driver file. Ensure this is compatible with the system being recovered.
- **Kernel Parameters** specify any extra parameters to be passed to the kernel at boot time. Be careful - this is not syntax checked.
- **Include new password** option will include your new ssh/http password if you have changed it in the tools menu prior to building the custom ISO.

Populate the fields as required, for example. Then click [OK](#) to begin the ISO creation.





The following progress screen will show when the ISO is successfully built.



Click **Close** to complete the operation. At this point you may either cancel the recovery operation or continue as required.

The created ISO may now be used to directly recover the host from the backup. However

operator intervention will be required to specify the backup location details.

8.2 Command Line Recoveries

XBMR also has the ability to control all aspects of a DR sequence without using the web or curses based GUIs. To do this it uses a script based command line manually run from the built-in bash prompt. This is an advanced feature and should not be used until the User becomes familiar with TBMR DR principles and procedures.

The command line parameters supplied to the script are divided into 4 groups, **Network**, **Mount**, **Spectrum Protect** and **General**, as follows:

Network options:

<code>--network_number=<number></code>	Set network number (default is 0)
<code>--route_number=<number></code>	Set route number (default is 0)
<code>--ip_address=<ip_address></code>	Set recovery environment IP address
<code>--netmask=<ip_address></code>	Set recovery environment network mask
<code>--hostname=<string></code>	Set recovery environment hostname
<code>--gateway=<ip_address></code>	Set recovery environment default gateway
<code>--ethtool=<command></code>	Pass options to ethtool

Mount options:

<code>mount_number=<number></code>	Set mount number (default is 0)
<code>mount_path=<path></code>	Set mountpoint
<code>mount_share<device></code>	Set mount device
<code>mount_username=<name></code>	Set mount username
<code>mount_passwd=<passwd></code>	Set mount password
<code>mount_ip_address<ip_address></code>	Set mount IP address

Spectrum Protect options:

<code>--tsm_ip_address=<ip_address></code>	Set TSM server IP address
<code>--tsm_port=<number></code>	Set TSM server port number
<code>--tsm_node=<string></code>	Set TSM server node name
<code>--tsm_passwd=<string></code>	Set TSM server password
<code>--tsm_certificate=<path></code>	Set TSM certificate path
<code>--cbmr_tsm_node=<string></code>	Set TSM node name
<code>--cbmr_tsm_passwd=<string></code>	Set TSM node password
<code>--cbmr_tsm_filespace=<string></code>	Set TSM node filesystem name

forces a tar backup of /boot - this is needed for block based backups to work

General options:



<code>--help</code>	Show help message and exit
<code>--sshd=<1 0></code>	Start ssh daemon if value=1
<code>--reload=<string></code>	Reload module with options
<code>--passwd=<string></code>	Set password for SSH and HTTP
<code>--find_multipaths=<yes/no></code>	Set find_multipaths option in multipath.conf
<code>--disshw=<1 0></code>	Turn on dissimilar hardware support if value=1
<code>--m_path=<1 0></code>	Turn on multipath support if value=1
<code>--sleep=<number></code>	Sleep for <number> seconds
<code>--log_dir=<path></code>	Copy logs to mounted <path>
<code>--bootloader=<name></code>	Set bootloader to <name>
<code>--autorelabel=<1 0></code>	Turn on SELinux autorelabel if value=1
<code>--convert_to_mbr</code>	Supply when recovering an EFI system to an MBR target
<code>--product=<type></code>	One of abmr, cbmr, cobmr, nbmr, rbmr or tbmr

Example (a TBMR recovery)

```
restore --product=tbmr --reload="ibmveth old_large_send=1" --ethtool="-K eth0 tso c
--ip_address="10.10.10.186" --netmask="255.0.0.0" --hostname="cristiel"
--gateway="10.0.1.100" --tsm_ip_address="10.10.11.98" --convert_to_mbr
--tsm_node="chrisw-sles11-hyperv-mpath" --tsm_passwd="chrisw"
--find_multipaths="no" --m_path="1" --disshw="1" --sshd="1"
--log_dir="/mnt/log/log" --bootloader="yaboot" --autorelabel="0"
--mount_path="/mnt/log" --mount_share="//10.1.1.26/chris$"
--mount_username="chris" --mount_passwd="mypassword"
```

Since this is a complex command line, and easy to get wrong during data entry, we advise preparing the command line in an editor elsewhere and pasting it into the bash prompt.




