CoBMR For Linux

Bare Machine Recovery for Cohesity

User Guide

Version 9.5.1 released September 2023

Revision 1 - 27th September 2023

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

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

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

Contents

1 Document Conventions

The following typographical conventions are used throughout this guide:

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

2 Introduction

Bare Machine Recovery for Cohesity provides disaster recovery capability for Cohesity DataProtect 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 CoBMR. More detailed information is available from `man` pages for the CoBMR components. The `man` pages are available after installation of CoBMR.

This guide relates to CoBMR for Linux Intel version 9.5.1 only.

> ***Note: CoBMR can only be used in conjunction with Cohesity DataProtect.***

This guide describes how to:

- *Save Configuration data using cobmr`cfg`*
- *Configure and run your Cohesity DataProtect Client backup*
- *Perform a Disaster Recovery*

2.1 Limitations

There are limits to what this version of CoBMR 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 CoBMR may be found in the **Cristie Knowledge Base** (https://kb.cristie.com) or the **Cristie Forum (**https://forum.cristie.com).

3 System Requirements

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

CoBMR requires Cohesity DataProtect client version 6.3 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 Cohesity DataProtect client/server support for CoBMR Version 9.5.1.

Before CoBMR 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 CoBMR Version 9.5.1.

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:-

```
cobmrcfg -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 CoBMR For Disaster Recovery

This section describes the steps involved in using Cohesity DataProtect in conjunction with CoBMR for disaster recovery.

This description assumes that the Cohesity DataProtect client software has already been installed and configured correctly.

To ensure your system is protected observe the following steps:

1. *Install CoBMR on the system you wish to protect.*
2. *Use the* `cobmrcfg` *program to capture and store the configuration of the system.*
3. *From the Cohesity DataProtect server run a file-based backup of the system to your Cohesity DataProtect server as usual.*

6.1 Saving the System Configuration

Configuration is always saved to **/CoBMRCFG** - 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 `cobmrcfg` is used. It is recommended that this is run prior to running each backup to ensure the configuration is up to date.

6.2 CoBMRcfg

To use the command line configuration saving program, type `cobmrcfg`. 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 `cobmrcfg` can be shown using:

```
cobmrcfg --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:

```
cobmrcfg -b grub -d /dev/sda
```

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

```
cobmrcfg -b grub -d /dev/hda
```

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

This is a full list of options:

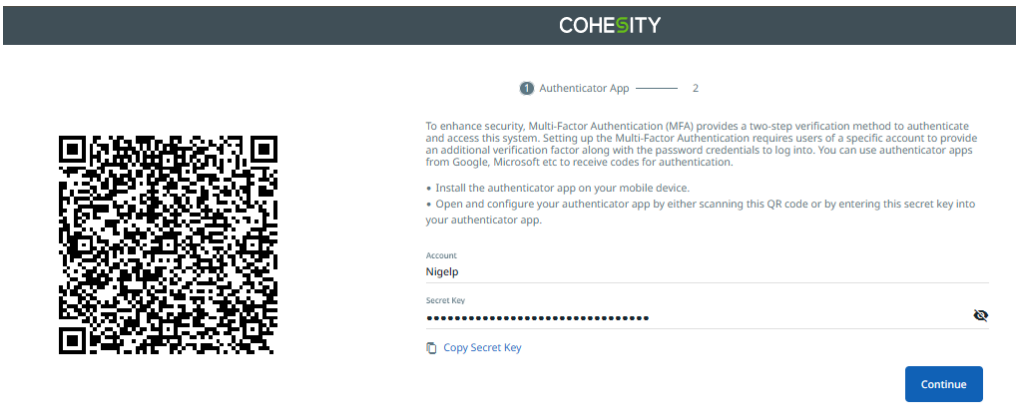
Option	Description
-b<name>, --bootloader=<name>	Set boot loader to <name> (default is grub)
-d<name>, --bootdevice=<name>	Set boot device name to <name>
-l<file>, --logfile=<file>	Set log file (default is cbmrcfg.log)
-o<file>, --output=<file>	Set output file (default is disrec.ini)
-p<permissions>	Set output file permissions (default 0600)
-v, --verbose	Verbose mode
--autorelabel=<n>	Automatically relabel SELinux if <n> != 0
--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>
--vg_regex=<regex>	Only create VGs matching <regex>
--vg_skip=<pattern>	Don't create VGs matching <pattern>
--vg_skip_regex=<regex>	Don't create VGs matching <regex>
--help, --usage	Print this message and exit
--version	Print the version and exit

7 Multi-factor Authentication

If your Cohesity DataProtect server is configured to use Multi-factor Authentication (MFA) you will be prompted during an interactive recovery sequence for an MFA code.

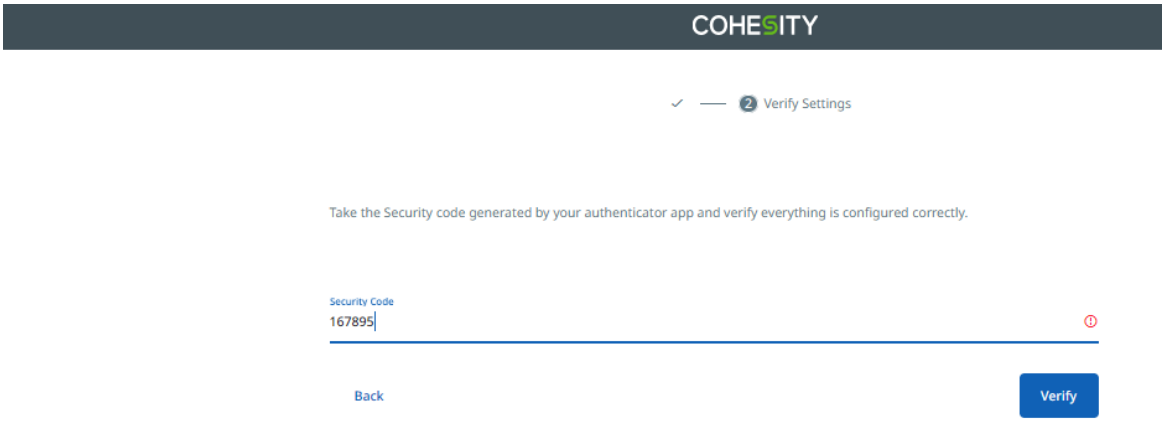
To generate such a code you will need an authentication app installed on a mobile device (e.g. phone or tablet) and an entry added for your server. For example Microsoft and Google provide such Authenticator apps.

When configuring an entry in the app for your server you will need to use the server generated QR code to do this. For example:

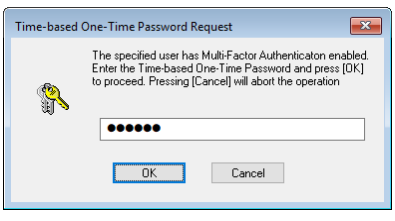


Scan the code with your mobile device to setup an entry for the server in the authenticator app.

