CBMR For Linux

Cristie Bare Machine Recovery

User Guide

Version 9.6.1 released April 2024

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

- *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

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

Cristie Bare Machine Recovery (CBMR) for Linux provides disaster recovery capability for Linux based systems.

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 machine using CBMR. More detailed information is available from `man` pages for the CBMR components. The `man` pages are available after installation of CBMR.

This guide relates to CBMR for Linux version 9.6.1 only.

> ***Note: CBMR can be used independently or in conjunction with IBM Spectrum Protect (TSM).***

This guide describes how to:

- *Create a Backup Location*
- *Save Configuration Data*
- *Configure and run your Cristie CBMR Client backup*
- *Perform a Disaster Recovery*

2.1 Limitations

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

- *Platforms other than Intel 64bit.*
- *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 CBMR may be found in the **Cristie Knowledge Base** (https://kb.cristie.com) or the **Cristie Forum (**https://forum.cristie.com).

3 System Requirements

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

> ***If using IBM Spectrum Protect (TSM), the system should have IBM Spectrum Protect (TSM) API client version 7.1 or later 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 support for CBMR Version 9.6.1.

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

4 Supported File Systems

Please refer to this web page https://www.cristie.com/support/matrix/ to determine the latest file system support for CBMR 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:-

```
cbmrcfg -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 CBMR For Disaster Recovery

Cristie CBMR will recover your Linux machine in the event of a disaster. It can backup to tape drives, files, IBM Spectrum Protect (TSM) and cascaded devices.

The process may be run either from the Command line or a GUI interface. Backups can be taken periodically to reflect the changing content of the machine. In order to be able to recover this data, the machine configuration information must also be saved. This includes details of hard disks and network interfaces.

CBMR recognises three components needed for the recovery of any computer. Each of these elements will change at a different rate and is therefore best backed up on separate schedules. They are:

- **Configuration data** - defining the structure of the machine and its network characteristics
- **DR Backup data** - required to recover the operating system on that structure
- **Application data** - required to recover the applications and user data on top of the basic operating system

The main steps when performing the DR backup for the first time are:

- **Create a Backup Location**
- **Save Configuration Data**
- **Perform a DR Backup**

The main steps when performing a recovery of the operating system are:

- **Boot the Cristie Recovery Environment (XBMR)**
- **Establish Network connection**
- **Load Configuration Data**
- **Recreate the disk structure**
- **Restore the OS files from the DR Backup**
- **Reboot to the recovered OS**

Thereafter you should recover the Application data.

7 Performing a DR Backup

The process of performing a Data Recovery backup requires three steps:

- **Create a Backup Location** - which defines where the backup data will be stored.

  See Creating a Backup Location
- **Save the Configuration Data** - see Saving Configuration Data
- **Perform a DR Backup** - to the storage device. See Performing the DR Backup

7.1 Creating a Backup Location

A **Backup Location** is a definition of the entity to which you will backup data.

CBMR can backup to tape drives, tape libraries, virtual tape drives (files), incremental backups (files), IBM Spectrum Protect (TSM) Nodes and cascaded locations. The simplest way of creating a device is to use the GUI. However, you may also create the definition with a text editor.

The Backup Location definition is used in both the DR Backup and the Configuration Data. It only needs to be created once.

7.1.1 Creating a Backup Location using a Command Line Interface

It is unusual to define storage devices without the GUI. However, provided that you do not need to enter an encrypted password, you may use a text editor to create a **devices.ini** file.

Only IBM Spectrum Protect (TSM) and File Backup Locations can be handled this way. The **devices.ini** file which is located in `/etc/cbmr` could be amended or created with entries like:

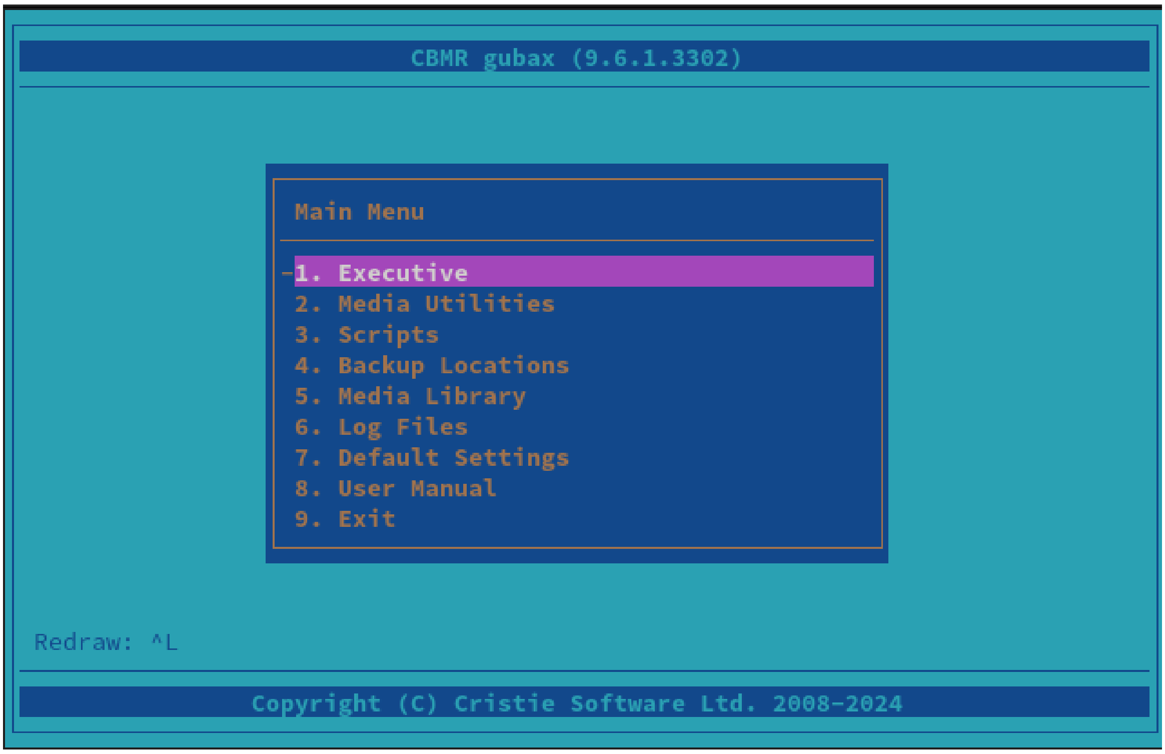
```
[CBMRLinux]
Class = 4
Path=/mnt/linux/backups/drbackup.vtd
SizeInMB=0
Remote=0
```

The example shows a VTD file backup type located on a mounted network share.

> ***It is not recommended that this be done with an editor. Backup Locations are best defined using the GUI.***

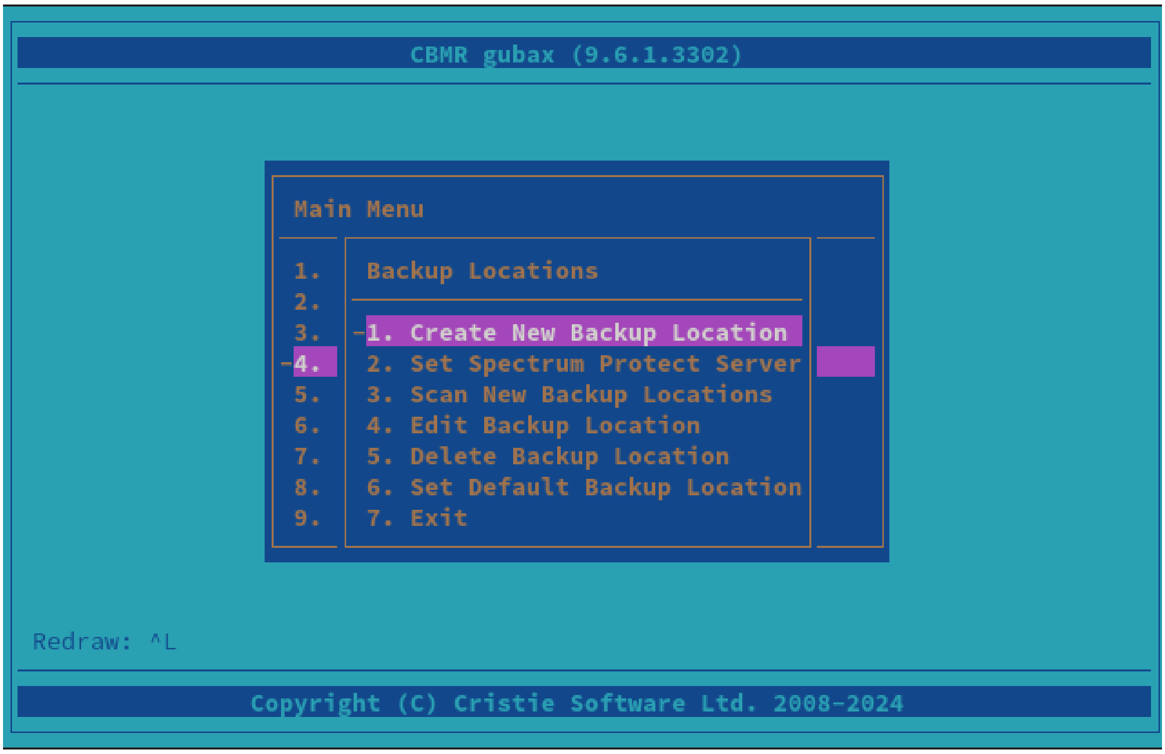
7.1.2 Creating a Backup Location using a Graphical User Interface

To run GUBAX, type `gubax` in a terminal session. This will show the main menu:



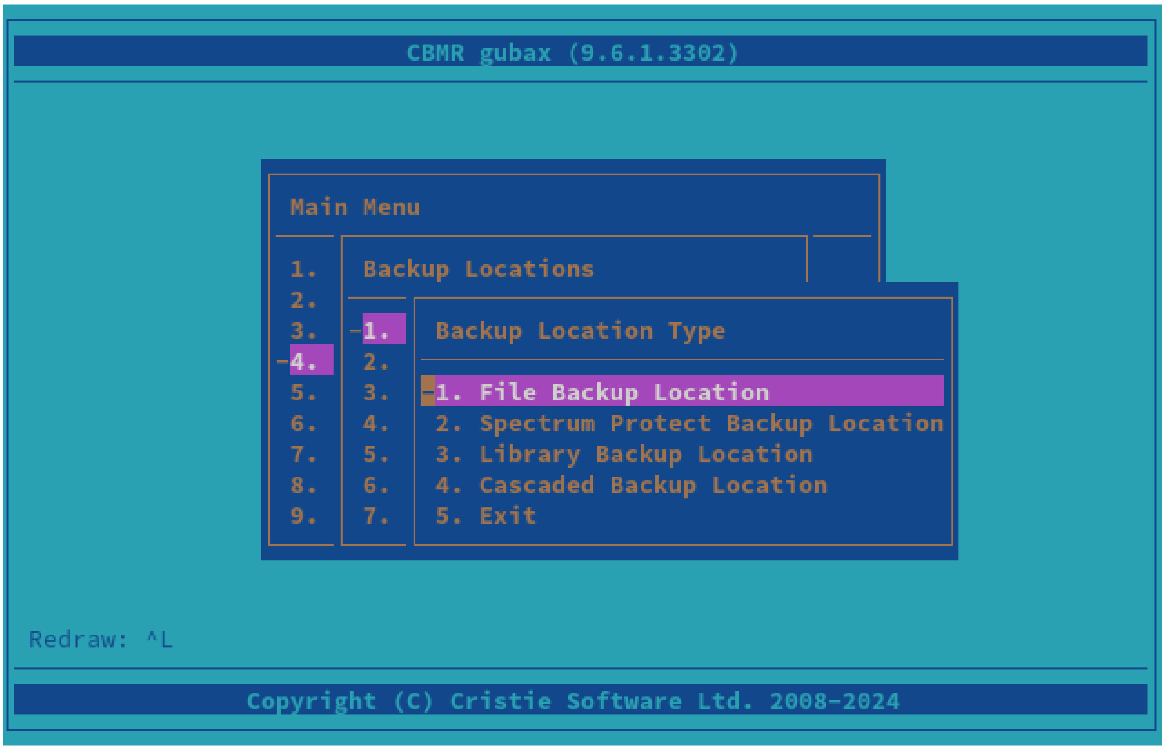
```
                         CBMR gubax (9.6.1.3302)

                  Main Menu

                 -1. Executive
                  2. Media Utilities
                  3. Scripts
                  4. Backup Locations
                  5. Media Library
                  6. Log Files
                  7. Default Settings
                  8. User Manual
                  9. Exit

  Redraw: ^L

              Copyright (C) Cristie Software Ltd. 2008-2024
```

Before you start a DR Backup or save your Configuration Data, you need to configure a Backup Location to define the location to which the data will be backed up. Select **Backup Locations** from the main menu.



```
                         CBMR gubax (9.6.1.3302)

                  Main Menu

                  1.   Backup Locations
                  2.
                  3.  -1. Create New Backup Location
                 -4.   2. Set Spectrum Protect Server
                  5.   3. Scan New Backup Locations
                  6.   4. Edit Backup Location
                  7.   5. Delete Backup Location
                  8.   6. Set Default Backup Location
                  9.   7. Exit

  Redraw: ^L

              Copyright (C) Cristie Software Ltd. 2008-2024
```

Next, choose the type of backup:



```
CBMR gubax (9.6.1.3302)

Main Menu

1.   Backup Locations
2.
3.  -1.  Backup Location Type
-4.  2.
5.   3.  -1. File Backup Location
6.   4.   2. Spectrum Protect Backup Location
7.   5.   3. Library Backup Location
8.   6.   4. Cascaded Backup Location
9.   7.   5. Exit

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2024
```

Each backup location type is now discussed.

7.1.2.1 File Backups

A File Backup Location allows you to save your complete system to a file location of your choice. There are two types of File Backup that can be created, an incremental backup (.tar.gz) or a full backup (.vtd).

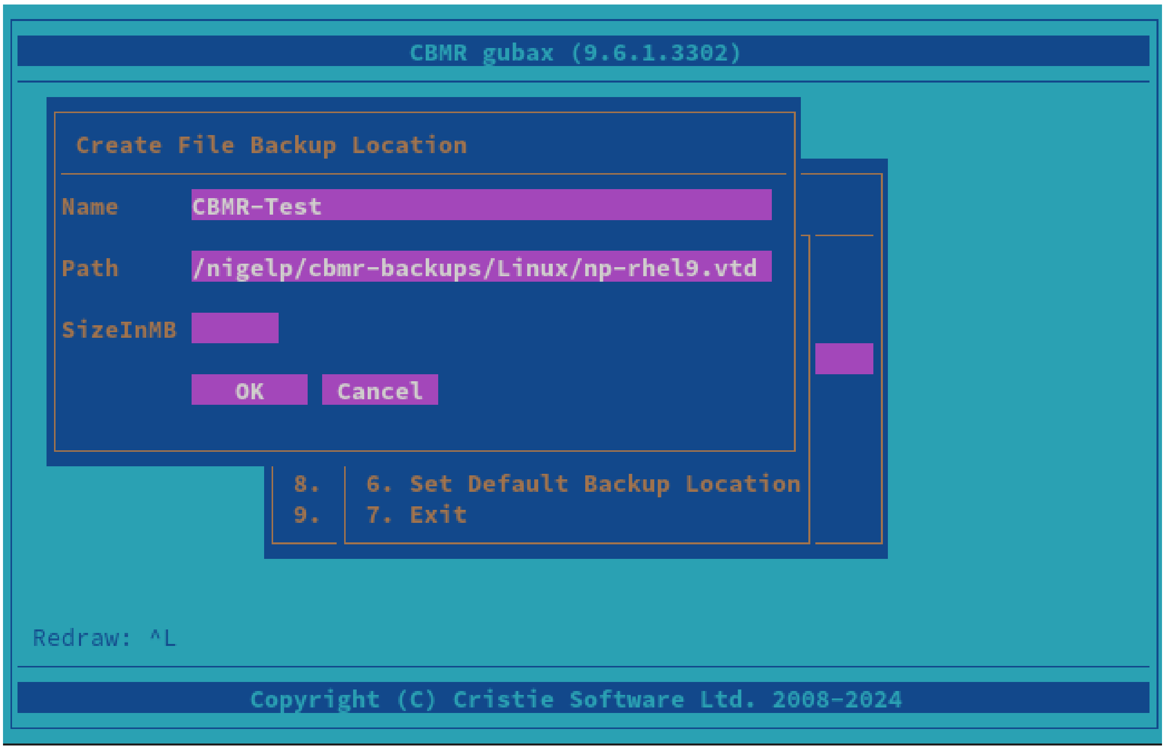
An incremental backup will store the file difference between the last and next backup stored in a compressed .tar.gz format. A full backup will always save a complete copy of the filesystem stored in a .vtd format.

If you wish to backup to a file, probably located on a network share, choose File Backup Location.

> *Note: creating the file backup location does NOT create the file itself - this is created when you start the first backup.*

Complete the form with your details and select OK to confirm. The entries shown in the example below are for illustration only:

Full Backup Configuration



```
CBMR gubax (9.6.1.3302)

Create File Backup Location

Name      CBMR-Test
Path      /nigelp/cbmr-backups/Linux/np-rhel9.vtd
SizeInMB
          OK   Cancel