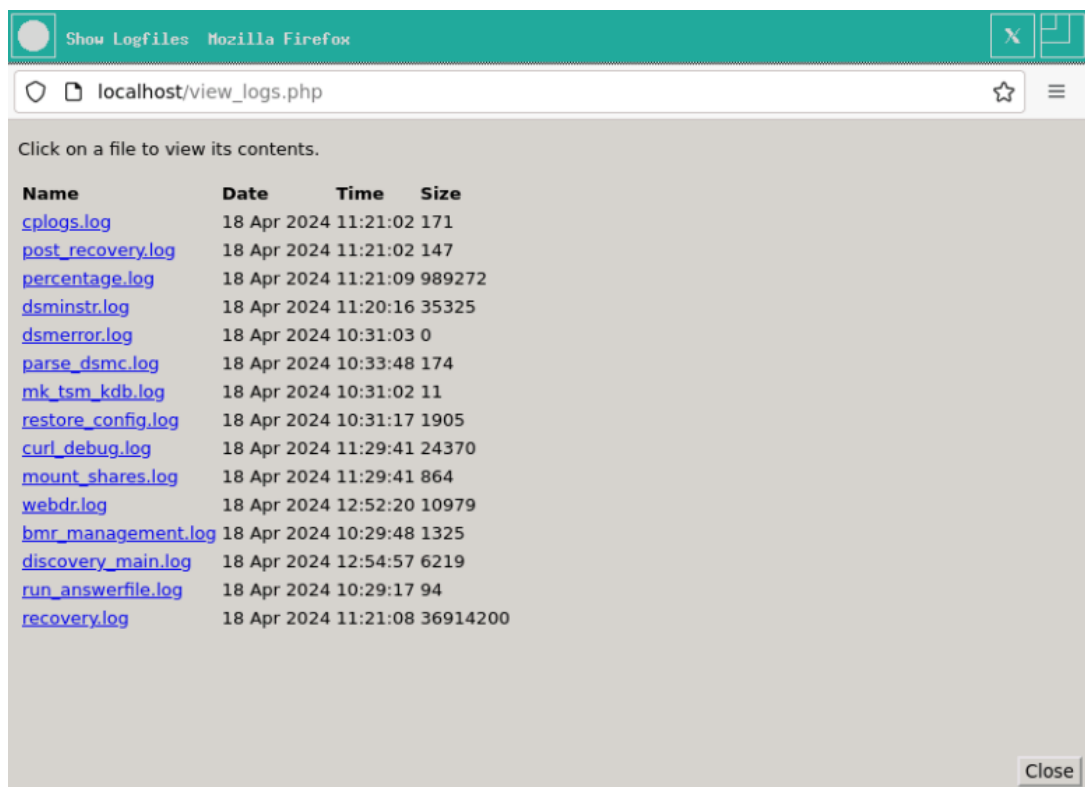
9 Post Recovery Options

After performing a recovery, it is possible to undertake the following actions:

- Copy Log Files (Cristie recommends that this action is always undertaken after a recovery)
- View Log Files

9.1 Show Log Files

To view log files, select the  icon from the Main Menu. This will display the list of available logfiles:



Click on the log you wish to view. Check the summary information at the bottom of the recovery status report for any errors.

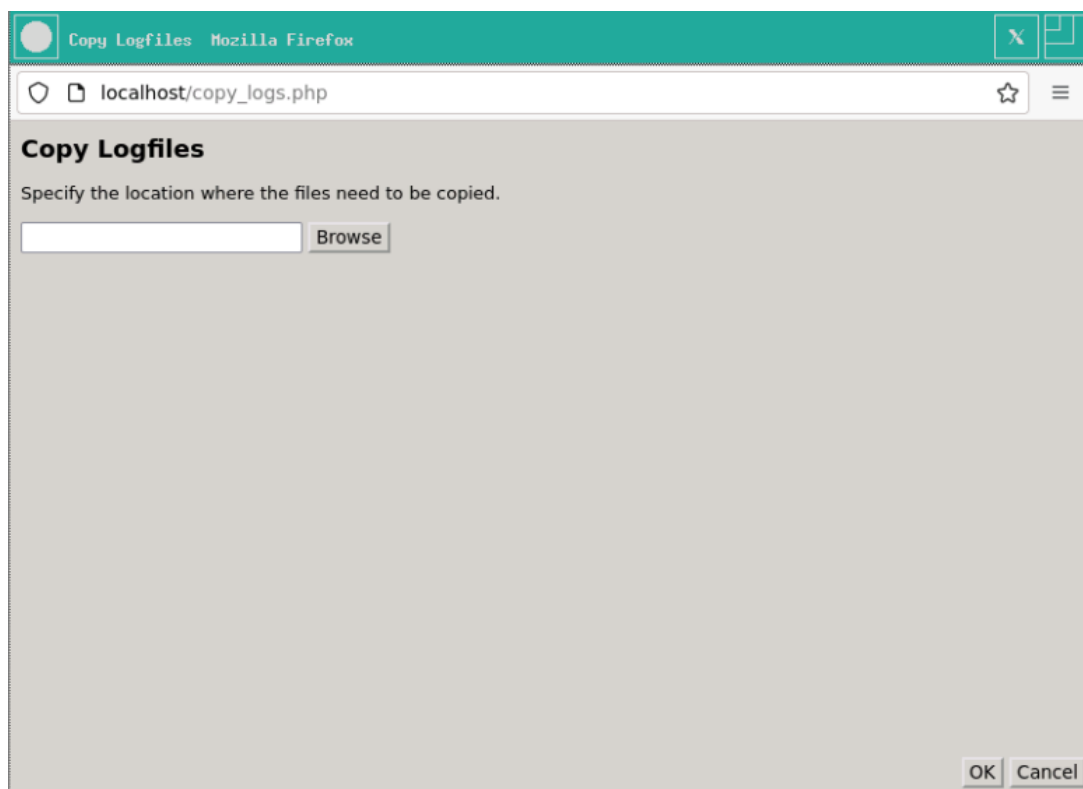
Click [Close](#) to finish.