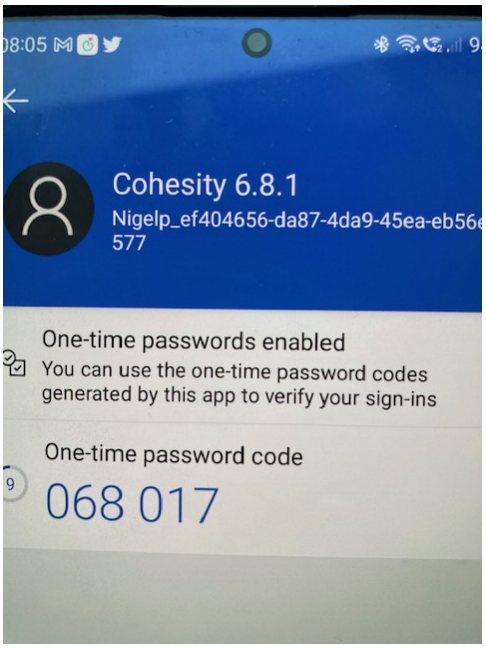
Then to login to the server you will see a prompt like this:



During a recovery operation you will be prompted for an MFA code. Use the entry in your authenticator app to generate an MFA code. For example:



The MFA app will show something similar to this when the code is generated:



Note: The MFA codes are only valid for a short period of time (e.g. 30 seconds). If you take too long to enter the code it will be incorrect. Re-generate the code and re-enter if this occurs.

8 Cohesity DataProtect Client Backup

Cohesity DataProtect can create backups either in either file-based or block-based form. CoBMR supports recoveries in either form.

Ensure the CoBMR configuration is in place and then run the backup from the Cohesity DataProtect server as usual.

For **btrfs** file system support only, it is recommended to exclude the snapshot directories (unless they are required). These directories are found in /.snapshots/*/snapshot. These can make the backups very large and are not required for disaster recovery.

8.1 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 Cohesity DataProtect backup is performed every time the operating system files change. In addition you should also configure a run of the CoBMRCfg.exe program using a pre-script on the server (if supported) prior to the backup.

This is not always possible, so **Cristie Software Ltd.** recommends that the Cohesity DataProtect 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 by defining a scheduled backup for the required client machine on the Cohesity DataProtect server.

9 Performing a Recovery

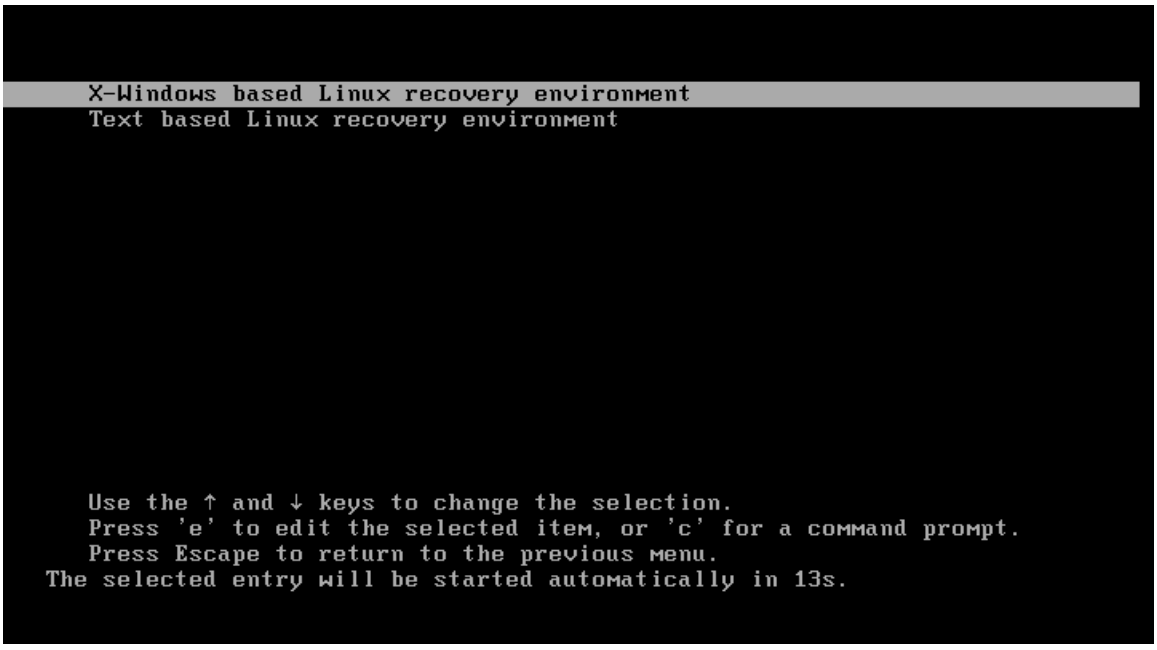
When a machine has failed, it can be recovered using the XBMR bootable product CD/ DVD-ROM or DR ISO (if your host supports this capability). XBMR is a separate product to CoBMR. It is a generic Recovery Environment for all Cristie Linux BMR products.

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

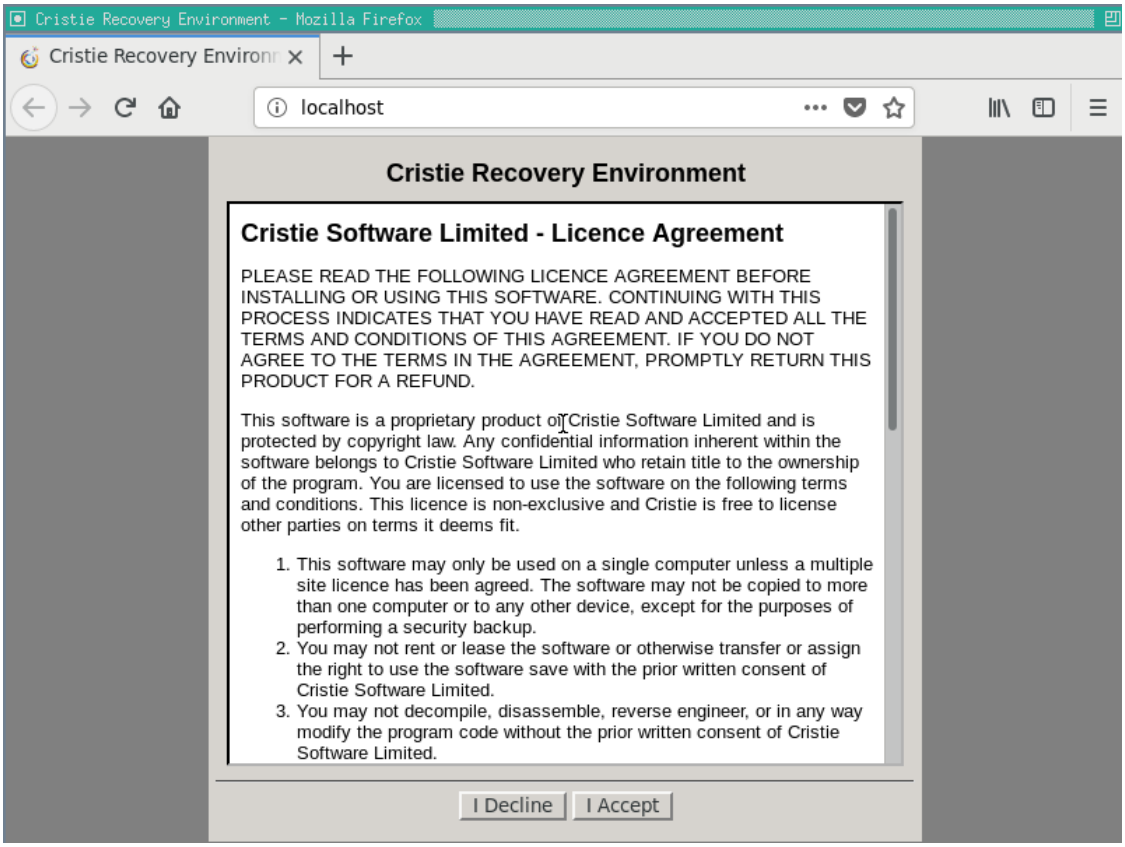
The process encompasses the following stages:

- **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:



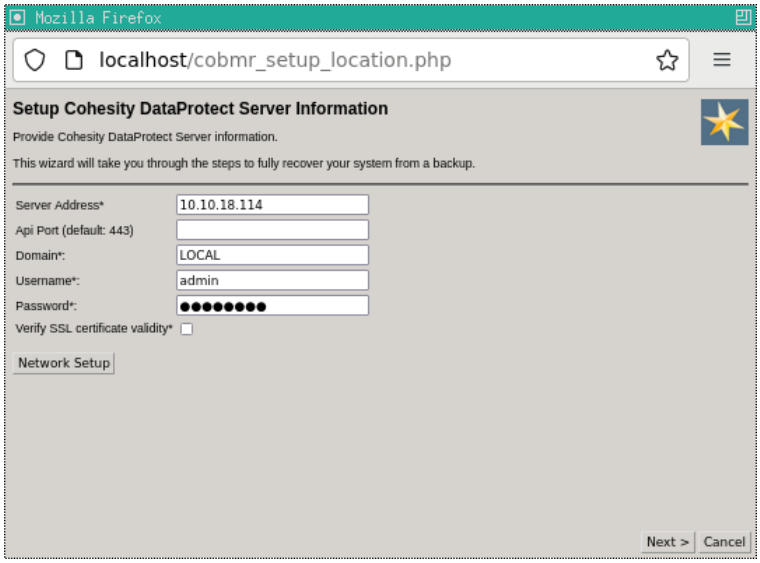
Cristie recommends that you choose the graphical X-Windows recovery environment mode which loads the **Cristie Recovery Environment.** You will be presented with the **license** screen. Click I Accept if you agree with the licencing terms.



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

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

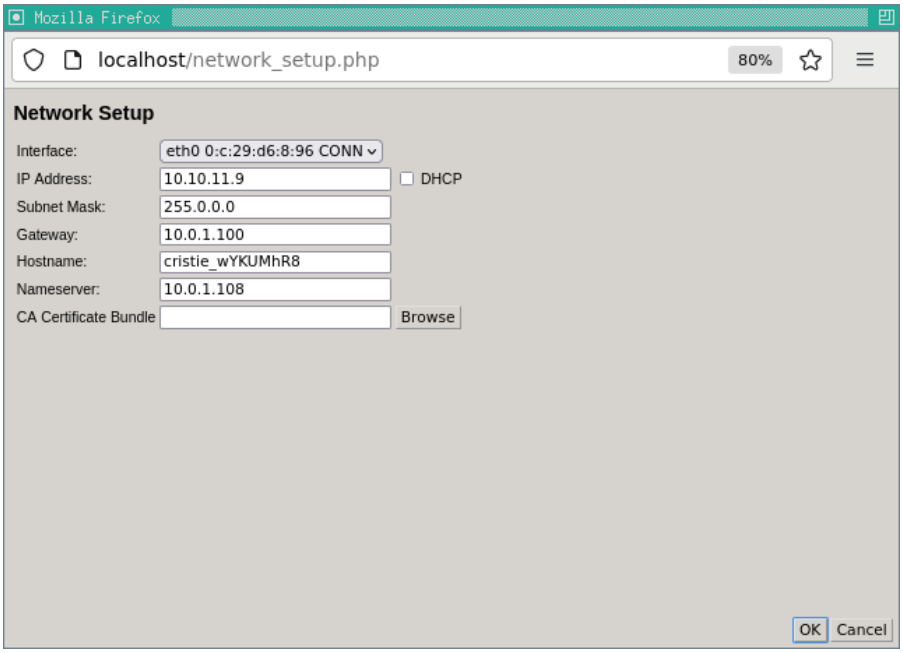
Cristie recommends selecting the **Automatic Recovery Wizard** option from the **Recovery Environment** main menu. This will then display the **Setup Cohesity DataProtect Server** dialogue.



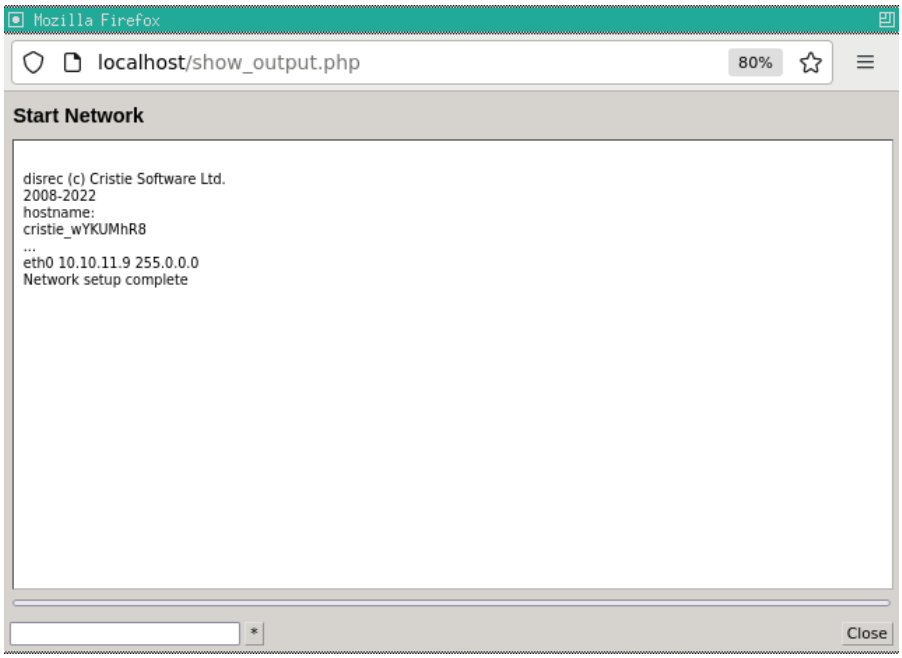
Now enter the Server details (of the Cohesity DataProtect Server where the backup resides).

Note the **Port** used is associated with the API interface (443 by default). Change this if your server uses a non-standard port otherwise leave blank. Click the **Verify SSL certificate validity** tick-box if you wish the server's certificate to be checked during the DR. If it is found to be invalid the recovery will be aborted. This check is enabled by default but can be disabled if (say) your server uses a self-signed/default certificate. Untick the tick-box in this case. Contact your Cohesity DataProtect administrator if you are unsure of any of the settings.

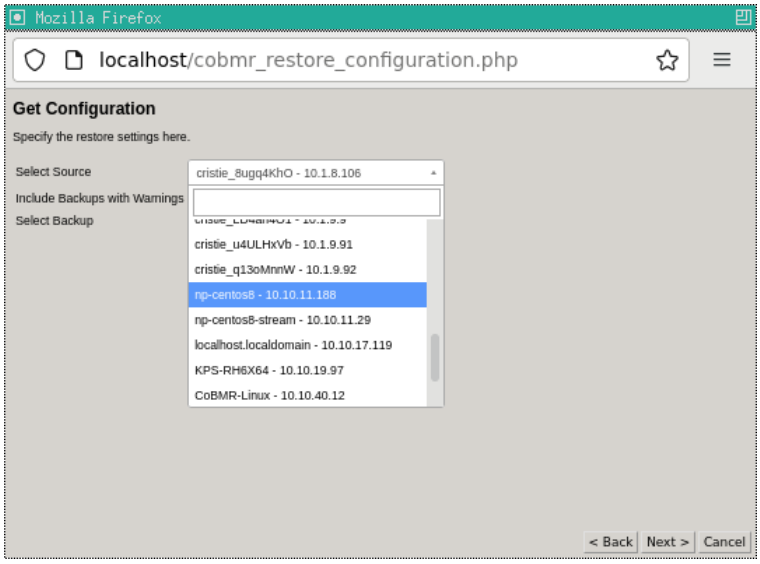
If it is required to configure the local network settings (i.e. the XBMR Recovery Environment), click the Network Setup button. Now enter your new network settings.