    8.   6. Set Default Backup Location
    9.   7. Exit

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2024
```

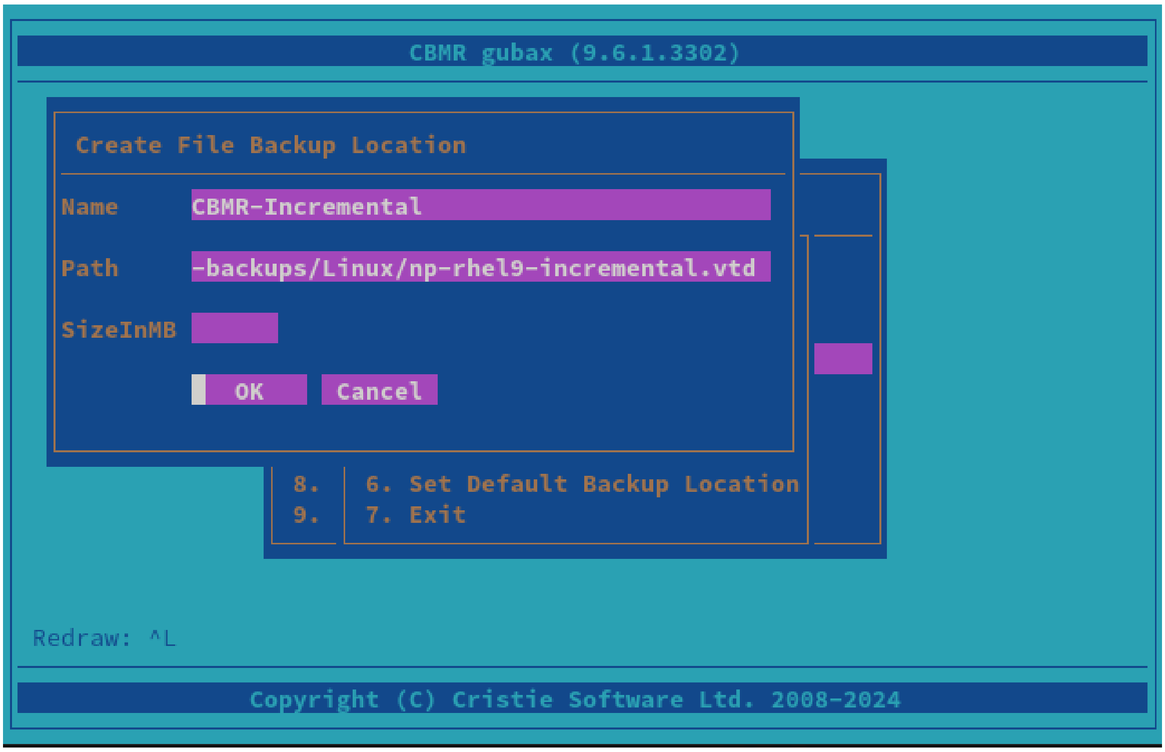
A full backup is created as a .VTD (Virtual Tape Drive) file. The path, which is case sensitive, defines the location where the VTD file should be created. This can be to the local filesystem or to an external NFS/CIFS share via its mount point (which must already be mounted).

It is recommended that you leave `SizeInMB` blank.

`SizeInMB` will set a maximum size to the file; by leaving this blank it will allow it to expand until it is complete or there is no more space on the disk.

> *Note: if you do set the maximum size of the file and the backup and the file reaches that size and needs to write more, you will get the message 'Please mount Volume 1'. There is no way to extend the current file or attach another file and the process should be restarted. If you wish to limit the size of the file because of disk space limitations, then consider creating this as one of several files in a Cascaded Backup Location.*

Incremental Backup Configuration



```
CBMR gubax (9.6.1.3302)

Create File Backup Location

Name       CBMR-Incremental
Path       -backups/Linux/np-rhel9-incremental.vtd
SizeInMB

           OK    Cancel

8.   6. Set Default Backup Location
9.   7. Exit

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2024
```

Incremental backups are stored in TGZ (tar/zip) format. The backup path, which is case sensitive, defines the directory location where all the incremental .tar.gz files are created. This can be a local filesystem or an external NFS/CIFS share via its mount point (which must already be mounted). If you specify a VTD location, the incremental backups will be created within the same directory as the VTD.

> *Note: if you specify a VTD location in the PATH field e.g. /mnt/linux/backup.vtd to use Full Backups you can still use Incremental Backups. The incremental backup files will be stored in the same directory as the VTD file.*

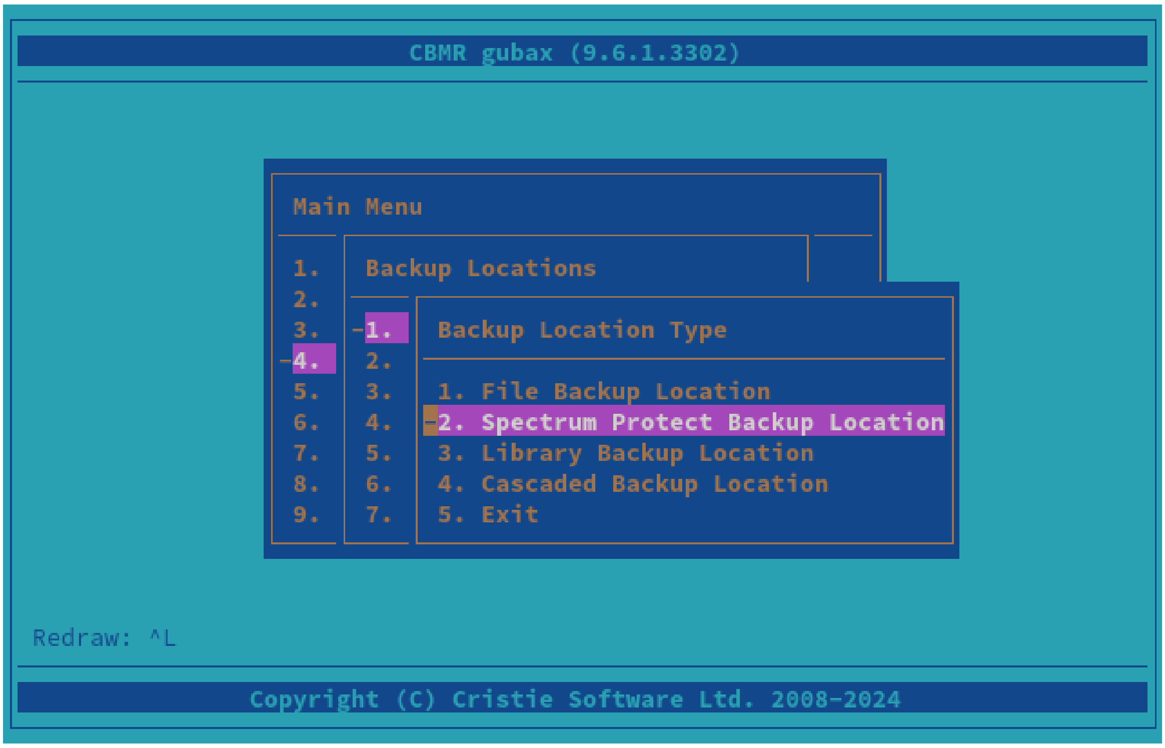
7.1.2.2 IBM Spectrum Protect (TSM) Backups

CBMR can be used in conjunction with IBM Spectrum Protect (TSM) to utilize IBM Spectrum Protect (TSM)'s centralised storage management benifits. CBMR treats a node as though it were a tape. This means that there are some restrictions to the way in which CBMR can be configured and used with IBM Spectrum Protect (TSM).

The node must be reserved for sole use by CBMR and may not be shared with any other process, particularly the BA Client. The node must also be set up with the options:

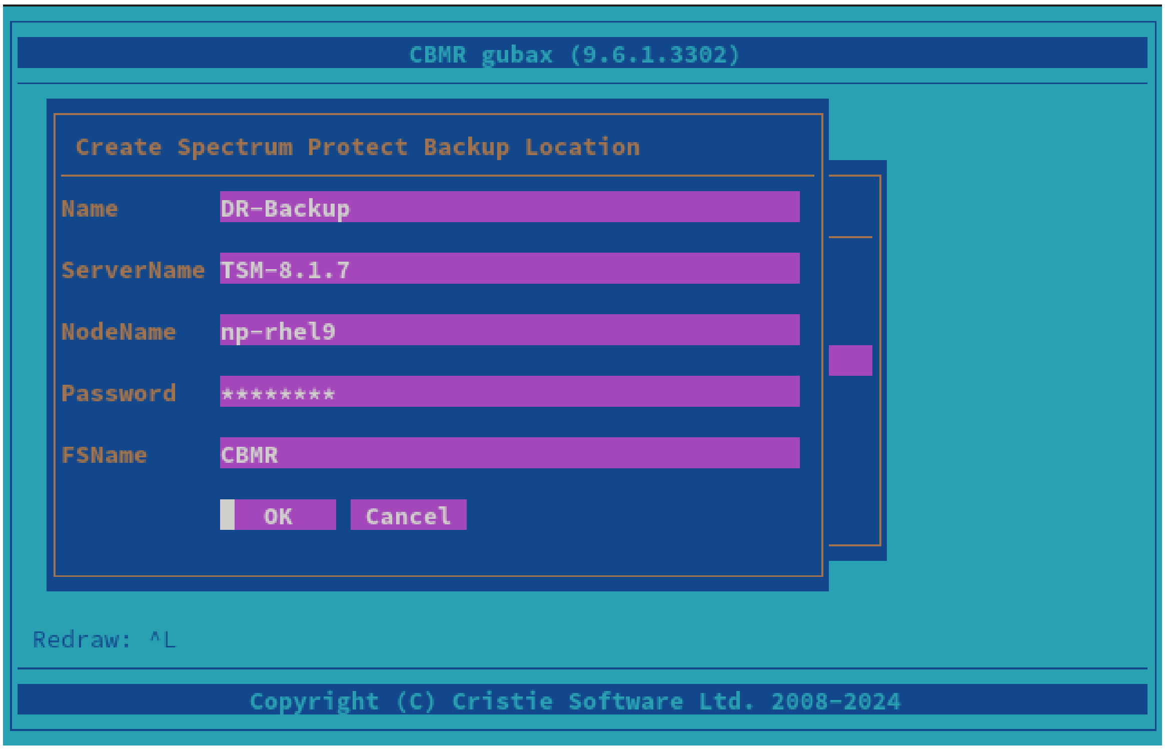
- Backup Delete Allowed = Yes
- Archive Delete Allowed = Yes
- Password Expires = 0

If you wish to backup to a node on your IBM Spectrum Protect (TSM) server, choose Spectrum Protect Backup Location from the **Backup Location Type** menu:



```
                          CBMR gubax (9.6.1.3302)

              Main Menu

              1.   Backup Locations
              2.
              3.  -1.   Backup Location Type
             -4.   2.
              5.   3.   1. File Backup Location
              6.   4.  -2. Spectrum Protect Backup Location
              7.   5.   3. Library Backup Location
              8.   6.   4. Cascaded Backup Location
              9.   7.   5. Exit

  Redraw: ^L

              Copyright (C) Cristie Software Ltd. 2008-2024
```

Then fill in the form with the IBM Spectrum Protect (TSM) node details that apply to your backup. The example below is for illustration purposes only:

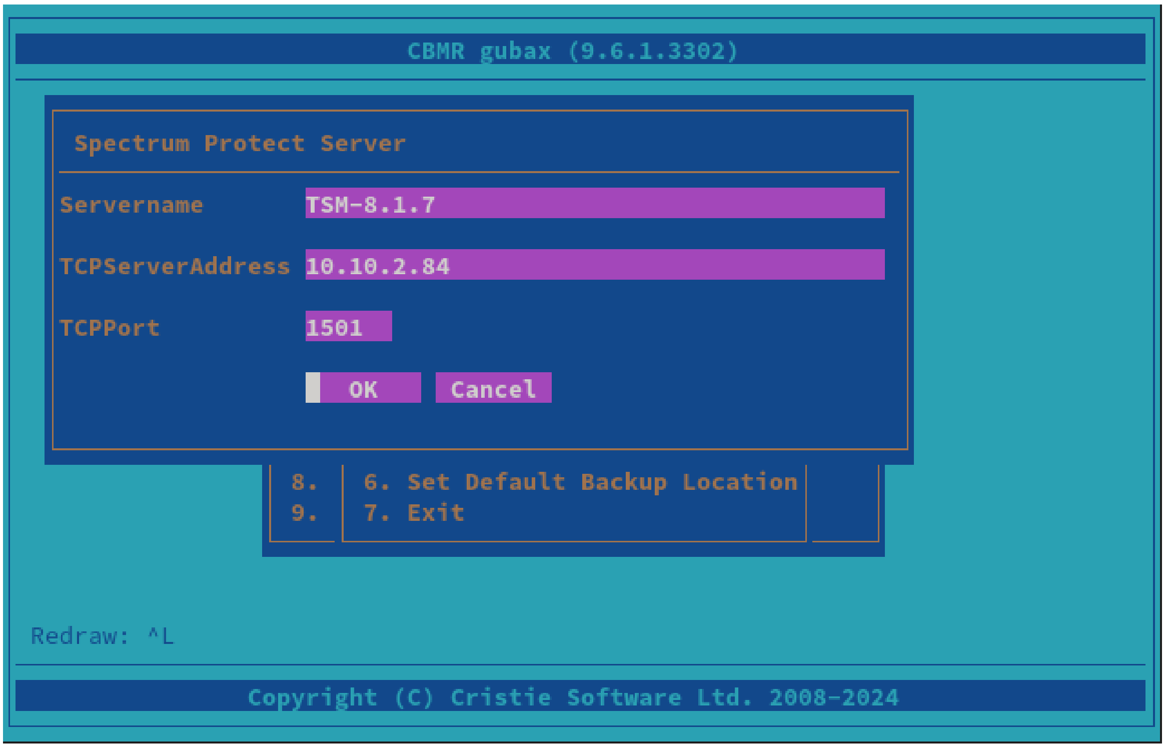


```
                          CBMR gubax (9.6.1.3302)

   Create Spectrum Protect Backup Location

  Name          DR-Backup

  ServerName    TSM-8.1.7

  NodeName      np-rhel9

  Password      ********

  FSName        CBMR

                  OK        Cancel

  Redraw: ^L

              Copyright (C) Cristie Software Ltd. 2008-2024
```

There is no validity check of the parameters at this time; they will be validated when you attempt the first backup. The Filespace will also be created by the first backup if it does not already exist.

For a IBM Spectrum Protect (TSM) Backup Location, you also need to provide connection information for the IBM Spectrum Protect (TSM) Server so that it can be accessed. This data is specified in the file `dsm.sys`.

If you have not already created the file, you may do so by selecting Set Spectrum Protect Server from the menu:



```
CBMR gubax (9.6.1.3302)