9.2 Copy Log Files

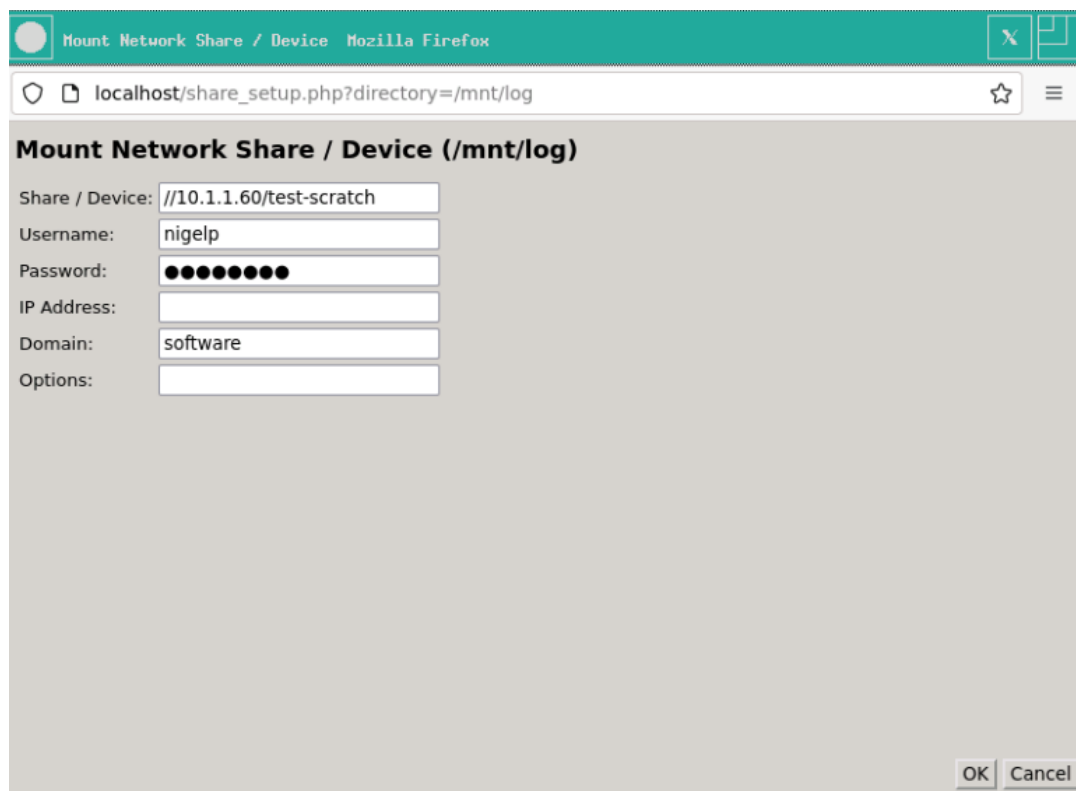
Select the  icon from the **Cristie Recovery Environment** main menu.

Click [Browse](#) to select a location to copy the log files to.