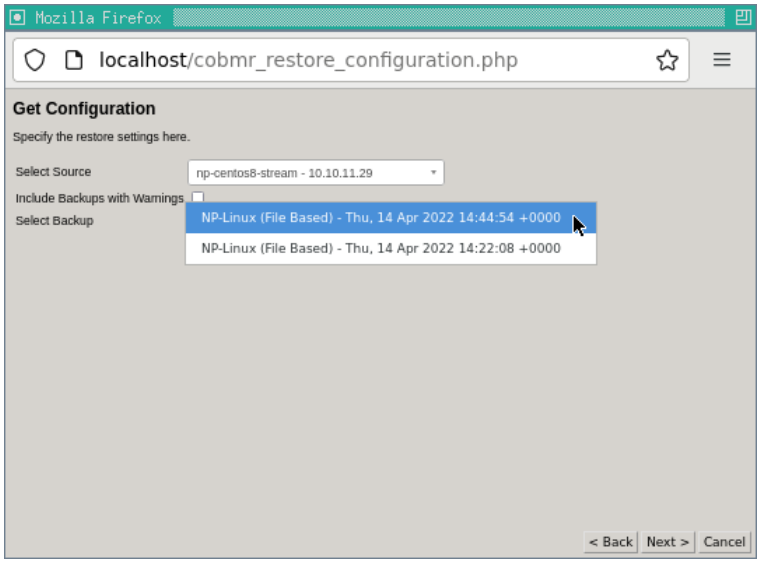
Select OK to save your changes. The Start Network screen will then display the network changes being implemented.



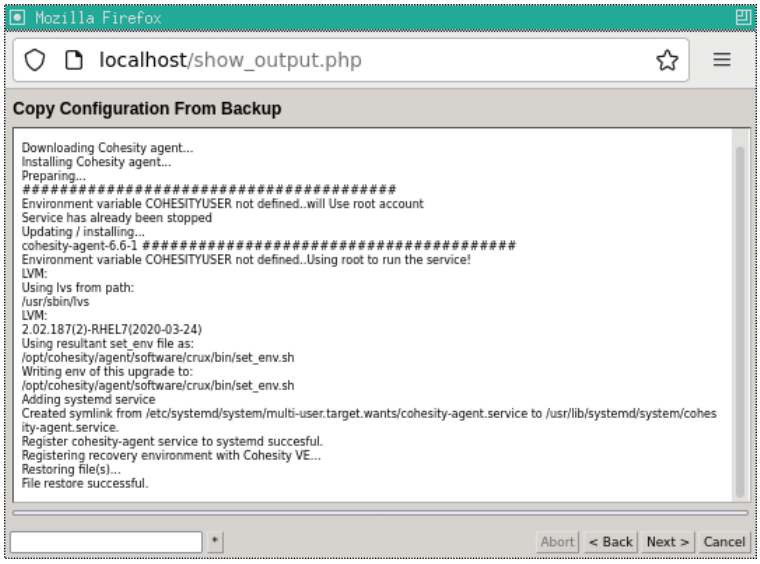
Click Close to return to the **Setup Cohesity DataProtect Server** dialogue.Now click Next > and the **Get Configuration** dialogue will be shown. Select the source backup to restore from the drop-down list.



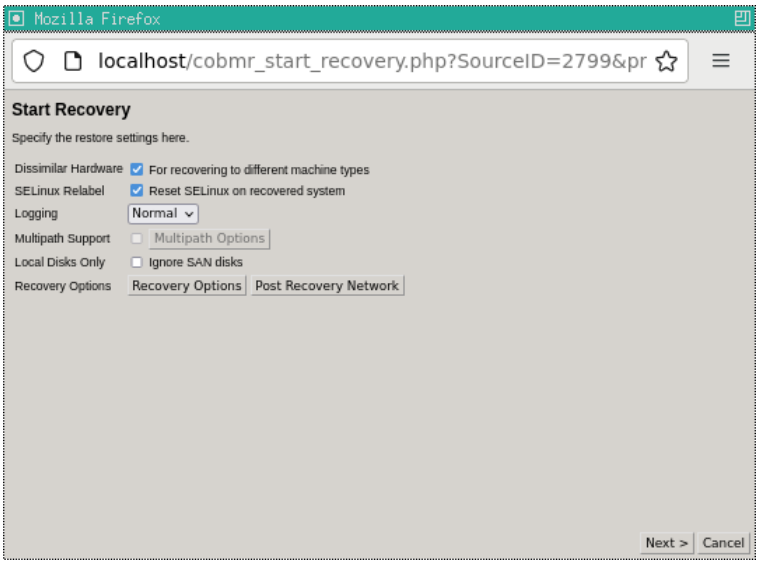
If you wish to recover a backup other than the latest (the default) select a particular date/time - a Point-in-Time (PIT). Select the required backup from the drop-down list:



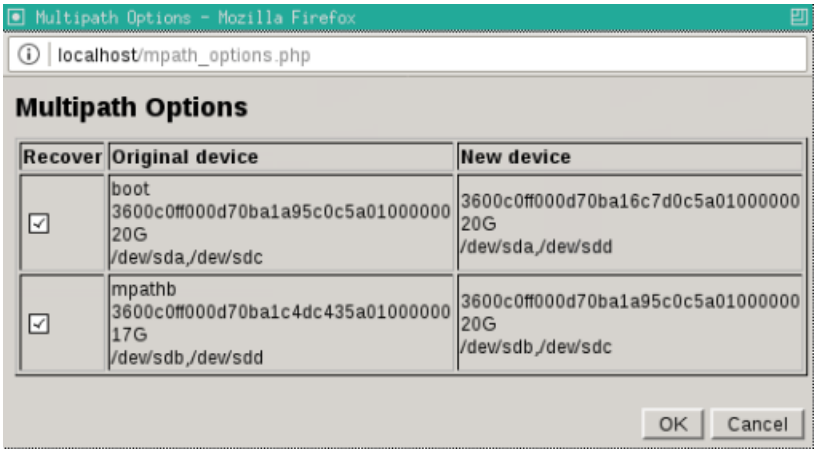
Click Next > to continue. This will then restore the configuration from the backup.