 Spectrum Protect Server

Servername        TSM-8.1.7
TCPServerAddress  10.10.2.84
TCPPort           1501

                   OK     Cancel

      8.  | 6. Set Default Backup Location
      9.  | 7. Exit

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2024
```

This function will overwrite any existing `dsm.sys` file. Depending on your systems architecture, this file is located in either the `/opt/tivoli/tsm/client/api/bin` or `/opt/tivoli/tsm/client/api/bin` directory.

> *Backup operations with IBM Spectrum Protect (TSM) server versions 8.1.2.x or later require the use of a Secure Sockets Layer (SSL) or Transport Layer Security (TLS) certificate. This is mandatory for this server version. The certificate will need to be configured on the source system before the backup can be taken. This can be configured using the following IBM Spectrum Protect (TSM) command outside of the gubax interface:* `dsmcert -add -server <server address> -file <certificate location>`

The displayed form allows you to specify the basic parameters for connecting to the IBM Spectrum Protect (TSM) server over TCP/IP. The parameters are written into `dsm.sys`.

> *Ensure that you use the same server name as you used on the IBM Spectrum Protect (TSM) Backup Location form.*

Transitional Nodes

If you backup to a node located on an IBM Spectrum Protect (TSM) Server version 7.1.8 or 8.1.2 and above, using an IBM Spectrum Protect (TSM) 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 IBM Spectrum Protect (TSM) client version 8.1.11 that enforces SSL communication. This will prevent older IBM Spectrum

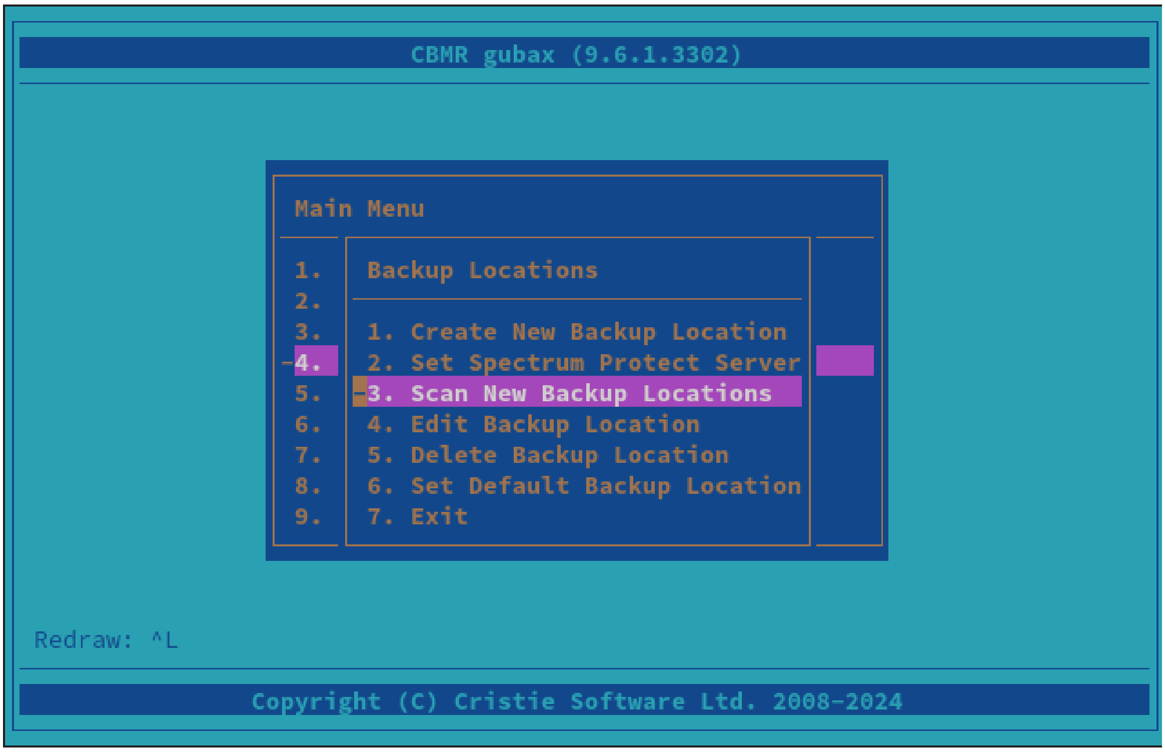
Protect (TSM) clients from accessing the node after the DR recovery.

You can update the node with the following command:

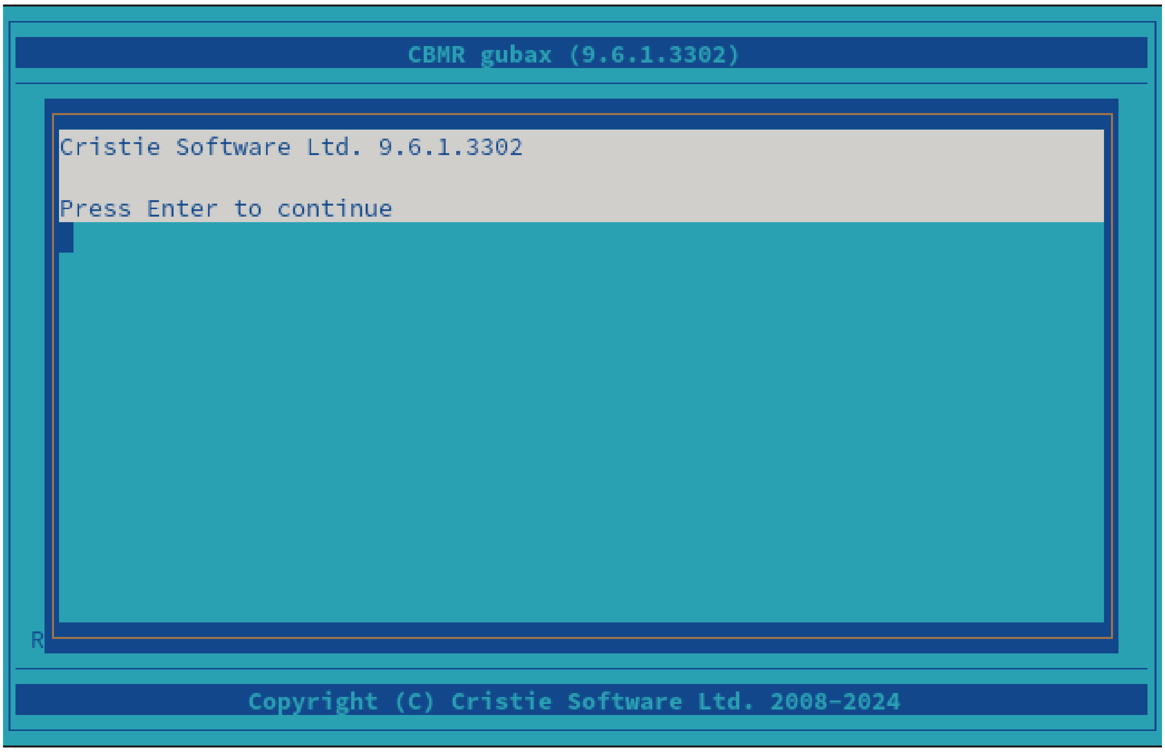
```
UPDATE <node_name> SESSIONSECURITY=Transitional
```

7.1.2.3 Tape Backups

If you are using a tape drive, this can be automatically detected by selecting the Scan New Backup Locations option from the **Backup Locations** menu as shown:



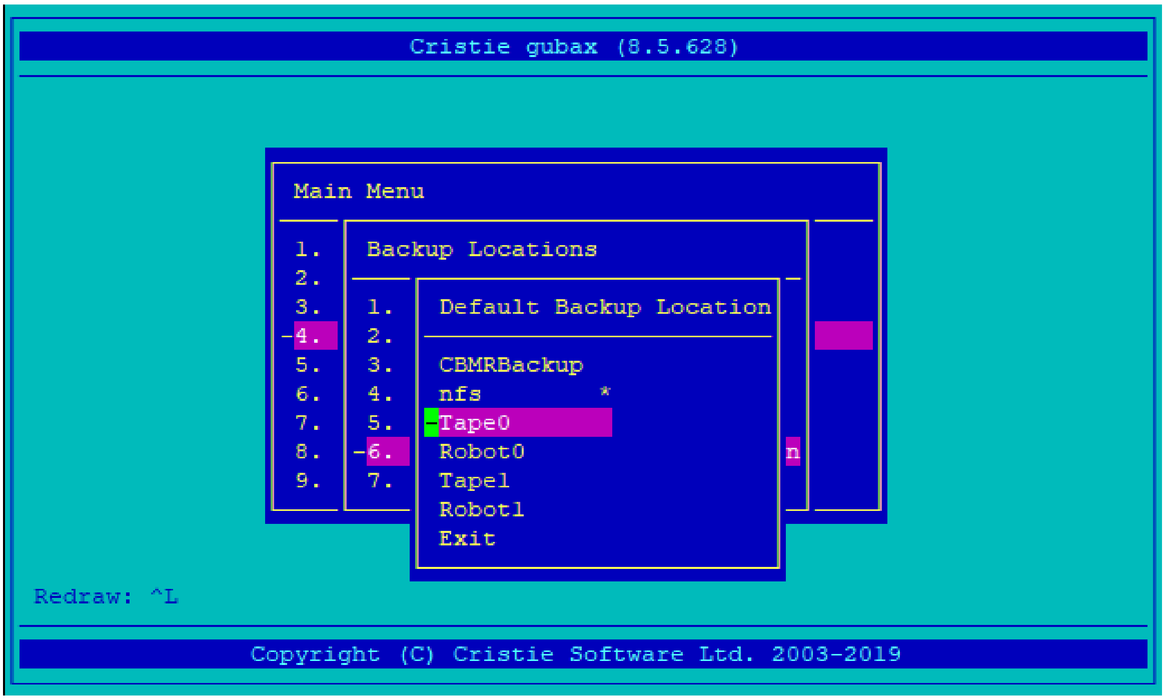
```
                         CBMR gubax (9.6.1.3302)

              Main Menu

              1.   Backup Locations
              2.
              3.   1. Create New Backup Location
             -4.   2. Set Spectrum Protect Server
              5.  -3. Scan New Backup Locations
              6.   4. Edit Backup Location
              7.   5. Delete Backup Location
              8.   6. Set Default Backup Location
              9.   7. Exit

 Redraw: ^L

              Copyright (C) Cristie Software Ltd. 2008-2024
```



```
CBMR gubax (9.6.1.3302)

Cristie Software Ltd. 9.6.1.3302

Press Enter to continue

Copyright (C) Cristie Software Ltd. 2008-2024
```

Any new devices found will be listed and then be available to choose as a default device by selecting Set Default Backup Location.

Note: if no device is listed during the scan it may have still been discovered. Check the Set Default Backup Location menu to check if the tape device has been detected.



Other types of device should be configured manually by selecting Create New Backup Location from the Backup Locations menu.

Library Backup Location

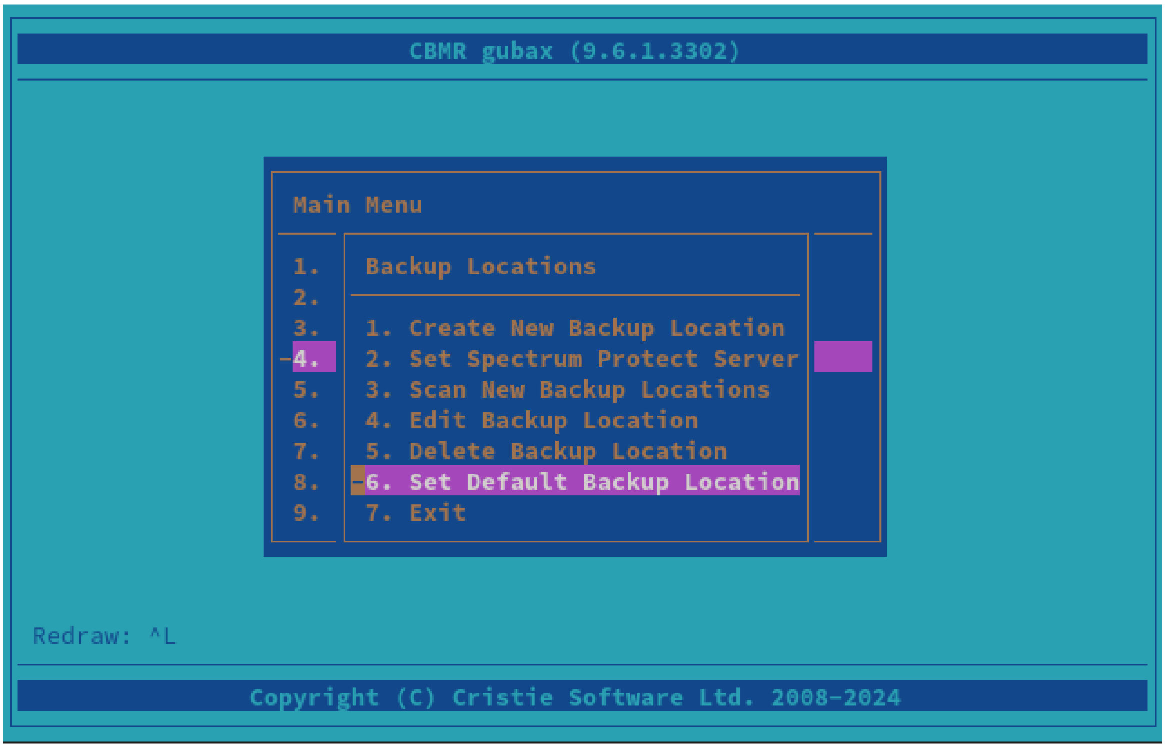
A locally attached tape library can be used as a Storage device. A CBMR library is defined as a drive and a number of tapes. You require the **CBMR Library Support** module to run this.

Cascaded Backup Location

A Cascaded Backup Location is a number of separate Backup Locations that are linked together, so that when the first fills it continues to the second, and so on. Typically one could use this on tape drives or virtual tape drives. In order to create a Cascaded Backup Location, you need first to create individual Backup Locations that you can then cascade. This type is not particularly useful in a CBMR context where speed of recovery is important.

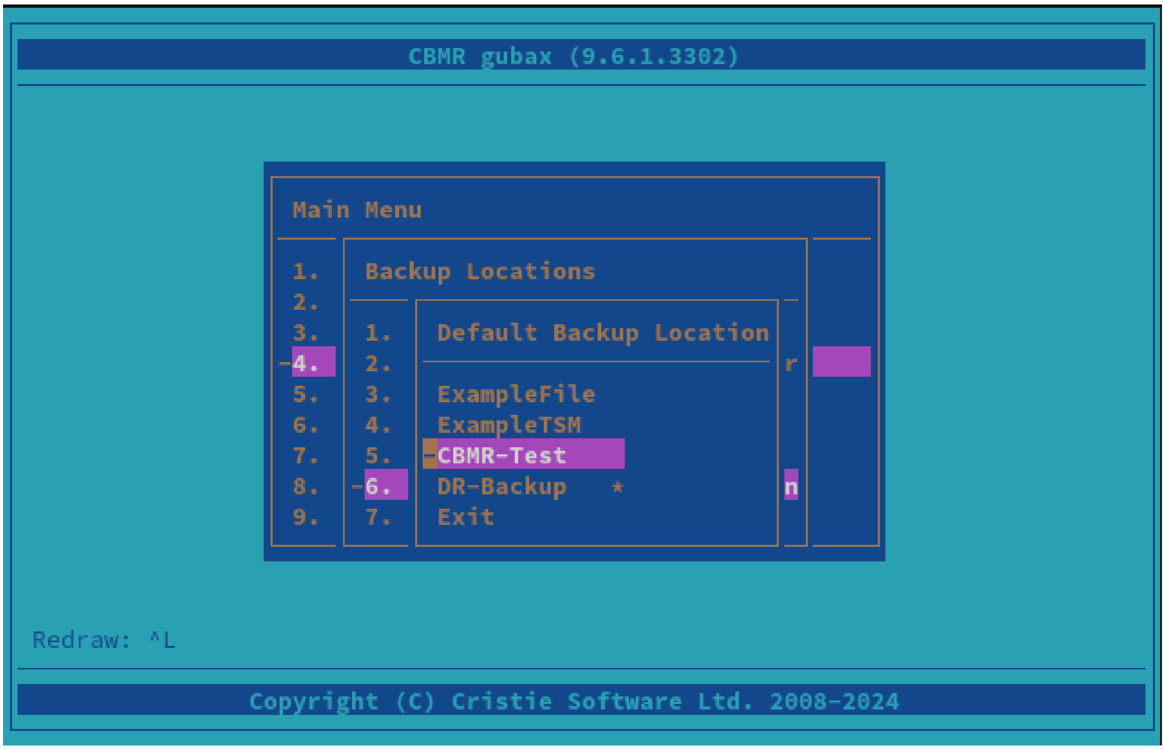
7.1.2.4 Default Backup Location

Once you have configured the backup location, you should set it as the default. Do this from the Set Default Backup Location option on the **Backup Locations** menu.



```
                      CBMR gubax (9.6.1.3302)


               Main Menu

               1.  Backup Locations
               2.
               3.  1. Create New Backup Location
              -4.  2. Set Spectrum Protect Server
               5.  3. Scan New Backup Locations
               6.  4. Edit Backup Location
               7.  5. Delete Backup Location
               8. -6. Set Default Backup Location
               9.  7. Exit


 Redraw: ^L

            Copyright (C) Cristie Software Ltd. 2008-2024
```

The device name marked with an asterisk (*) is the current default device. Select the device that you want to be the Default and press Enter.



7.2 Saving Configuration Data

Configuration information, including details of disks and network configuration, must be saved for each machine to be recovered. This may be saved to a unique external disk drive for each machine, or to a central configuration store located on a network share.

To save the configuration information for each machine, the command line program `cbmrcfg` is used. The Cristie recommended way to store the configuration is “as part of the backup”. This will save the configuration to a folder on the root file system and automatically included as part of the backup.

7.2.1 Saving Configuration Data Using CBMRcfg

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

```
cbmrcfg --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:

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

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

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

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

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>
--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

Include `cbmrcfg` in your backup script to run every time a backup is performed.

7.3 Performing the DR Backup

Files may be backed up from the command line program `ubax` or graphical program `gubax` for VTD File Backups, IBM Spectrum Protect (TSM) Backups and Tape Backups. Incremental Backups may be performed using the command line program `cbmr_backup`.

7.3.1 Performing a DR Backup using the Command Line Interface

To use the command line backup program `ubax`, you should first configure a storage device. the steps required for this are explained in the previous section Creating a Backup Location using a Command Line Interface. This only needs to be done once.

Once you have confirmed that the default backup location is correctly configured, you may back up the machine using the default script by using the following:

File Backups (VTD), IBM Spectrum Protect (TSM) and Tape Backups

```
ubax -b /etc/cbmr/scripts/cbmr.scp
```

The **Backup Location** definitions are held in the file `/etc/cristie/devices.ini`. Each location definition starts with the symbolic name of the location eg. `[ExampleLocation]`.

The file `/etc/cbmr/ubax.ini` must contain the symbolic name of the default location in the following form:

```
DefStorageDev=”ExampleLocation”
```

There are many command line options available for `ubax` which are described in the manual page which is available by typing `man ubax`.

Incremental Backups

Incremental Backups use '*forward incremental*' backup algorithms to allow recoveries to be made to a specific point-in-time. So, for example, the following command will backup the root directory and subdirectories, ignoring any special filesytems e.g. tmpfs, NFS, etc.:

```
cbmr_backup /
```

A `machine.tar.gz` file will be created in the configured directory (refer to the topic Create a File Backup Location). Running the command multiple times will create incremental files with an incrementing numerical value e.g. machine.tar.gz.1. There are no limits to the number of incremental files created. To regenerate the base `machine.tar.gz`, all the incremental files including the first `machine.tar.gz` must be deleted or moved out of the backup location.

`cbmr_backup` can also be used to incrementally backup and restore directories or files on the running system. Type `cbmr_backup` for usage details.

To restore an incremental backup version use the flags `-V <number> -r <path/to/restore/to> <path/you/want/to/recover>` e.g. `cbmr_backup -V 2 -r /home/testuserrestored /home/testuser`.

A list of backup versions can be viewed by typing `cbmr_backup -l`. Backup version numbers start at 2. To retrieve the first backup, machine.tar.gz, use `-V 2`, to restore from machine.tar.gz.1 (including all the previous versions i.e. machine.tar.gz and machine.tar.gz.0) use `-V 4`. To restore all the incremental versions do not set the `-V` flag.