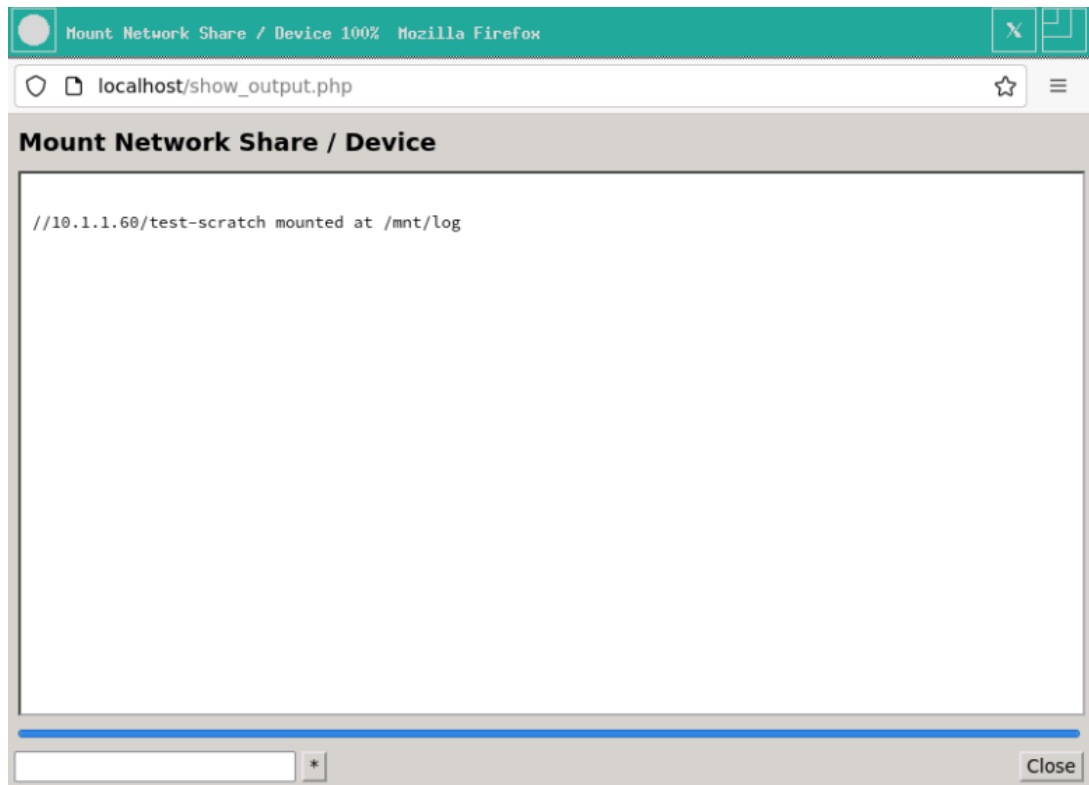


Select [Browse](#) to mount a network drive.