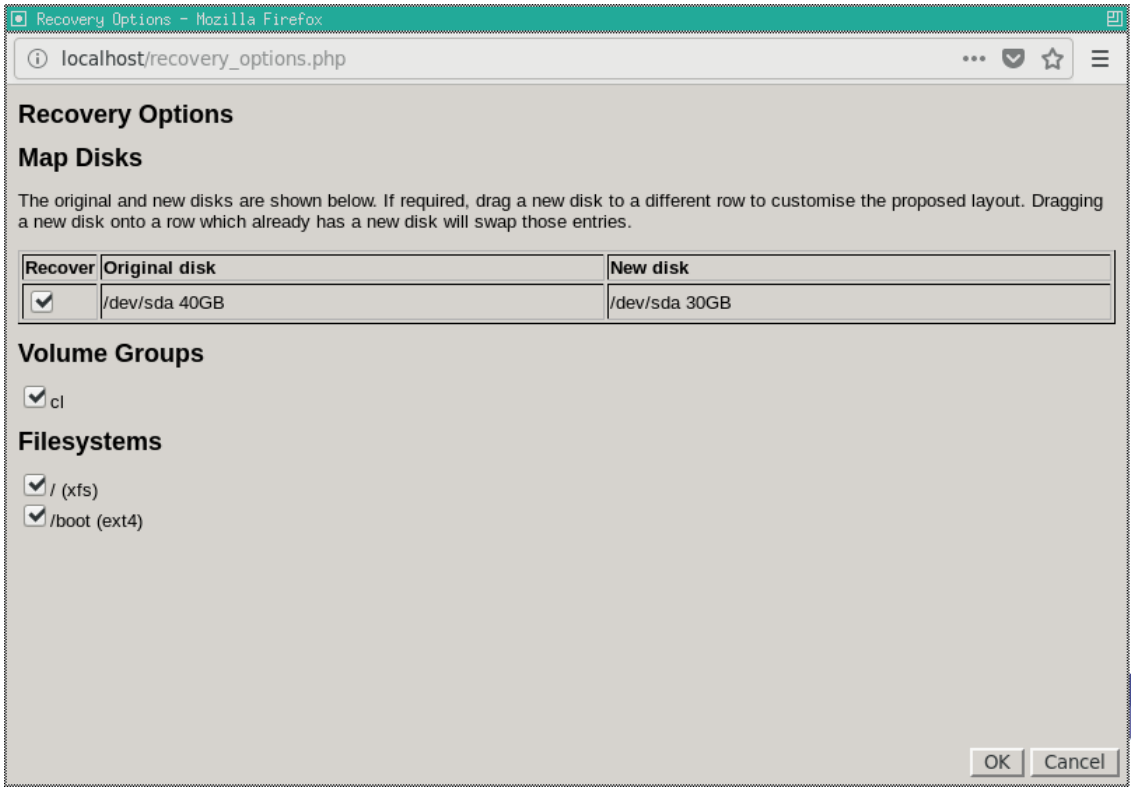
Click Next > to continue to the **Start Recovery** phase. You will then be presented with the Start Recovery options. Here you can change the configuration of the system being restored.



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



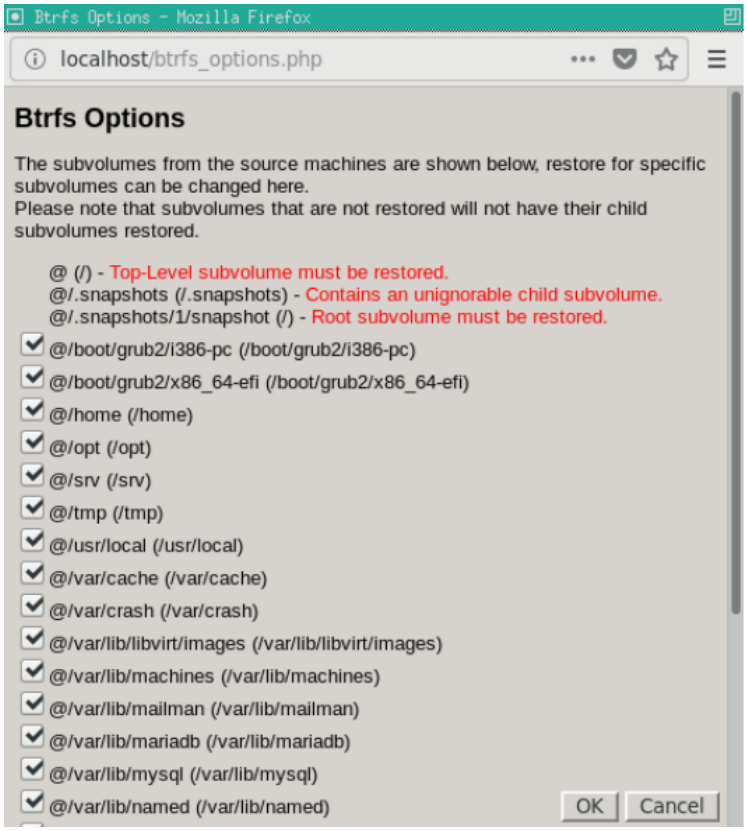
If you wish, you may customise your disk layout, volume group or filesystem selection by clicking on the Recovery Options button.



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

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

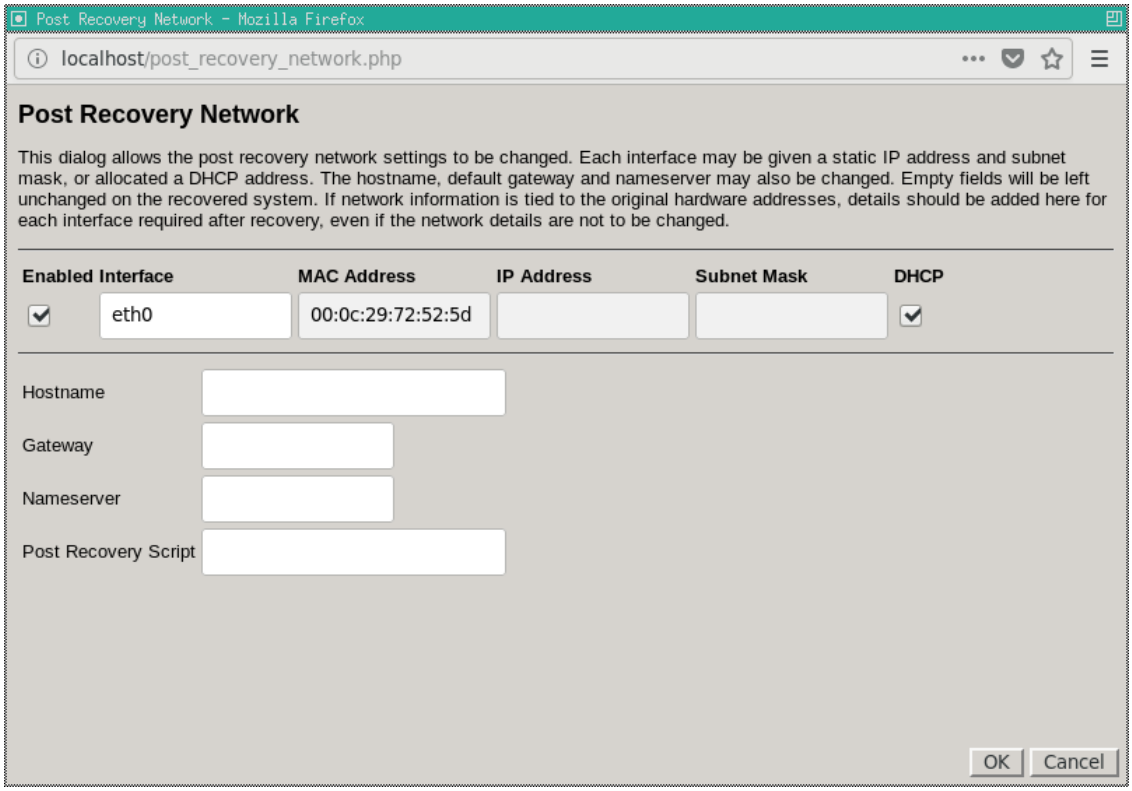
If the system to be recovered contains BTRFS subvolumes you may configure whether they are recreated during recovery. Click the Btrfs Options button to bring up the menu (note this option is only displayed if BTRFS volumes are present).