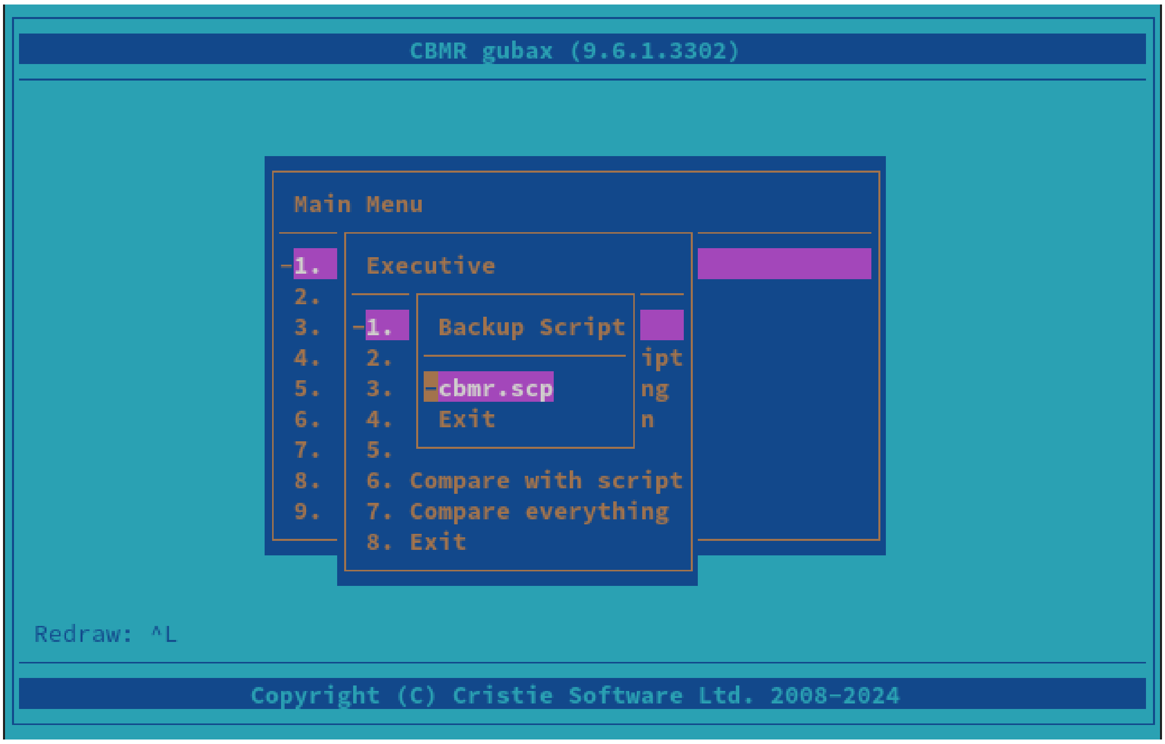
7.3.2 Performing a DR Backup using the Graphical User Interface

Before you perform a DR backup you need to make sure that you have completed the instructions in Creating a Backup Location.

> ***Note: Incremental Backups can not be performed using the Graphical User Inteface - see Performing a DR Backup using the Command Line Interface***

Type `gubax` from a command line; this will show the main menu.

Select **Executive** from the main menu and then choose Backup. A list of available scripts is shown:

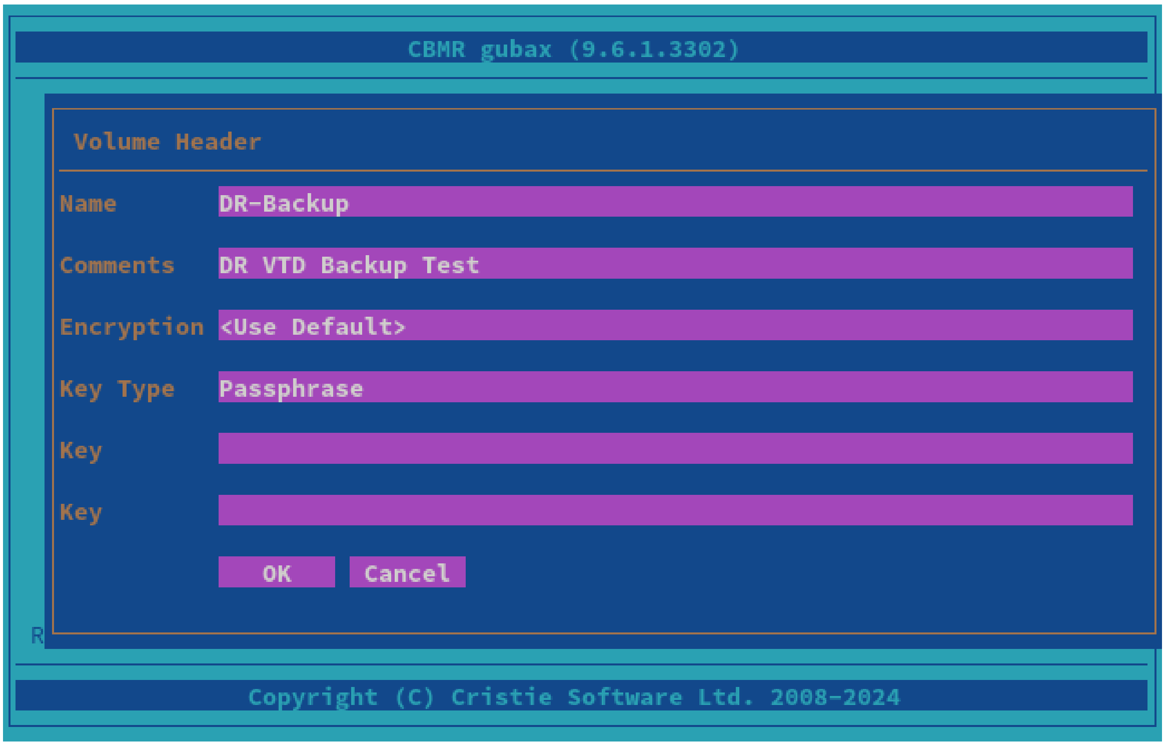


```
                         CBMR gubax (9.6.1.3302)

              Main Menu

             -1.  Executive
              2.
              3. -1.  Backup Script
              4.  2.                     ipt
              5.  3.  -cbmr.scp          ng
              6.  4.   Exit              n
              7.  5.
              8.  6. Compare with script
              9.  7. Compare everything
                  8. Exit

 Redraw: ^L
                Copyright (C) Cristie Software Ltd. 2008-2024
```

The default backup script `cbmr.scp` will backup all local file systems.

> *Note: if you wanted to include mounted CD ROMs for example, then they would need to be included specifically.*

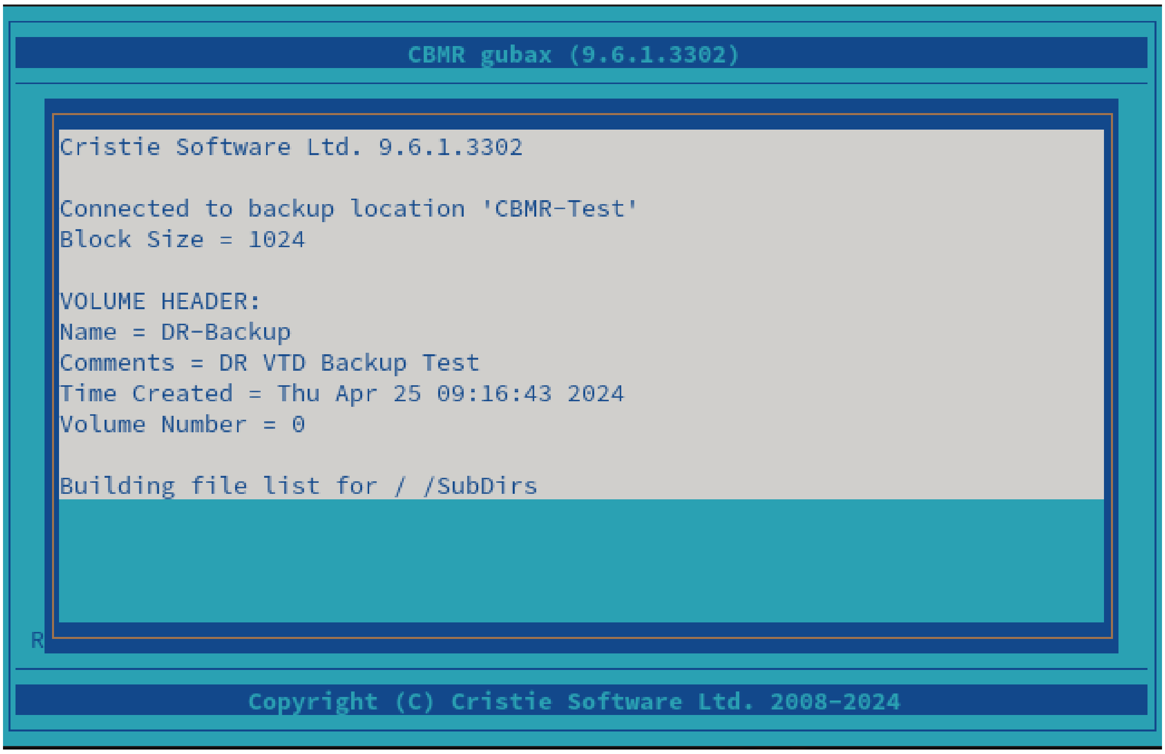
Select the script you require. Then **Volume Header** information can be specified if you wish:



```
                         CBMR gubax (9.6.1.3302)

  Volume Header

 Name        DR-Backup
 Comments    DR VTD Backup Test
 Encryption  <Use Default>
 Key Type    Passphrase
 Key
 Key
               OK     Cancel

                Copyright (C) Cristie Software Ltd. 2008-2024
```

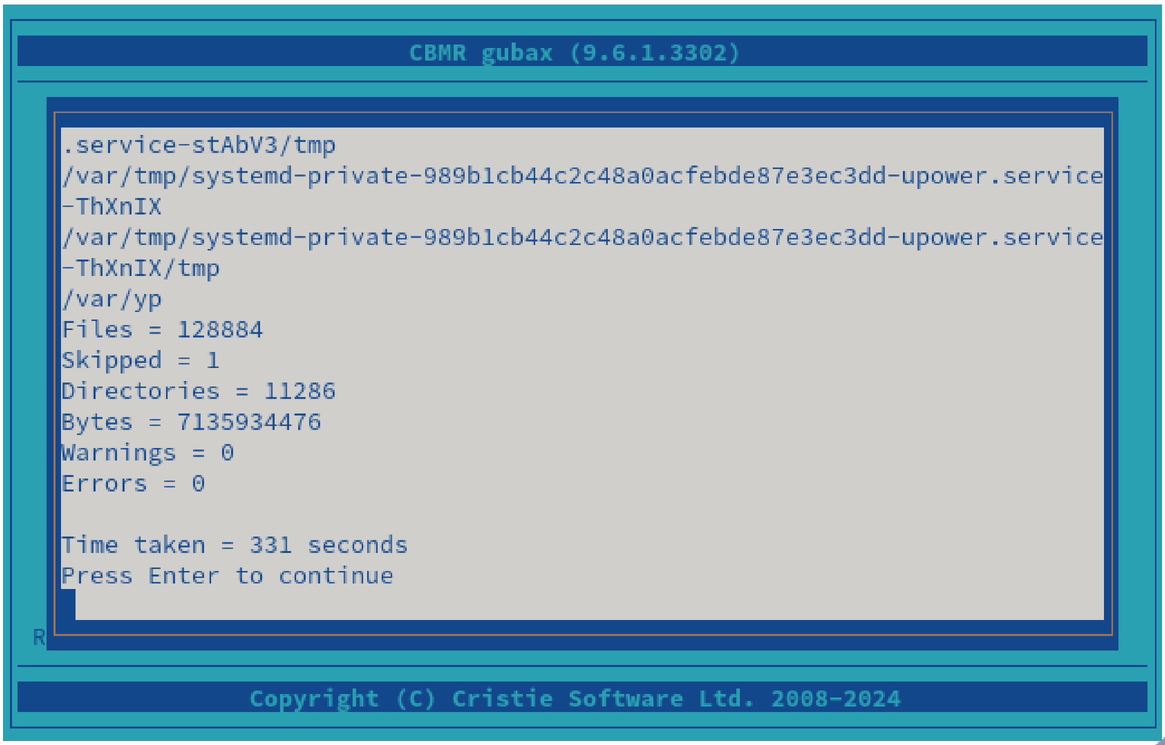
The **Volume Header** information is simply any names or comments that you wish to associate with the backup. If you wish to encrypt the backup, you may toggle through the method of encryption by pressing the up and down arrow keys when you are on the **Encryption** field. You will need to enter a key if you are encrypting your backup.

After pressing Enter on **OK**, the backup will begin (a VTD backup example is shown); an initial screen will be shown. In the example below, the Volume Header information has been left blank:



```
Cristie Software Ltd. 9.6.1.3302

Connected to backup location 'CBMR-Test'
Block Size = 1024

VOLUME HEADER:
Name = DR-Backup
Comments = DR VTD Backup Test
Time Created = Thu Apr 25 09:16:43 2024
Volume Number = 0

Building file list for / /SubDirs
```

The backup completes with a summary message:



```
.service-stAbV3/tmp
/var/tmp/systemd-private-989b1cb44c2c48a0acfebde87e3ec3dd-upower.service
-ThXnIX
/var/tmp/systemd-private-989b1cb44c2c48a0acfebde87e3ec3dd-upower.service
-ThXnIX/tmp
/var/yp
Files = 128884
Skipped = 1
Directories = 11286
Bytes = 7135934476
Warnings = 0
Errors = 0

Time taken = 331 seconds
Press Enter to continue
```

All scripts are located in `/etc/cristie/scripts/`. You can create your own script with the GUI by selecting **Scripts**, then Create New Script. This will open a new script with the vi editor.

Example Script

`cbmr.scp` will backup the whole machine and contains the following commands:

Script Text	Meaning
`Mode=Overwrite`	Overwrite the previous contents
`SNumber=0`	Use dataset 0
`/   /SubDirs`	Backup from/with all subdirectories
`/tmp /Xclude`	Exclude the directory

Typically, you would not wish to backup temporary files. These can be excluded by adding the line: `/tmp /Xclude` below the `/ /Subdirs`.

If you wanted to backup a single sub-directory, you should add the following below the `/ /Subdirs`:

```
/opt /Xclude
/opt/tivoli
```

and this would just backup the `/tivoli` subdirectory and no others within `/opt`.

7.4 Housekeeping

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

This is not always possible, so **Cristie Software Ltd.** recommend that the DR Backup be performed regularly. However, you should choose a period which reflects the rate of change 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. This can be achieved by creating a cron job for your schedule, including `cbmrcfg` in your backup script.

8 Performing a Recovery

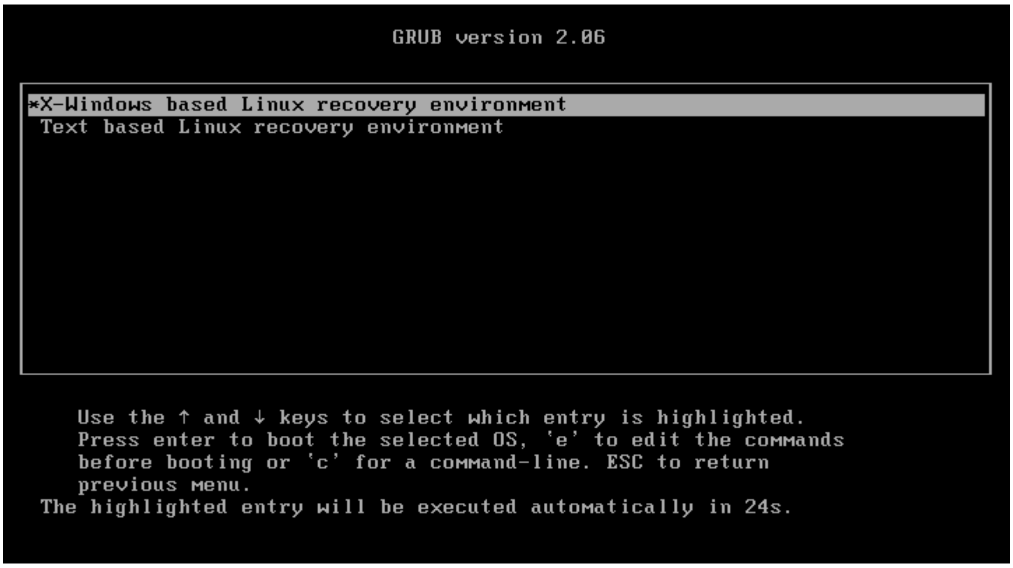
When a machine has failed, it can be recovered using the XBMR bootable product CD/ DVD-ROM or DR ISO (if your host supports this capability). XBMR is a separate product to CBMR. It is a generic Recovery Environment for all Cristie Linux BMR products.