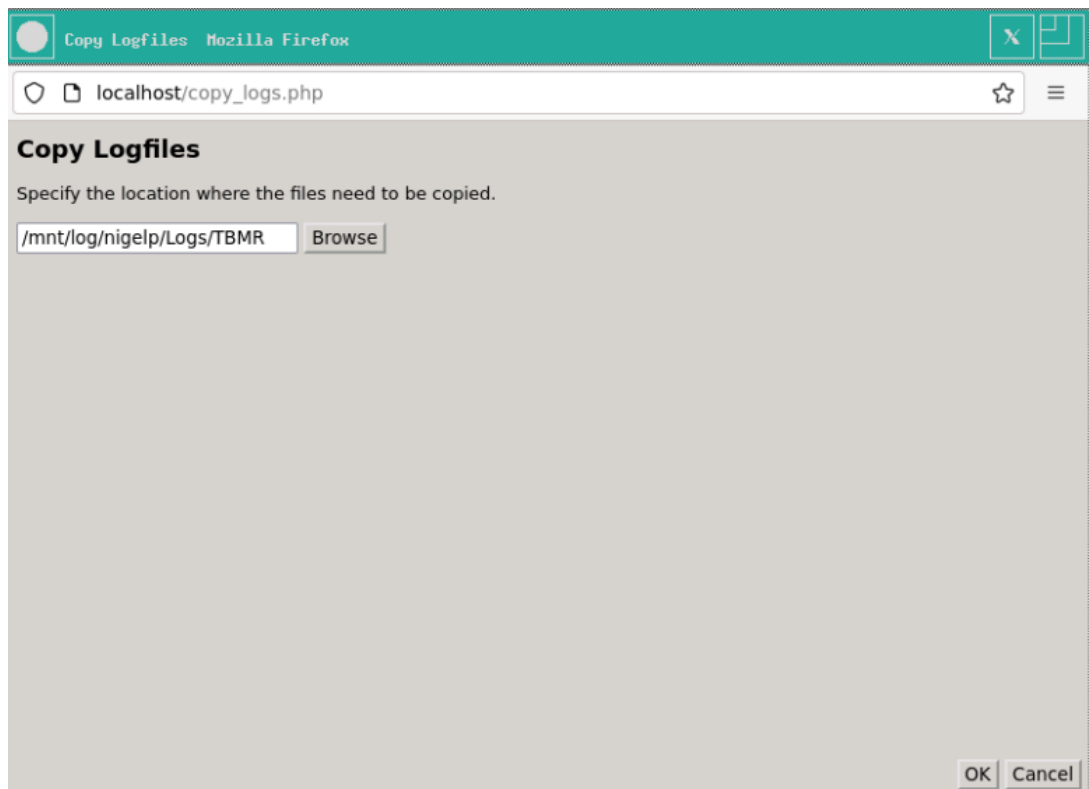


A successful mount is signified by:



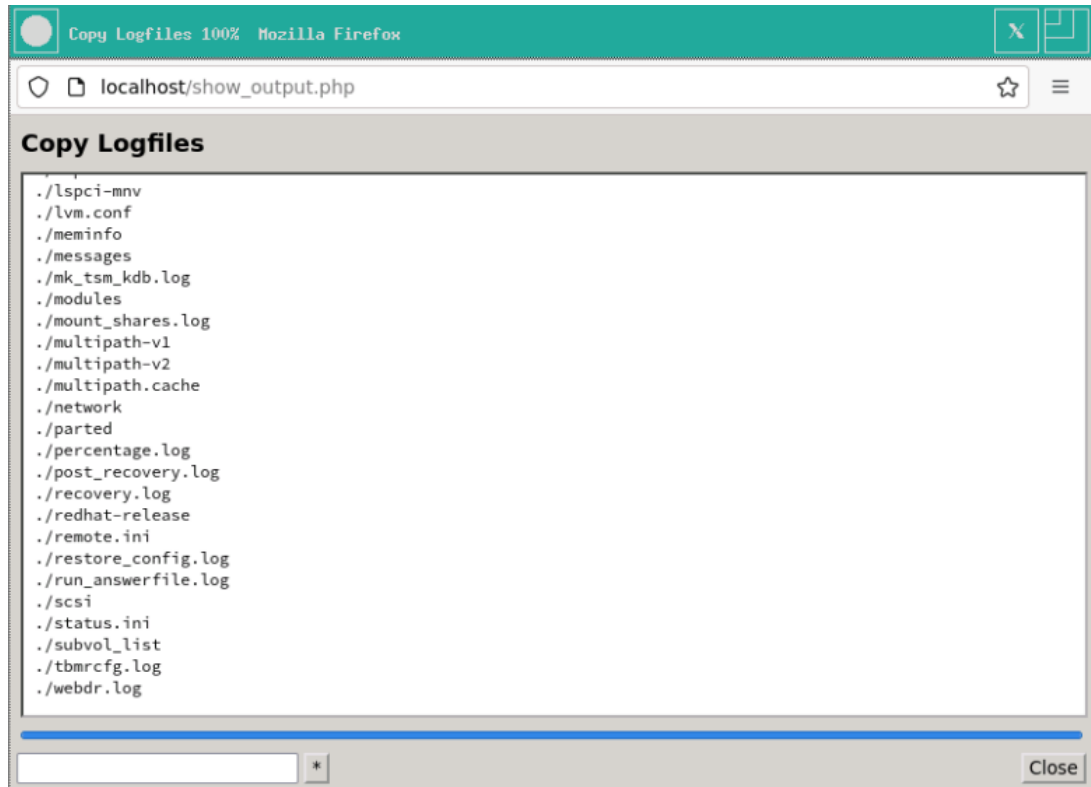


Select a directory on the mounted share:



Click **OK** to copy the logfiles.





Ensure this is a location which can be easily accessed in case there is a need to email the log files to Cristie for support purposes.

Click [Close](#) to return to the **Recovery Environment** Main Menu.

Note: log files are essential if you require support from Cristie. They detail exactly what has happened during the recovery on your system. Without them, it is very difficult for Cristie to offer meaningful support.



10 Cristie Technical Support

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

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

Contact Numbers - Cristie Software (UK) Limited

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

Support Hours

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

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

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

*Severity 1 issues are defined as: a production server failure, cannot perform recovery or actual loss of data occurring.

**For details on dates of UK Bank Holidays, please see www.cristie.com/support/

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