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.*

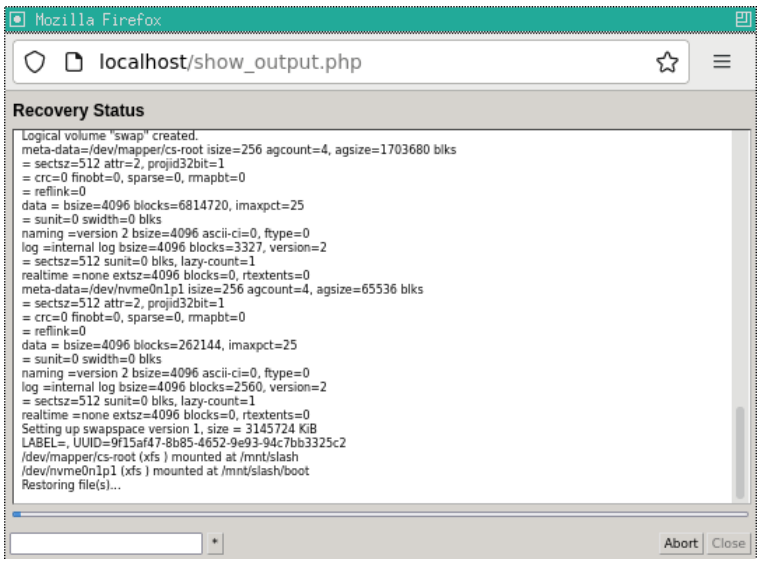
If you wish to change the Network Settings in advance of recovery, select **Post Recovery Network.** This option is only available for SLES 11 or later, and Red Hat 6 or later.



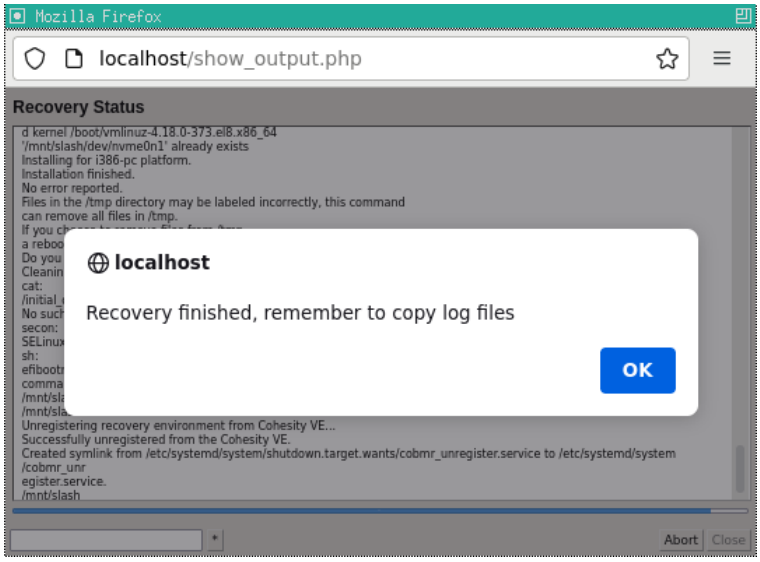
When you are satisfied that all options are correct, click OK to confirm.

> *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: CoBMR 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.

9.1 Selective Restores

Selective restores with CoBMR are not possible due to the nature of how Cohesity DataProtect restores data - there is no file/directory exclusion facility. This becomes a problem when a full backup is made that has a SAN attached and the SAN data is included in the backup.

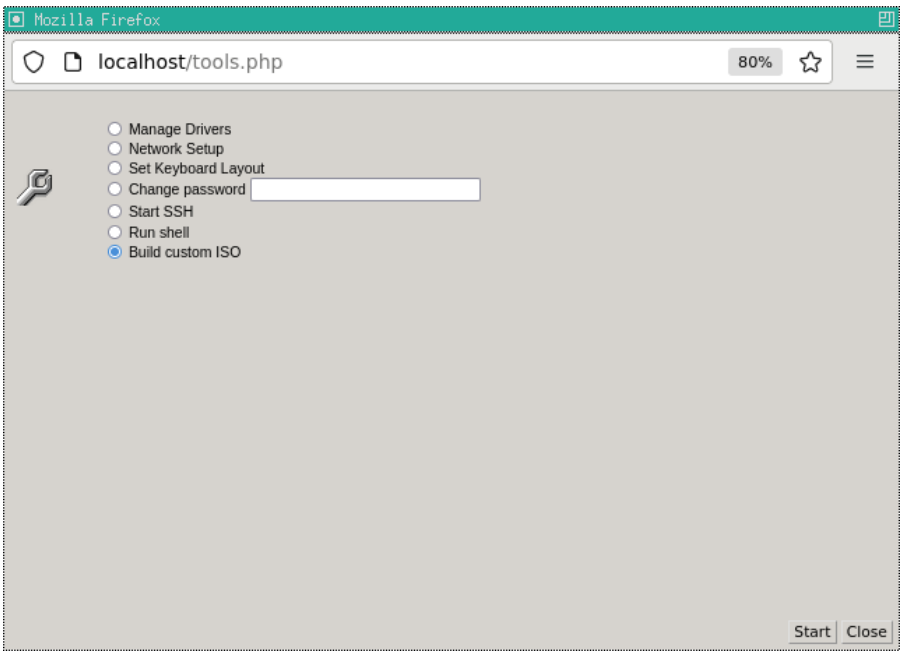
This causes recovery issues when the SAN data needs to be excluded from the recovery (say when only a single node in a cluster is to be recovered).

So to circumvent this issue configure the backups instead. You can either:

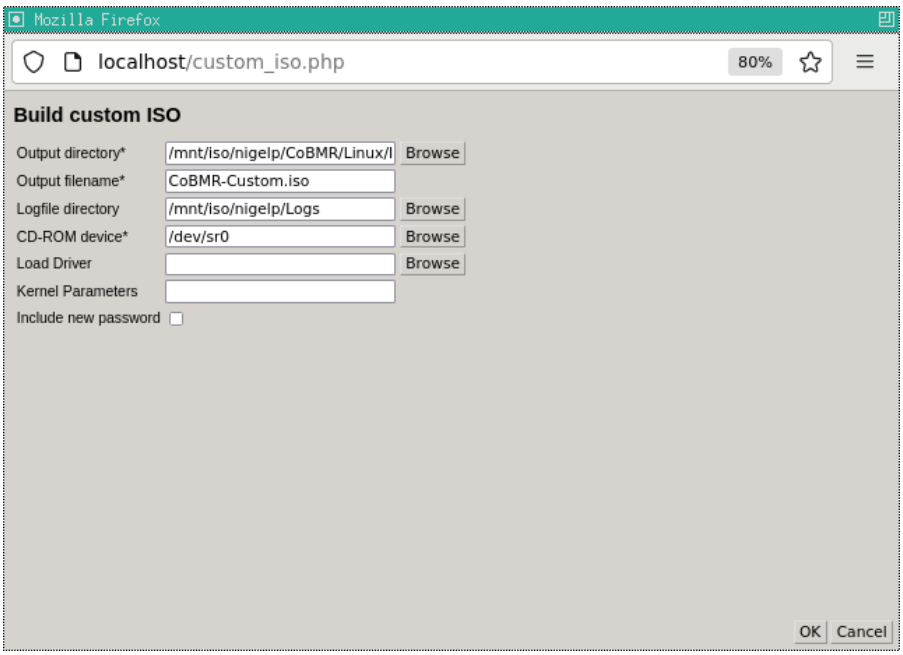
- Create multiple backup jobs - one for the root Volume Group and one for everything else.
- Create SAN mount point exclusions on the main backup job.
- Create file directives.