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

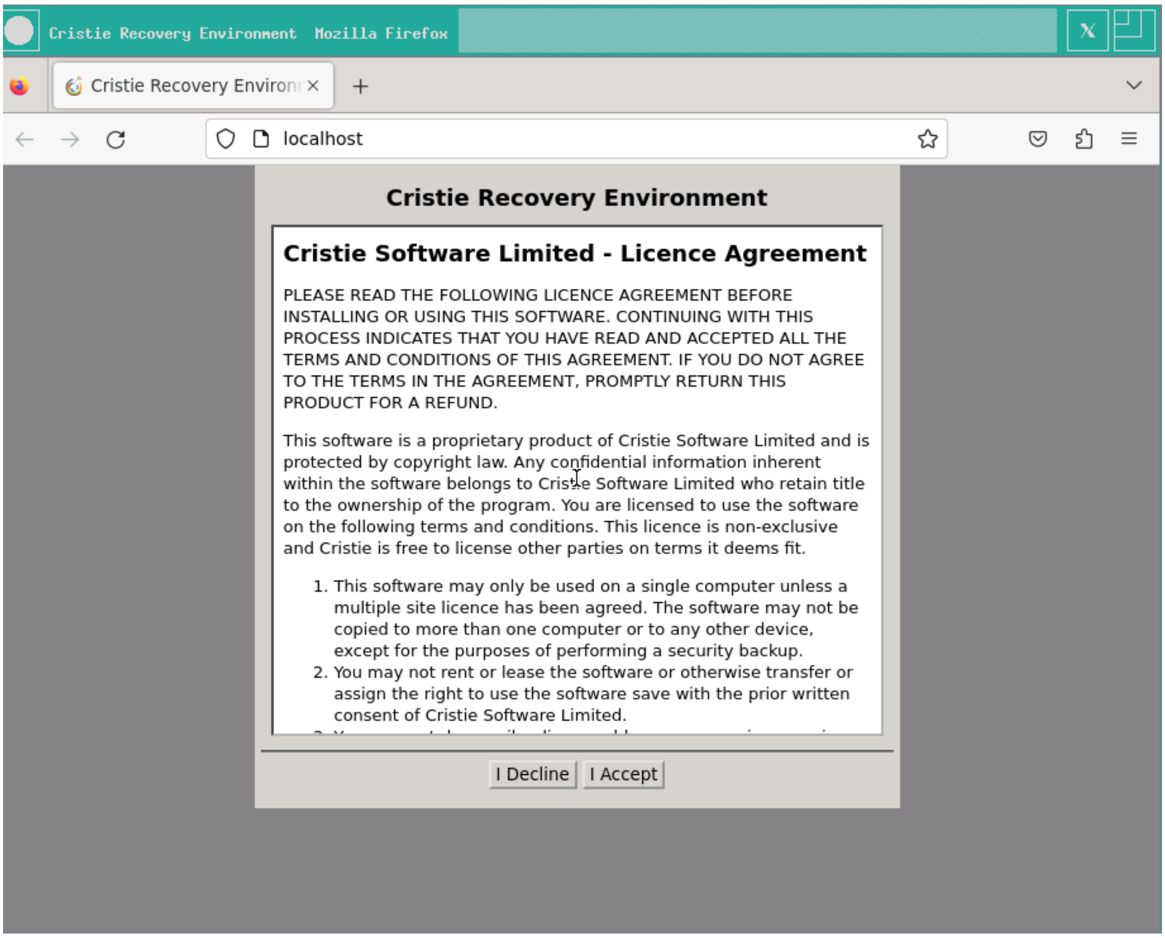
Boot the machine using the XBMR bootable CD/DVD ROM or ISO. You will be presented with the screen below:



```
                    GRUB version 2.06

*X-Windows based Linux recovery environment
 Text based Linux recovery environment

     Use the ↑ and ↓ keys to select which entry is highlighted.
     Press enter to boot the selected OS, 'e' to edit the commands
     before booting or 'c' for a command-line. ESC to return
     previous menu.
 The highlighted entry will be executed automatically in 24s.
```

Cristie recommend 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 XBMR licencing terms.



Cristie Recovery Environment

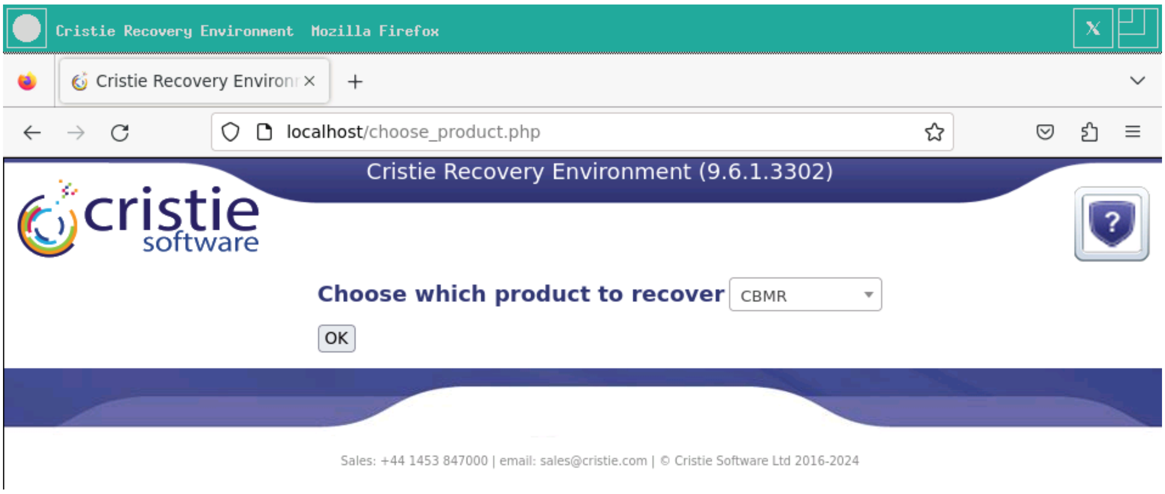
Cristie Software Limited - Licence Agreement

PLEASE READ THE FOLLOWING LICENCE AGREEMENT BEFORE INSTALLING OR USING THIS SOFTWARE. CONTINUING WITH THIS PROCESS INDICATES THAT YOU HAVE READ AND ACCEPTED ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS IN THE AGREEMENT, PROMPTLY RETURN THIS PRODUCT FOR A REFUND.

This software is a proprietary product of Cristie Software Limited and is protected by copyright law. Any confidential information inherent within the software belongs to Cristie Software Limited who retain title to the ownership of the program. You are licensed to use the software on the following terms and conditions. This licence is non-exclusive and Cristie is free to license other parties on terms it deems fit.

1. This software may only be used on a single computer unless a multiple site licence has been agreed. The software may not be copied to more than one computer or to any other device, except for the purposes of performing a security backup.
2. You may not rent or lease the software or otherwise transfer or assign the right to use the software save with the prior written consent of Cristie Software Limited.

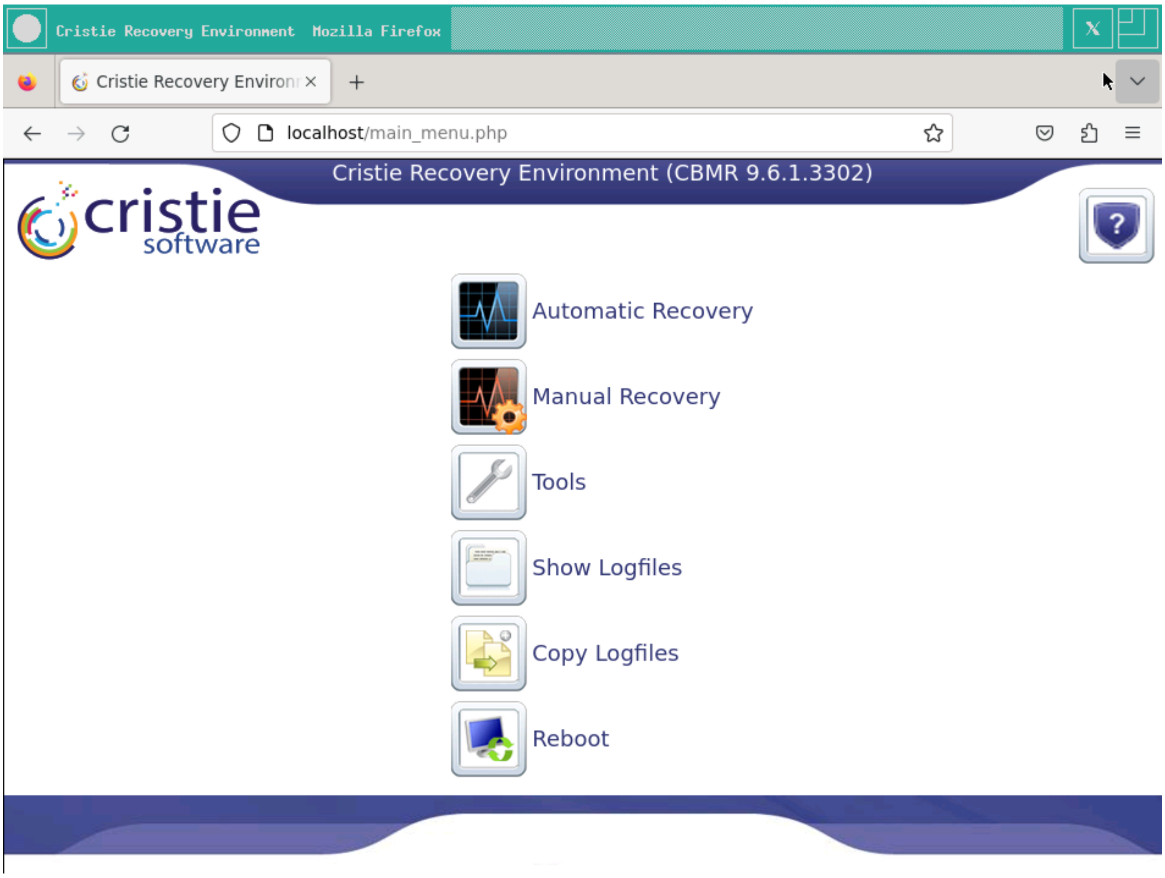
The Product Selection drop-down menu will then be shown. Now select the Cristie product used during the backup - CBMR in this case.


Cristie Recovery Environment Mozilla Firefox
Cristie Recovery Environ
localhost/choose_product.php
Cristie Recovery Environment (9.6.1.3302)
cristie software
OK

Choose which product to recover CBMR

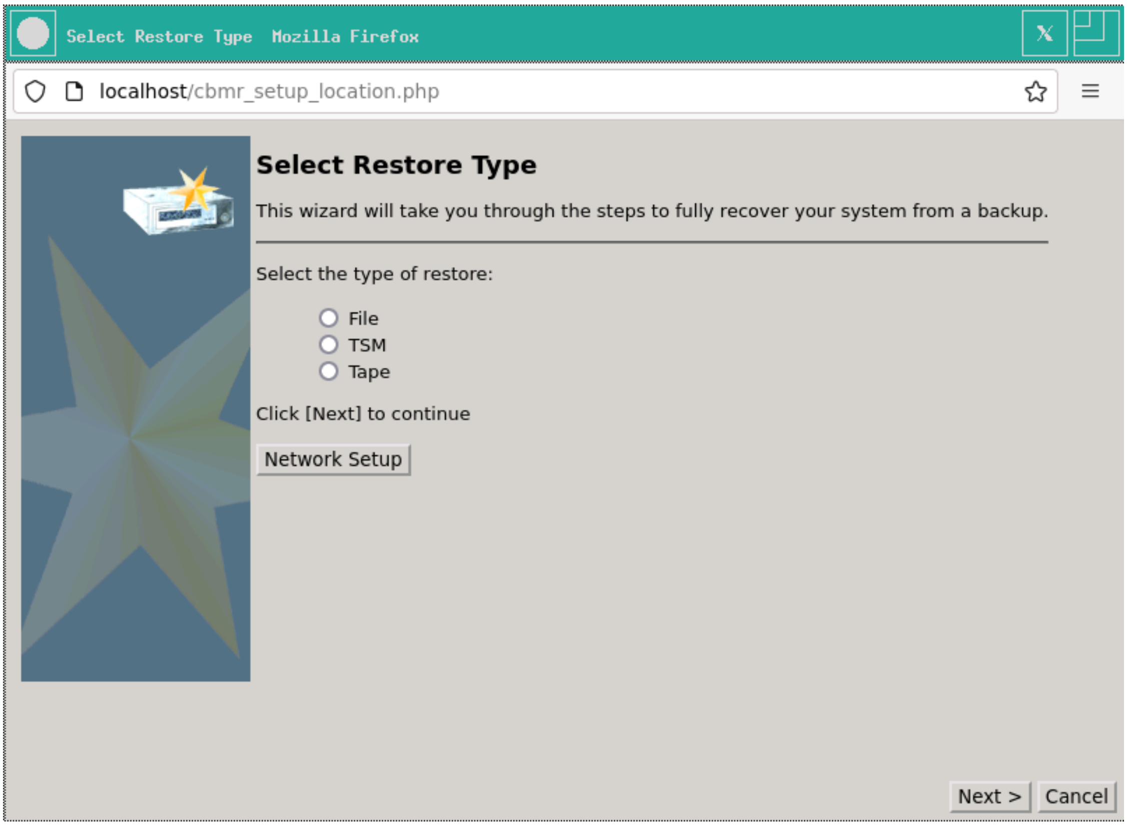
Sales: +44 1453 847000 | email: sales@cristie.com | © Cristie Software Ltd 2016-2024

You will then see the **Recovery Environment** main menu:



Cristie recommends using the **Automatic Recovery Wizard** option from the **Recovery Environment** main menu.

The **Select Restore Type** dialogue box will be shown first. At this point, you must indicate to XBMR where your backup file(s) are located. The examples illustrated are those most commonly used - **File Location** and **TSM Location**



Select Restore Type Mozilla Firefox
localhost/cbmr_setup_location.php
Network Setup
Next >
Cancel

Select Restore Type

This wizard will take you through the steps to fully recover your system from a backup.

Select the type of restore:

○ File
○ TSM
○ Tape

Click [Next] to continue

File Location - choose a file location for your backup.

TSM Location - choose an IBM Spectrum Protect (TSM) location by entering the server and client information.

Tape Location - allows you to scan for SCSI or IDE tape devices.

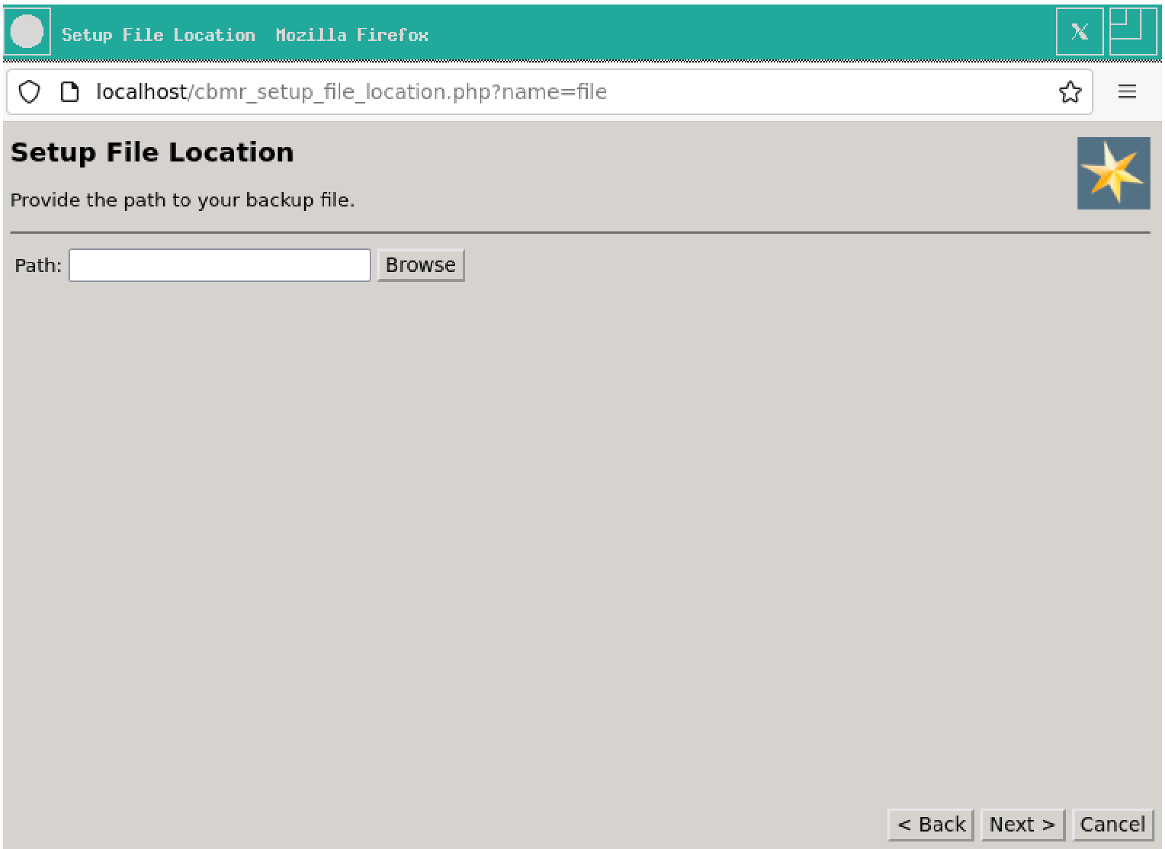
Network Setup - defaults to DHCP but can be customised to use a static IP address if required.

8.1 Backup located in a 'File Location'

> *Note: it is not currently possible to restore incremental backups using the GUI. To restore incremental backups follow the Incremental File Backups section to restore using the command line.*

8.1.1 VTD File Backups

From the **Select Restore Type** dialogue, select **File** and then click the Next > button to proceed. You will then be prompted to provide the network path to the location of your backup VTD file:


Setup File Location Mozilla Firefox
localhost/cbmr_setup_file_location.php?name=file

Setup File Location

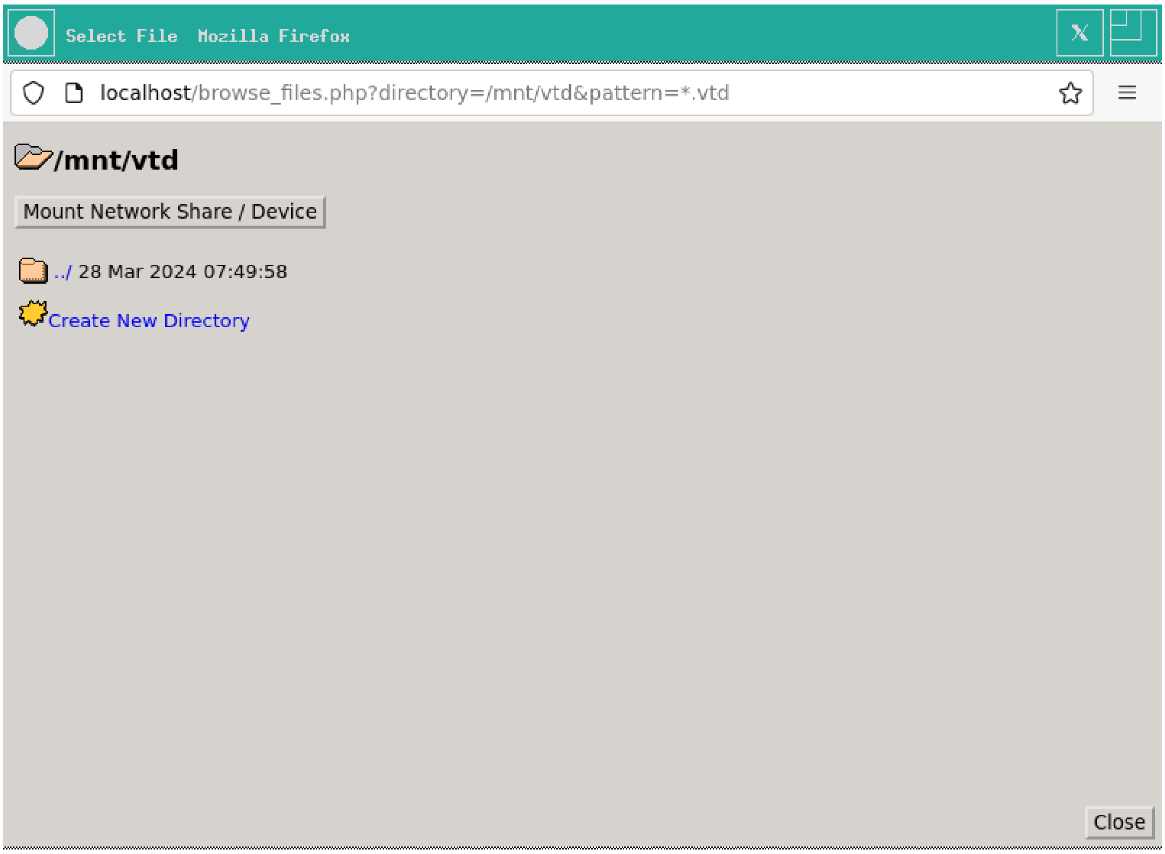
Provide the path to your backup file.

Path:

Browse
< Back
Next >
Cancel

If required, you can locate where your backup file(s) are stored by clicking the Browse button; it is also possible to mount any required network shares.

To mount a new network share, select **Mount Network Share**:



Select File Mozilla Firefox
localhost/browse_files.php?directory=/mnt/vtd&pattern=*.vtd

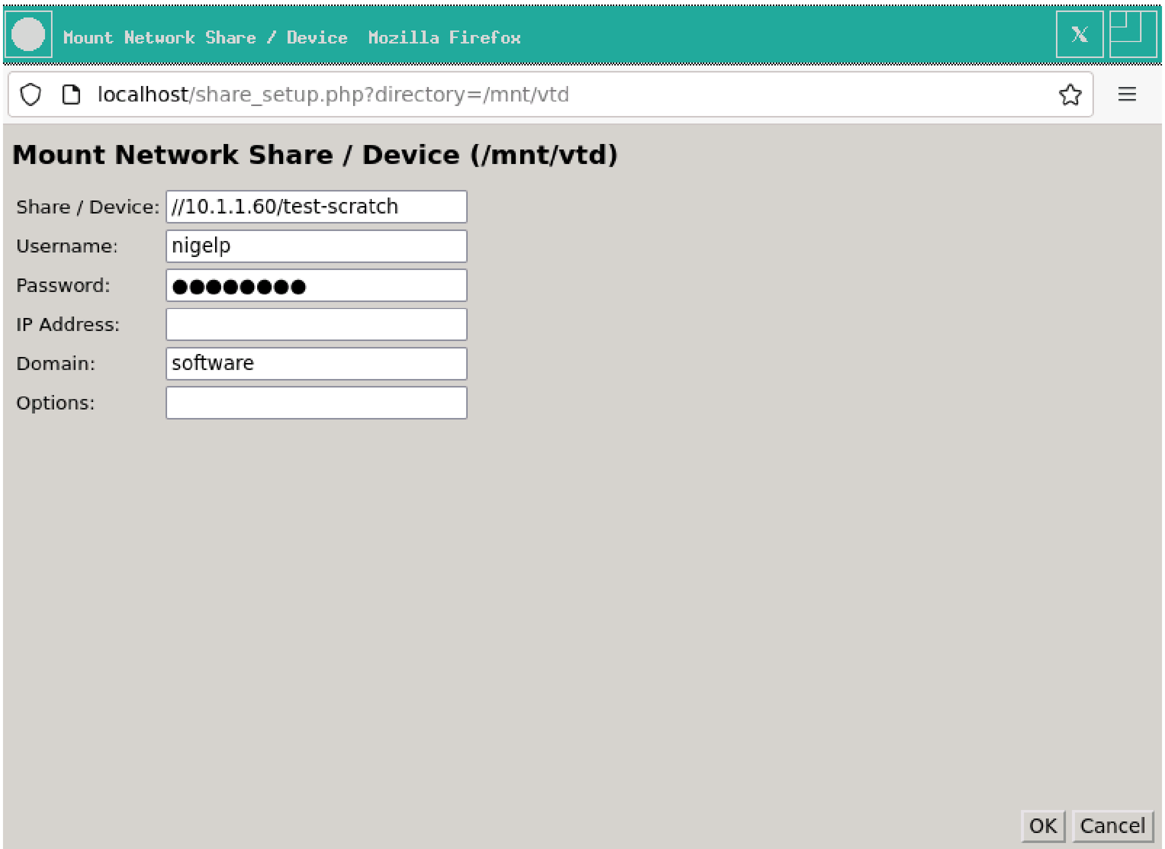
/mnt/vtd

Mount Network Share / Device

../ 28 Mar 2024 07:49:58

Create New Directory
Close

Complete the form with the required details. Click OK to proceed.



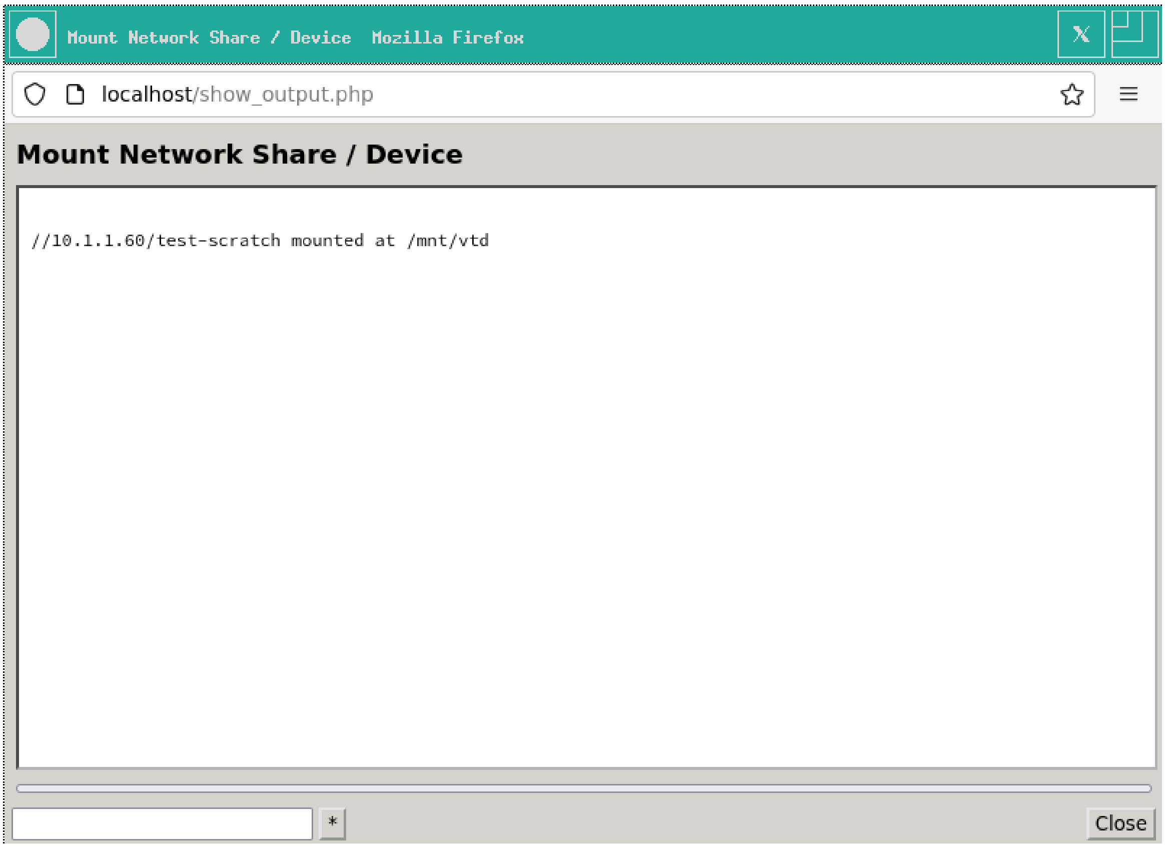
Mount Network Share / Device Mozilla Firefox
localhost/share_setup.php?directory=/mnt/vtd

Mount Network Share / Device (/mnt/vtd)

Share / Device:	//10.1.1.60/test-scratch
Username:	nigelp
Password:	●●●●●●●●
IP Address:	
Domain:	software
Options:	

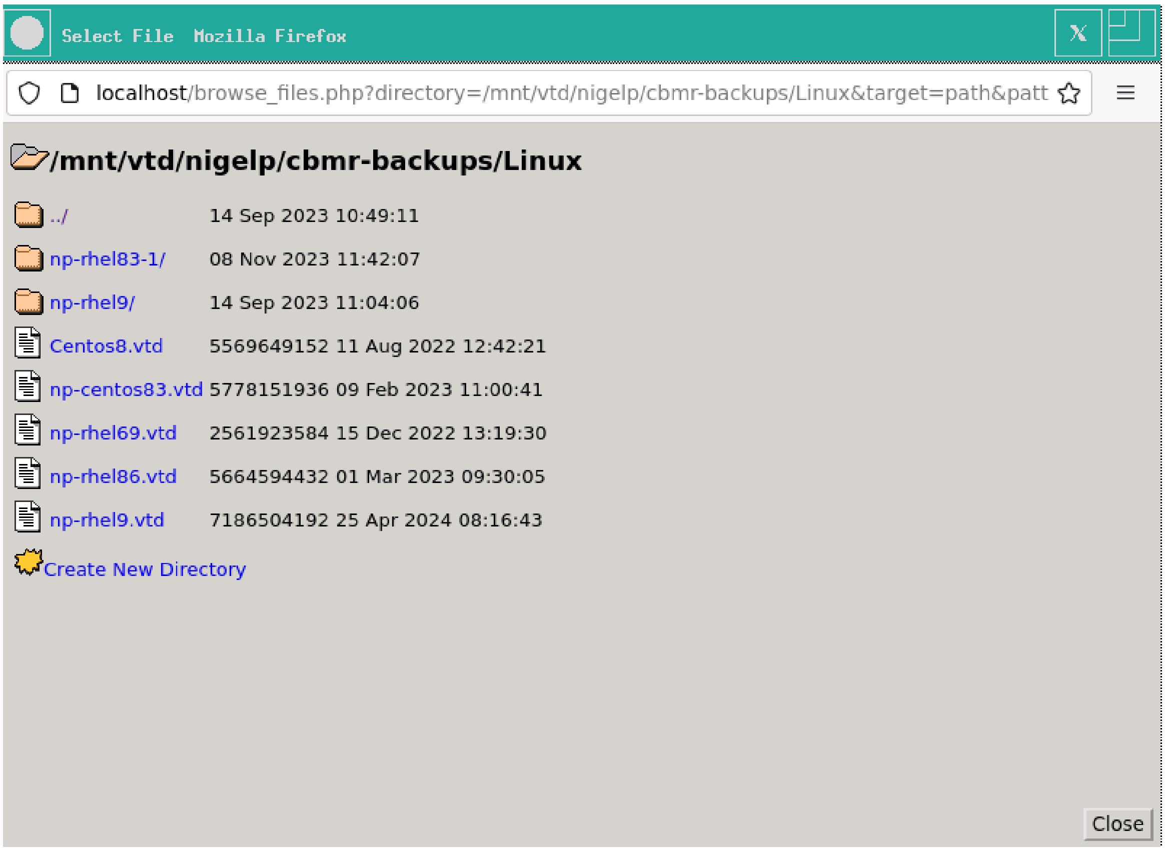
Note: the "Share / Device" field can be populated with the share location e.g. <IP>:</path/to/mount> or an attached device e.g. a usb device at /dev/sdx

A summary message will then be displayed informing if the network share was mounted successfully.


Mount Network Share / Device Mozilla Firefox
localhost/show_output.php
Mount Network Share / Device
*
Close

```
//10.1.1.60/test-scratch mounted at /mnt/vtd
```

Select Close to continue. The mounted network share details are then displayed: Navigate to the location of your backup and click the required vtd file.

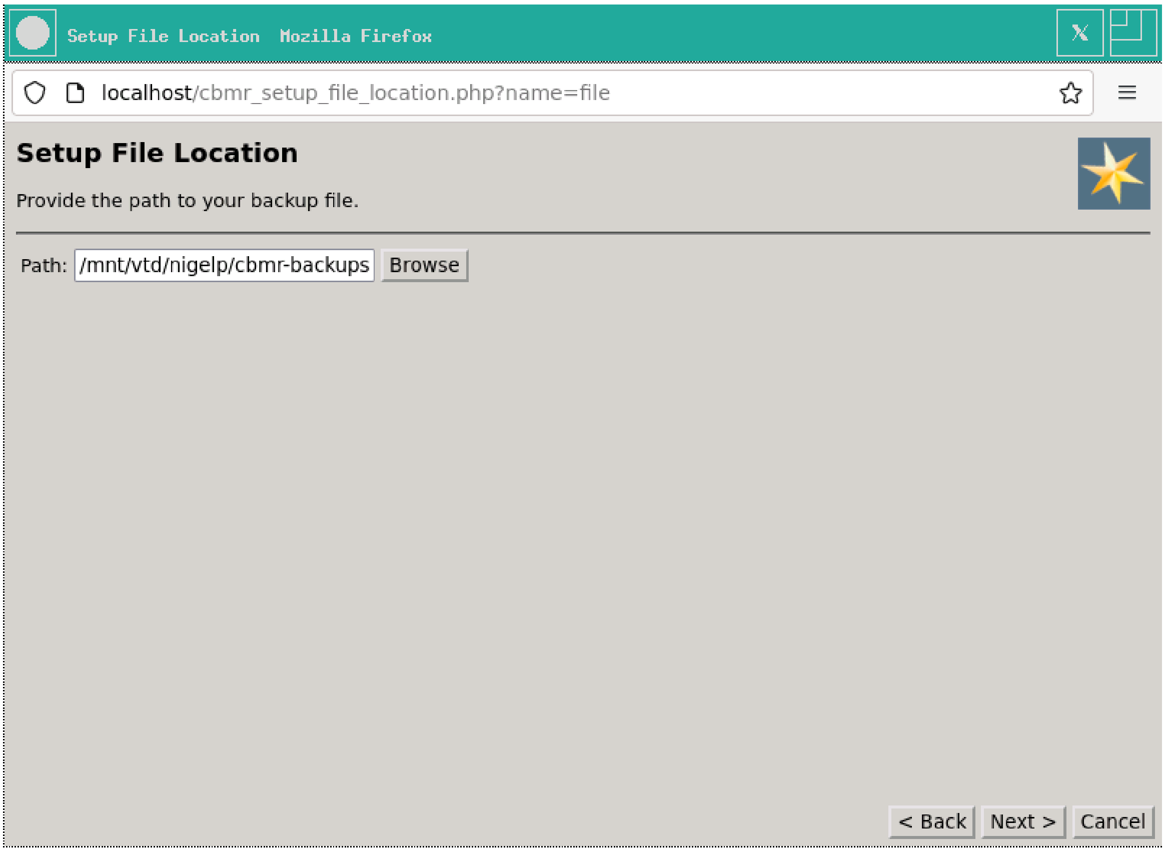

Select File Mozilla Firefox
localhost/browse_files.php?directory=/mnt/vtd/nigelp/cbmr-backups/Linux&target=path&patt
Close

/mnt/vtd/nigelp/cbmr-backups/Linux

../	14 Sep 2023 10:49:11
np-rhel83-1/	08 Nov 2023 11:42:07
np-rhel9/	14 Sep 2023 11:04:06
Centos8.vtd	5569649152 11 Aug 2022 12:42:21
np-centos83.vtd	5778151936 09 Feb 2023 11:00:41
np-rhel69.vtd	2561923584 15 Dec 2022 13:19:30
np-rhel86.vtd	5664594432 01 Mar 2023 09:30:05
np-rhel9.vtd	7186504192 25 Apr 2024 08:16:43

Create New Directory

You will then be presented with the **Setup File Location** dialogue box again.