9.2 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:

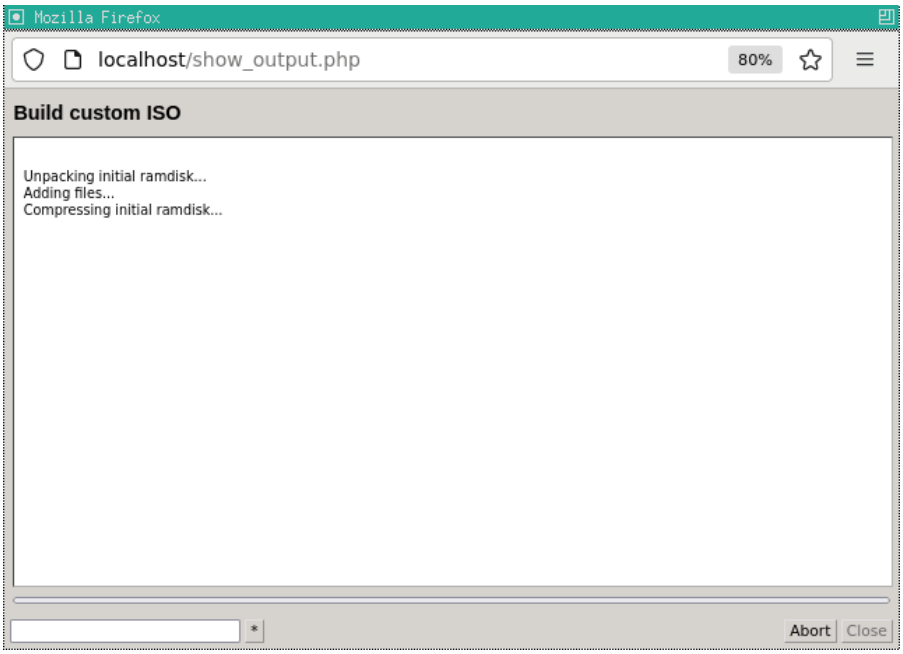


You will need to configure the following fields:

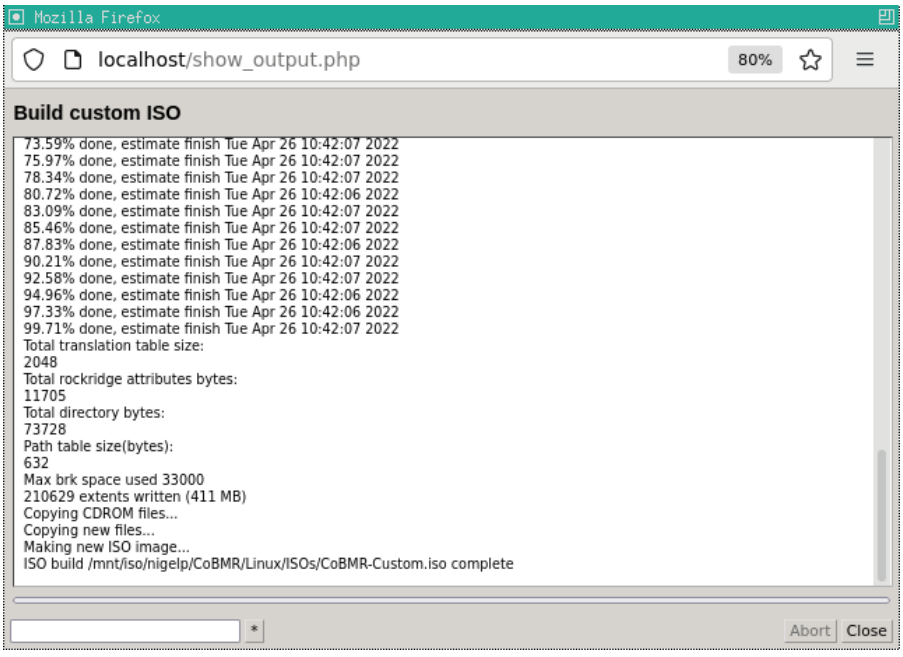
- **Output directory** is a network share (use Browse to select and mount a share).
- **Output filename** must include the .iso extension.
- **Logfile directory** is a network share (use Browse to select and mount a share).

- **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.

9.3 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 CoBMR DR principles and procedures.

The command line parameters supplied to the script are divided into 3 groups, **Network**, **Mount**, and **General**, as follows:

Network options:

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

Mount options:

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

General options:

--help	Show help message and exit
--sshd=<1|0>	Start ssh daemon if value=1
--reload=<string>	Reload module with options
--passwd=<string>	Set password for SSH and HTTP
--find_multipaths=<yes|no>	Set find_multipaths option in multipath.conf
--disshw=<1|0>	Turn on dissimilar hardware support if value=1
--mpath=<1|0>	Turn on multipath support if value=1
--sleep=<number>	Sleep for <number> seconds
--log_dir=<path>	Copy logs to mounted <path>

--bootloader=<name>	Set bootloader to <name>
--autorelabel=<1|0>	Turn on SELinx autorelabel if value=1
--convert_to_mbr	Supply when recovering an EFI system to an MBR target
--product=<type>	One of abmr, cbmr, cobmr, nbmr or tbmr