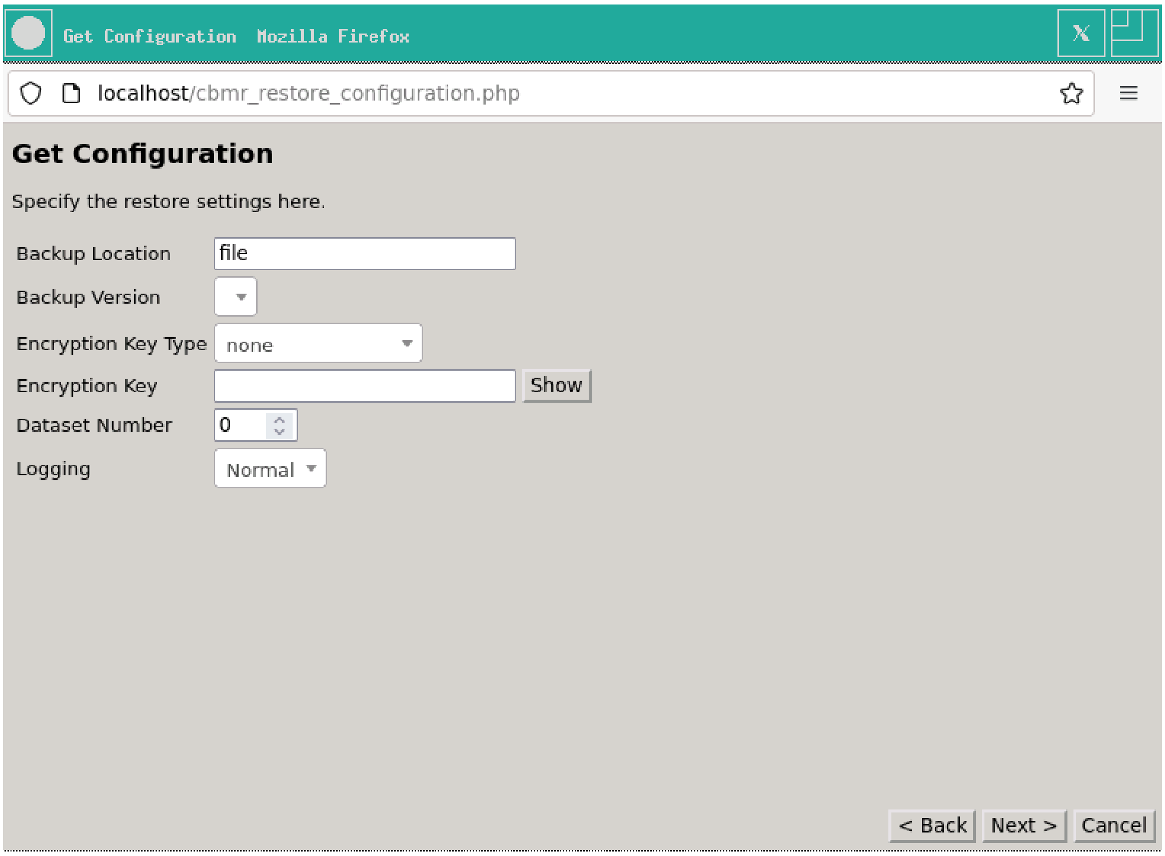

Setup File Location Mozilla Firefox
localhost/cbmr_setup_file_location.php?name=file
Browse
< Back
Next >
Cancel

Setup File Location

Provide the path to your backup file.

Path: /mnt/vtd/nigelp/cbmr-backups

Select Next > to proceed. You will then be presented with the **Get Configuration** dialogue box:


Get Configuration Mozilla Firefox
localhost/cbmr_restore_configuration.php

Get Configuration

Specify the restore settings here.

Backup Location	file
Backup Version	
Encryption Key Type	none
Encryption Key	
Dataset Number	0
Logging	Normal

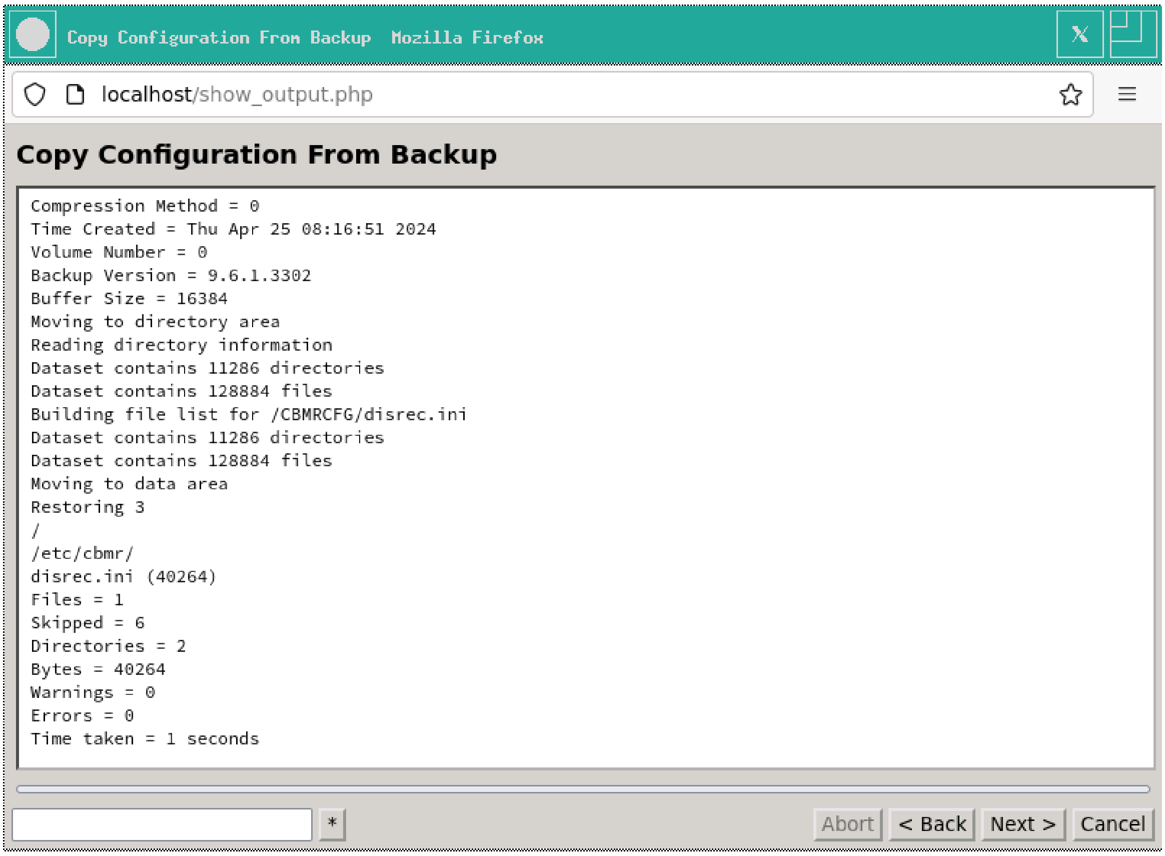
Show
< Back
Next >
Cancel

If the backup is encrypted, you should select the **Encryption Key Type** drop-down menu, select the correct encryption, then enter the correct Encryption Key.

> ***Note: under normal circumstances you should leave 'Dataset Number' as 0.***

Click Next to continue.

You will then be presented with a screen which summarises the copying of the Configuration from the backup file you just selected:


Copy Configuration From Backup Mozilla Firefox
localhost/show_output.php

Copy Configuration From Backup

```
Compression Method = 0
Time Created = Thu Apr 25 08:16:51 2024
Volume Number = 0
Backup Version = 9.6.1.3302
Buffer Size = 16384
Moving to directory area
Reading directory information
Dataset contains 11286 directories
Dataset contains 128884 files
Building file list for /CBMRCFG/disrec.ini
Dataset contains 11286 directories
Dataset contains 128884 files
Moving to data area
Restoring 3
/
/etc/cbmr/
disrec.ini (40264)
Files = 1
Skipped = 6
Directories = 2
Bytes = 40264
Warnings = 0
Errors = 0
Time taken = 1 seconds
```

Click Next to continue.

Further details on the Recovery process are described in the section **Continuing the Recovery**.

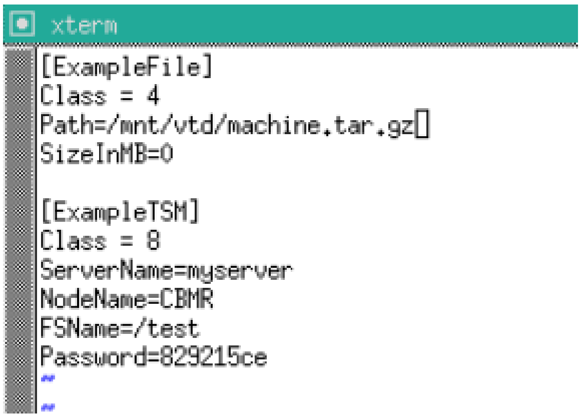
8.1.2 Incremental File Backups

Incremental Backups cannot currently be recovered using the Automatic or Manual Recovery methods. To perform an Incremental restore you must use the command line within the recovery environment.

To open a shell prompt go to Tools on the main menu and then click **Run Shell** and then Start. Alternatively, you can press the shortcut keys `CTRL + ALT + F2`.

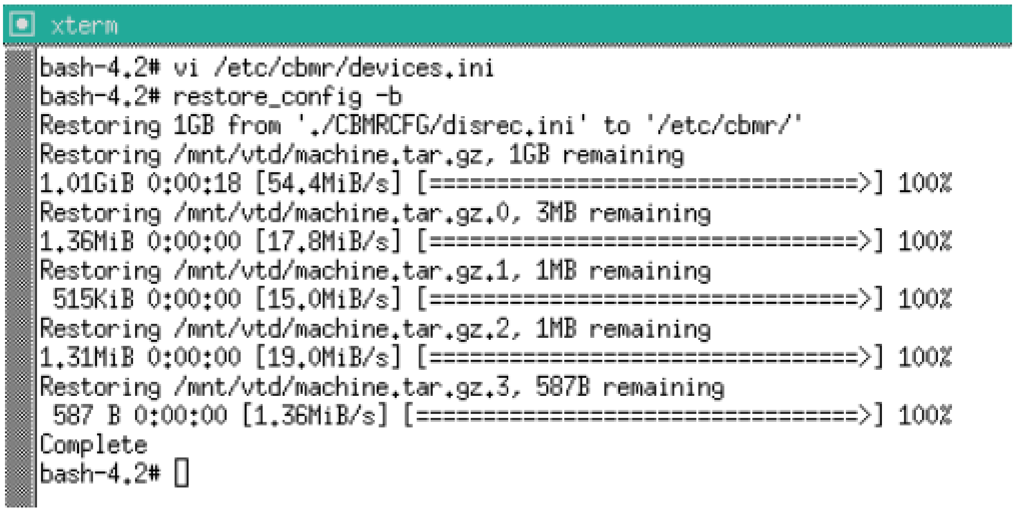
Firstly, mount the network share where the incremental files are stored using `mount` or `mount.cifs` to the mount point `/mnt/vtd`, e.g. `mount 10.1.1.50:/backups/rhel7incrementals /mnt/vtd`

Once the share is mounted you will then need to edit the file `/etc/cbmr/devices.ini`. Change the Path under [ExampleFile] to point to the `machine.tar.gz` file located on your share as shown in the following example.



```
[ExampleFile]
Class = 4
Path=/mnt/vtd/machine.tar.gz
SizeInMB=0

[ExampleTSM]
Class = 8
ServerName=myserver
NodeName=CBMR
FSName=/test
Password=829215ce
~
~
```

Save the changes. You can now restore the backup configuration file using the command `restore_config -b`, the latest configuration file will be retrieved.



```
bash-4.2# vi /etc/cbmr/devices.ini
bash-4.2# restore_config -b
Restoring 1GB from './CBMRCFG/disrec.ini' to '/etc/cbmr/'
Restoring /mnt/vtd/machine.tar.gz, 1GB remaining
1.01GiB 0:00:18 [54.4MiB/s] [================================>] 100%
Restoring /mnt/vtd/machine.tar.gz.0, 3MB remaining
1.36MiB 0:00:00 [17.8MiB/s] [================================>] 100%
Restoring /mnt/vtd/machine.tar.gz.1, 1MB remaining
 515KiB 0:00:00 [15.0MiB/s] [================================>] 100%
Restoring /mnt/vtd/machine.tar.gz.2, 1MB remaining
1.31MiB 0:00:00 [19.0MiB/s] [================================>] 100%
Restoring /mnt/vtd/machine.tar.gz.3, 587B remaining
 587 B 0:00:00 [1.36MiB/s] [=================================>] 100%
Complete
bash-4.2# 
```

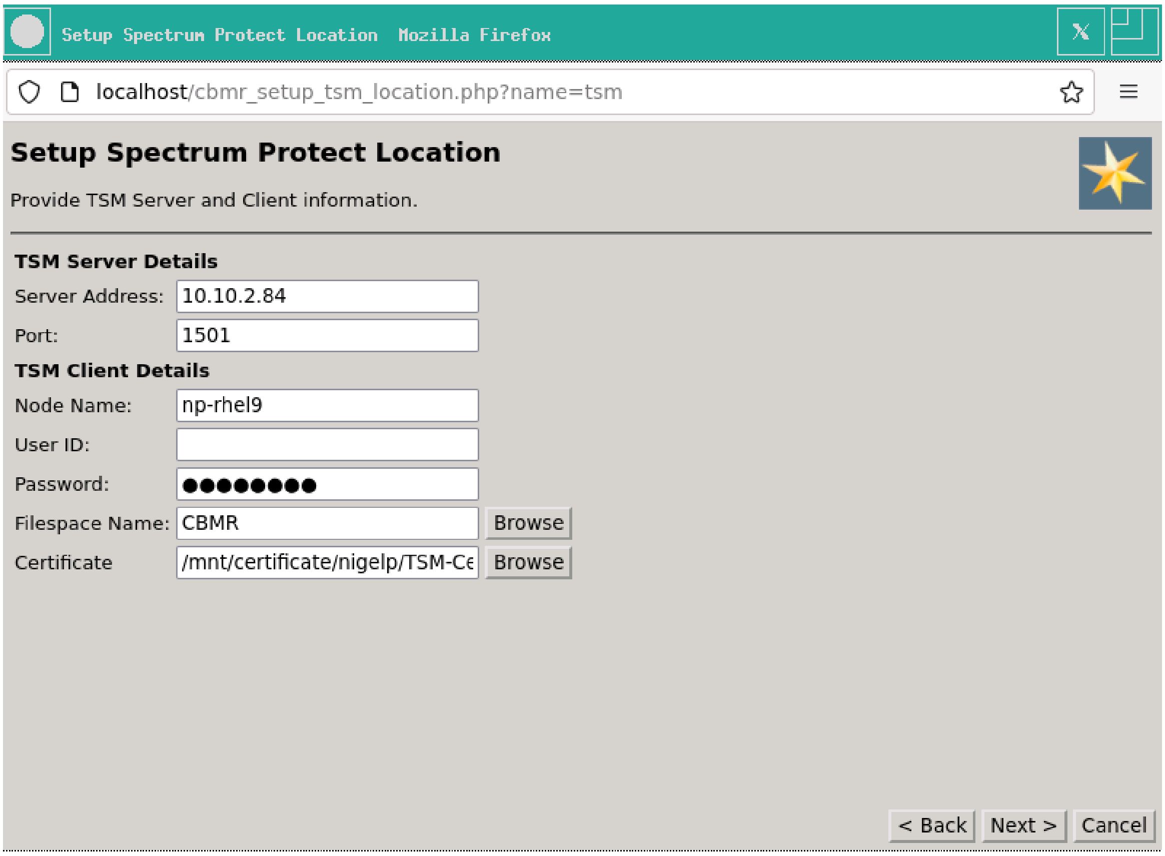
If you wish to change the disk configuration before the restore you can return to the main menu by closing the Shell window or using `CTRL + ALT + F1`, then click **Manual Recovery** and then click either **Recovery Options** or **Multipath Options** (only applicable for multipath systems) - you will not be able to restore the incremental data through the Manual Recovery menu, this must be done using the command stated below. Save the Recovery Options and return the Shell.

To begin the recovery use the following command: `disrec -pfdthbc`. The command will partition and format the disks, mount the filesystems, restore the incremental data and then make the system bootable.

Once finished you can return to the main menu to copy the log files or reboot.

8.2 Backup located in a IBM Spectrum Protect (TSM) Location

If you have chosen a IBM Spectrum Protect (TSM) location for your backup location, you be presented with the **Setup TSM Location** dialogue box.


Setup Spectrum Protect Location Mozilla Firefox
localhost/cbmr_setup_tsm_location.php?name=tsm
Browse
Browse
< Back
Next >
Cancel

Setup Spectrum Protect Location

Provide TSM Server and Client information.