Example (a TBMR recovery)

```
restore --product=tbmr --reload="ibmveth old_large_send=1" --ethtool="-K eth0 tso o
        --ip_address="10.10.10.186" --netmask="255.0.0.0" --hostname="cristie1"
        --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" --mpath="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.

10 Post Recovery Options

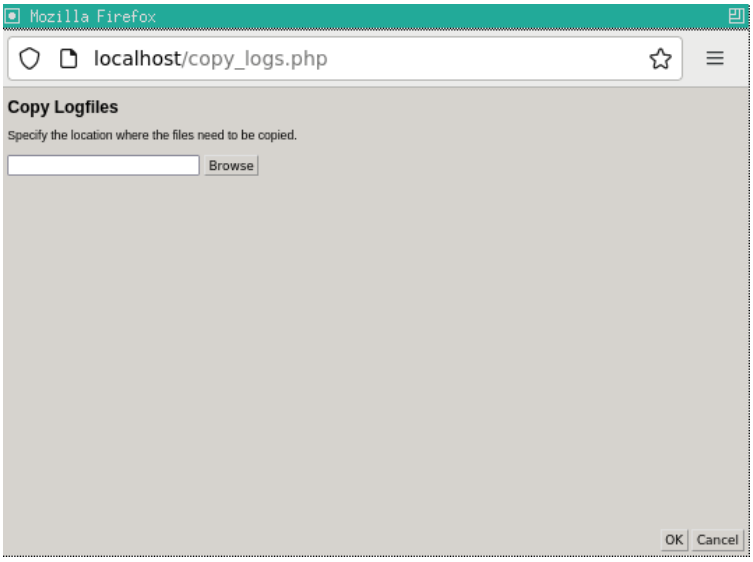
After performing a recovery, it is possible to undertake the following actions:

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

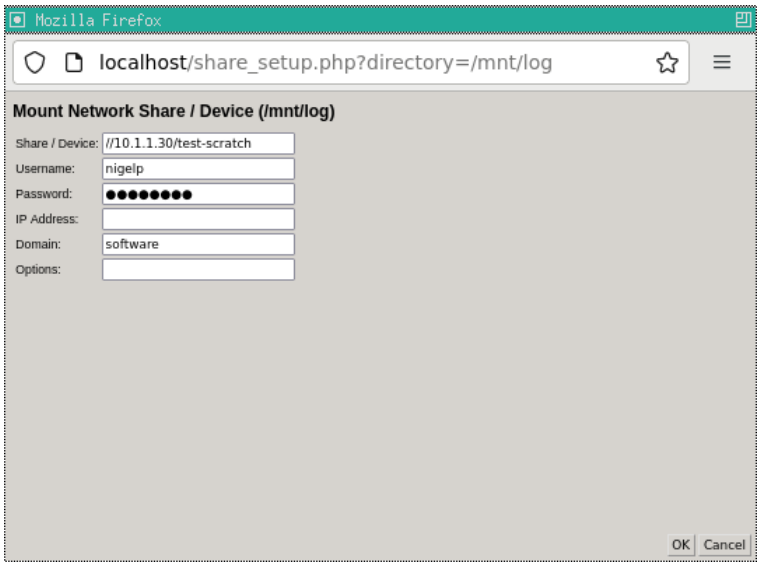
10.1 Copy Log Files

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

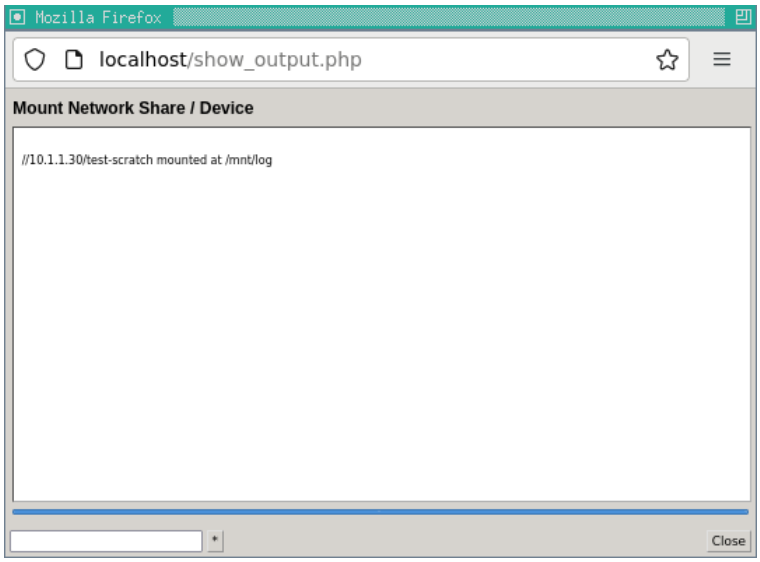
Click Browse to select a location to copy the log files to.



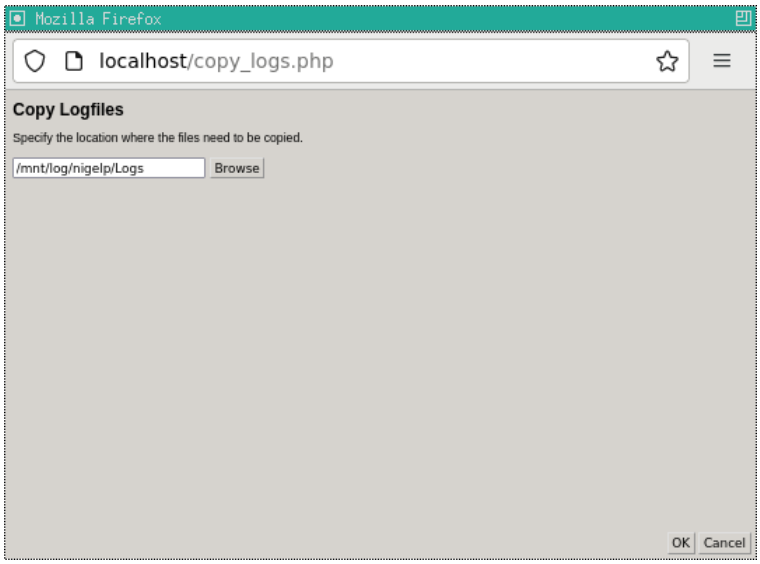
Select Browse to mount a network drive.



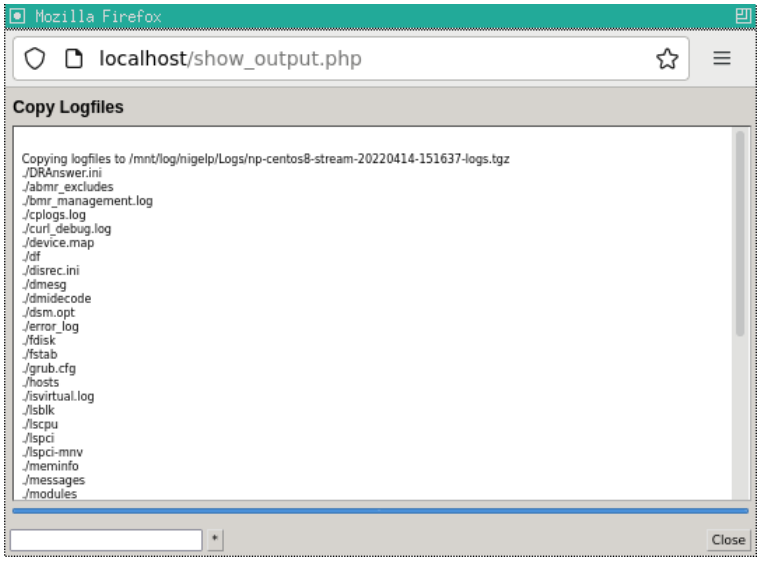
A successful mount is signified by:



Select a directory on the mounted share:



Click OK to copy the logfiles.



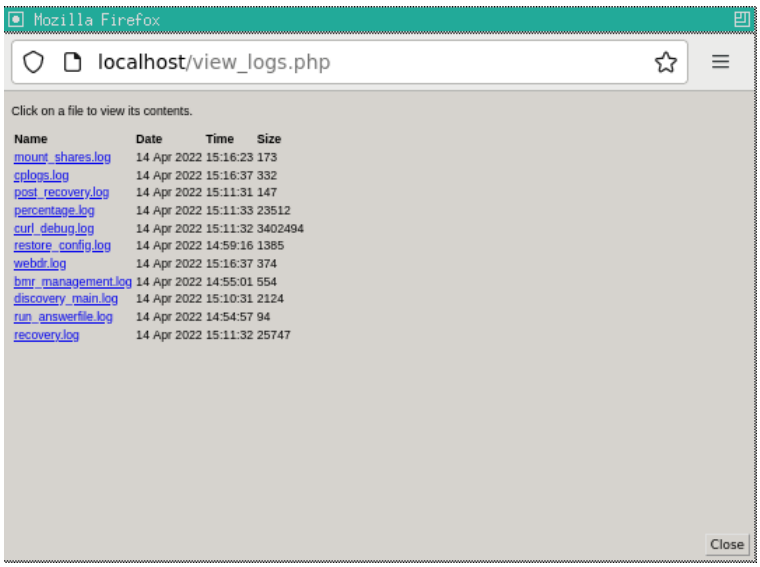
Ensure this is a location which can be easily accessed in case there is a need to email the log files to Cristie for support purposes.

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.***

10.2 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.

11 Cristie Technical Support

If you have any queries or problems concerning your Bare Machine Recovery for Cohesity 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:

- CoBMR 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.