TSM Server Details

Server Address: 10.10.2.84

Port: 1501

TSM Client Details

Node Name: np-rhel9

User ID:

Password: ●●●●●●●●●

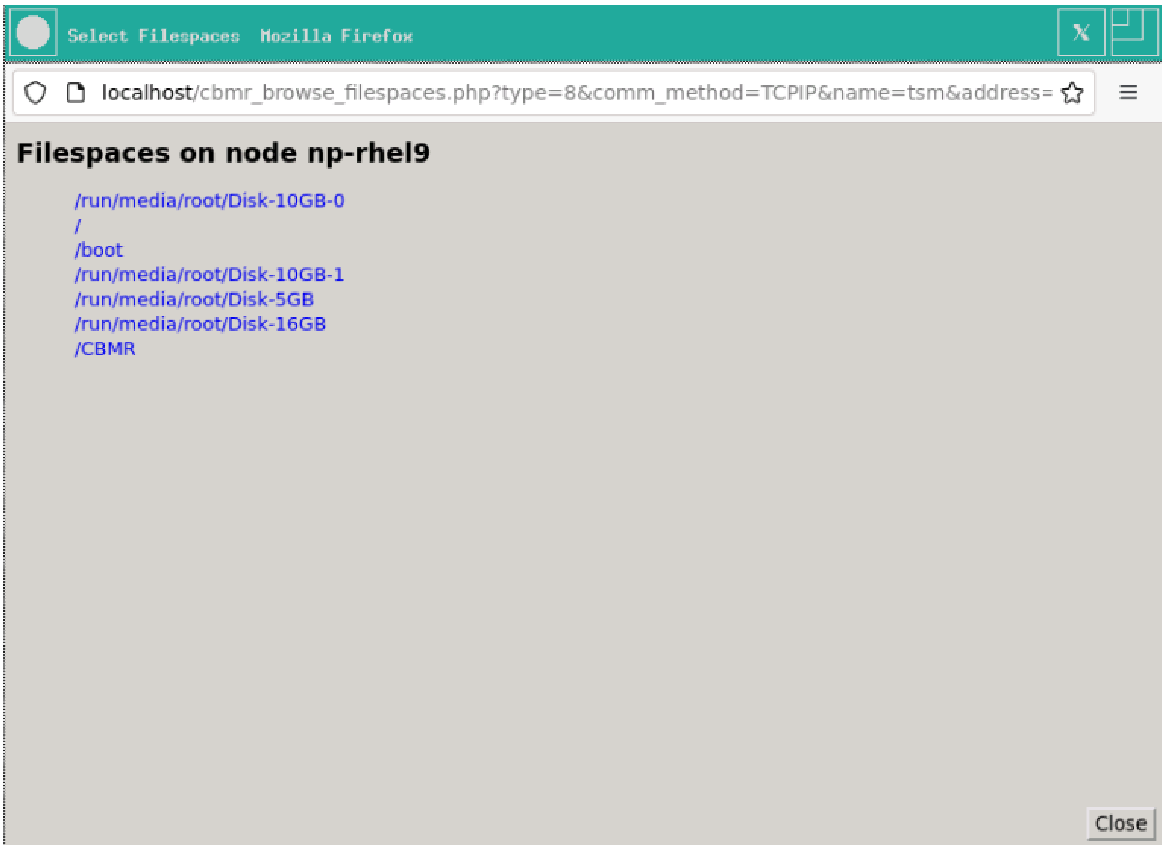
Filespace Name: CBMR

Certificate /mnt/certificate/nigelp/TSM-Ce

Fill in all your IBM Spectrum Protect (TSM) server and node information - you must complete every field in order to continue. Contact your IBM Spectrum Protect (TSM) administrator if you are unsure of any of the required information.

> *Note: IBM Spectrum Protect (TSM) server versions 8.1.2.0 or later are configured to use SSL encryption by default. To access such a server you will need to provide an SSL server certificate. Use the **Certificate** option to do this.*

You can enter the Filespace name if you wish, alternatively you can click the Browse button to display a list of available Filespaces. In this case though you need to set the **User ID** to a user that has the privilege to run `dsmadmc` on the server.



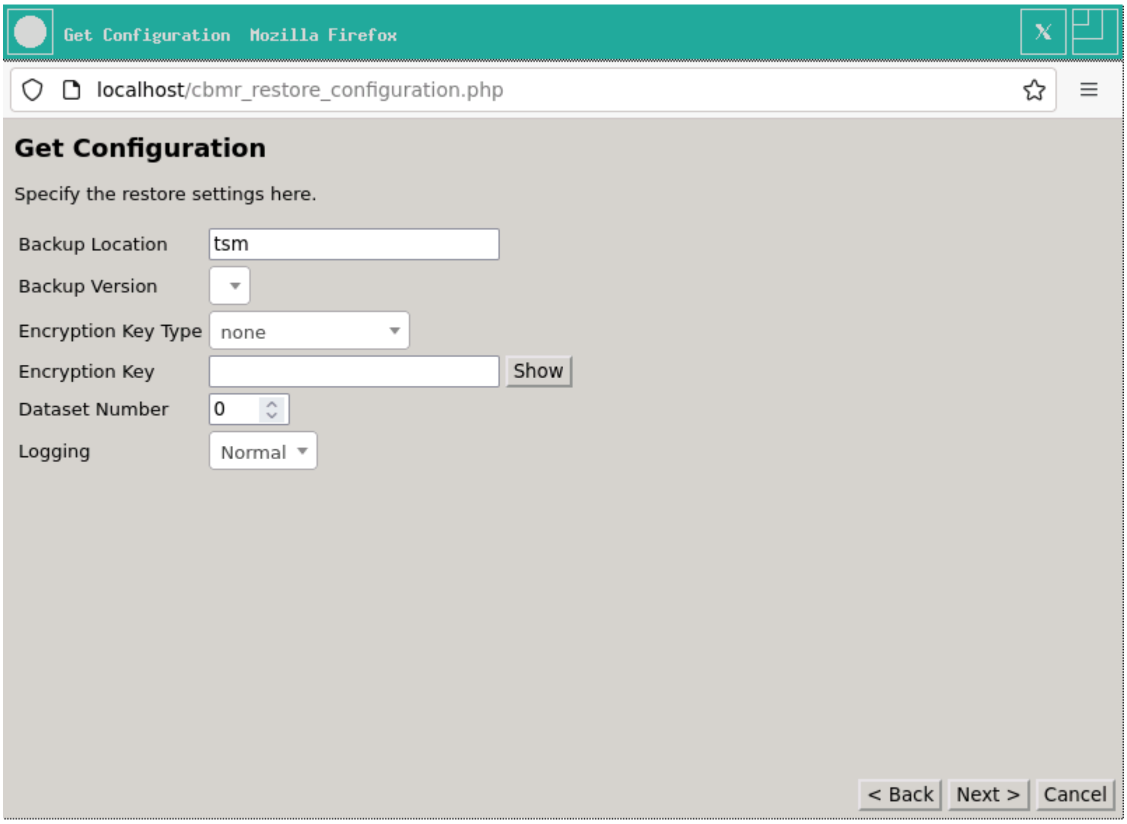
Select Filespaces Mozilla Firefox
localhost/cbmr_browse_filespaces.php?type=8&comm_method=TCPIP&name=tsm&address=

Filespaces on node np-rhel9

/run/media/root/Disk-10GB-0
/
/boot
/run/media/root/Disk-10GB-1
/run/media/root/Disk-5GB
/run/media/root/Disk-16GB
/CBMR

Click on the filespace that you wish to apply. Click Next to continue when you are happy the correct filespace name is specified.

You will then see the Get **Configuration** dialogue box.


Get Configuration Mozilla Firefox
localhost/cbmr_restore_configuration.php

Get Configuration

Specify the restore settings here.

Backup Location	tsm
Backup Version	
Encryption Key Type	none
Encryption Key	
Dataset Number	0
Logging	Normal

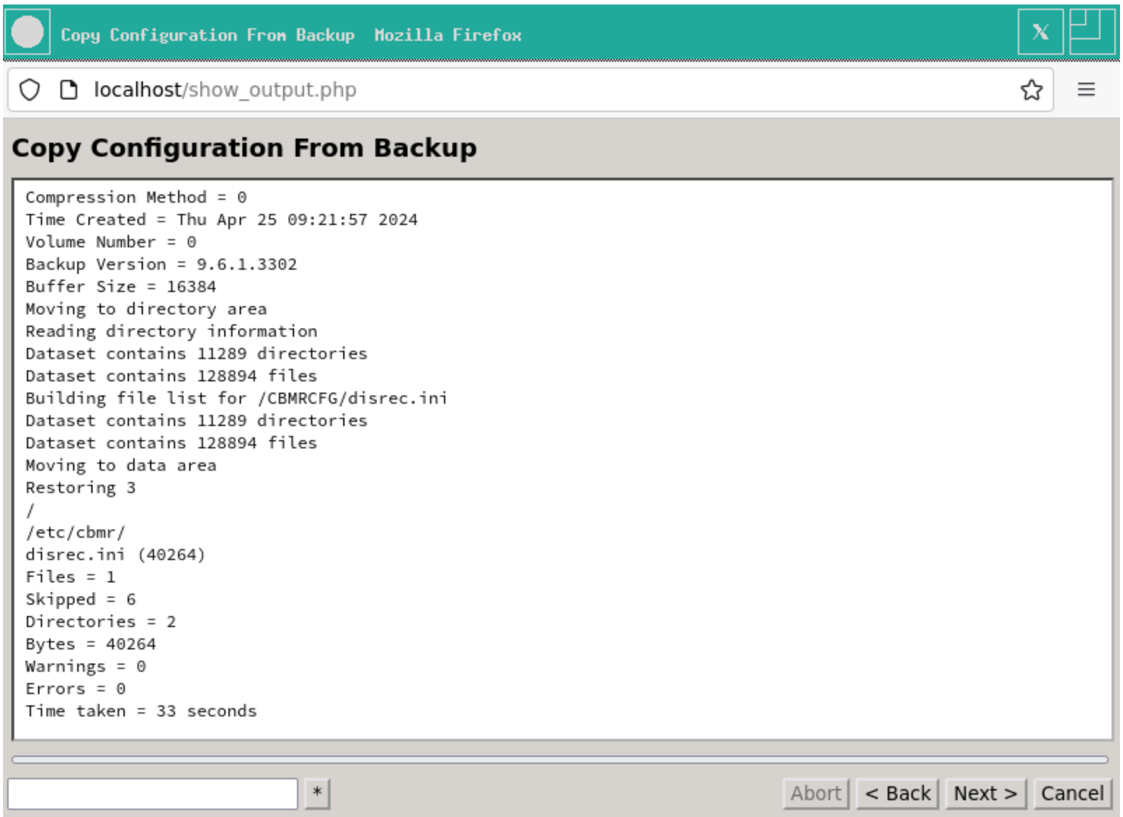
Show
< Back
Next >
Cancel

You can specify the version of the backup to be used (if you have multiple versions stored). Click the drop-down menu and select the one you want.

If the backup is encrypted, you should select the **Encryption Key Type** drop-down menu, select the correct encryption, then enter the correct Encryption Key.

Note: under normal circumstances you should leave the 'Dataset Number' as 0

Click Next to continue. You will then be presented with a screen which summarises the copying of the Configuration from the backup file you just selected.


Copy Configuration From Backup Mozilla Firefox
localhost/show_output.php
Copy Configuration From Backup
*
Abort
< Back
Next >
Cancel

```
Compression Method = 0
Time Created = Thu Apr 25 09:21:57 2024
Volume Number = 0
Backup Version = 9.6.1.3302
Buffer Size = 16384
Moving to directory area
Reading directory information
Dataset contains 11289 directories
Dataset contains 128894 files
Building file list for /CBMRCFG/disrec.ini
Dataset contains 11289 directories
Dataset contains 128894 files
Moving to data area
Restoring 3
/
/etc/cbmr/
disrec.ini (40264)
Files = 1
Skipped = 6
Directories = 2
Bytes = 40264
Warnings = 0
Errors = 0
Time taken = 33 seconds
```

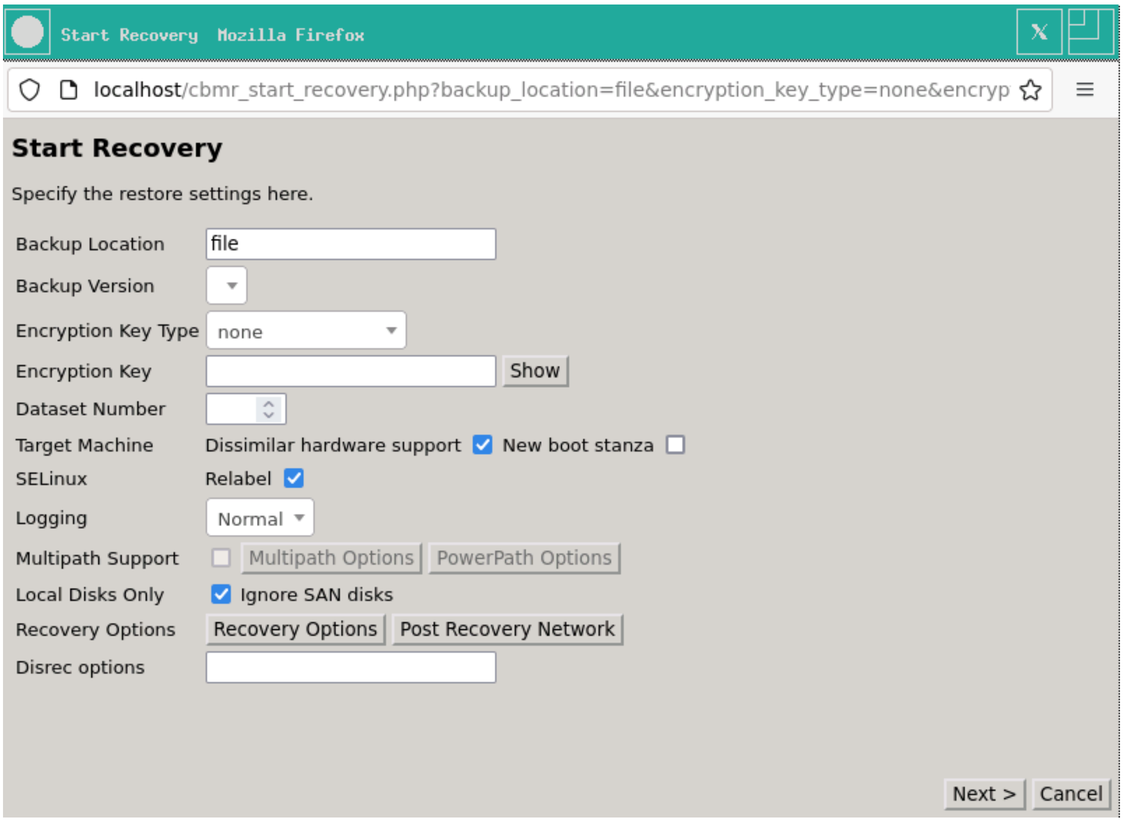
Click Next to continue.

Further details on the Recovery process are included in **Continuing the Recovery**.

8.3 Continuing the Recovery

The **Start Recovery** screen contains the previously specified information:

- **Backup Location**
- **Backup Version** (if previous versions exist)
- **Encryption options**
- **Dissimilar Hardware support**
- **Recovery Options**



Start Recovery Mozilla Firefox

localhost/cbmr_start_recovery.php?backup_location=file&encryption_key_type=none&encryp

Start Recovery

Specify the restore settings here.

Backup Location: file

Backup Version:

Encryption Key Type: none

Encryption Key:

Dataset Number:

Target Machine: Dissimilar hardware support ☑ New boot stanza □

SELinux: Relabel ☑

Logging: Normal

Multipath Support: □

Local Disks Only: ☑ Ignore SAN disks

Recovery Options:

Disrec options:

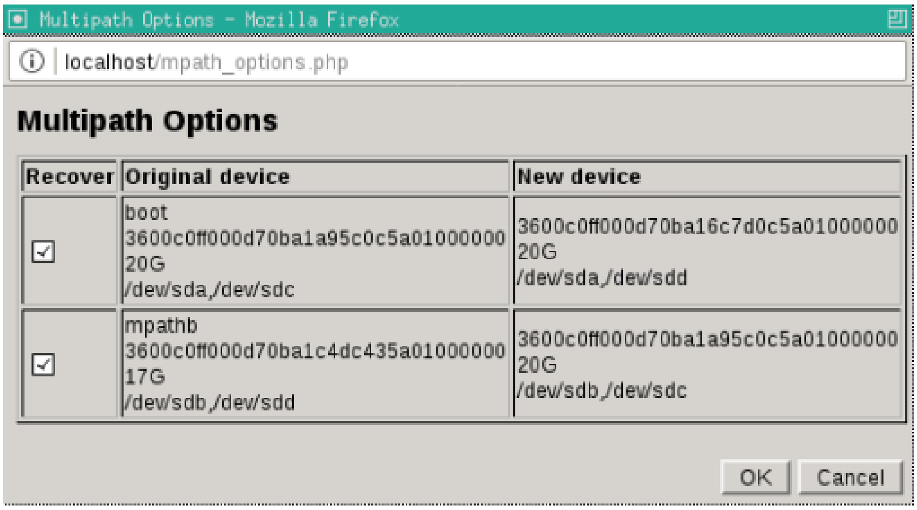
You should select the relevant **encryption options** from the drop-down menu if you chose to encrypt your backup earlier.

> *Note: if you are recovering to dissimilar hardware, CBMR will find the required module (s) automatically. Normally this will happen with no further user intervention. If CBMR cannot find the required module, you will be prompted at the end of the recovery to provide a location that contains the required module(s).*

SELinux Relabel is required to ensure successful recovery of your system. **Do not** untick this box unless instructed to do so by Cristie support or if you are sure that the system does not need to be relabeled.

New boot stanza means a new initial ramdisk is created rather than overwriting the existing one and also create **Cristie Recovered System** as a new boot menu item.

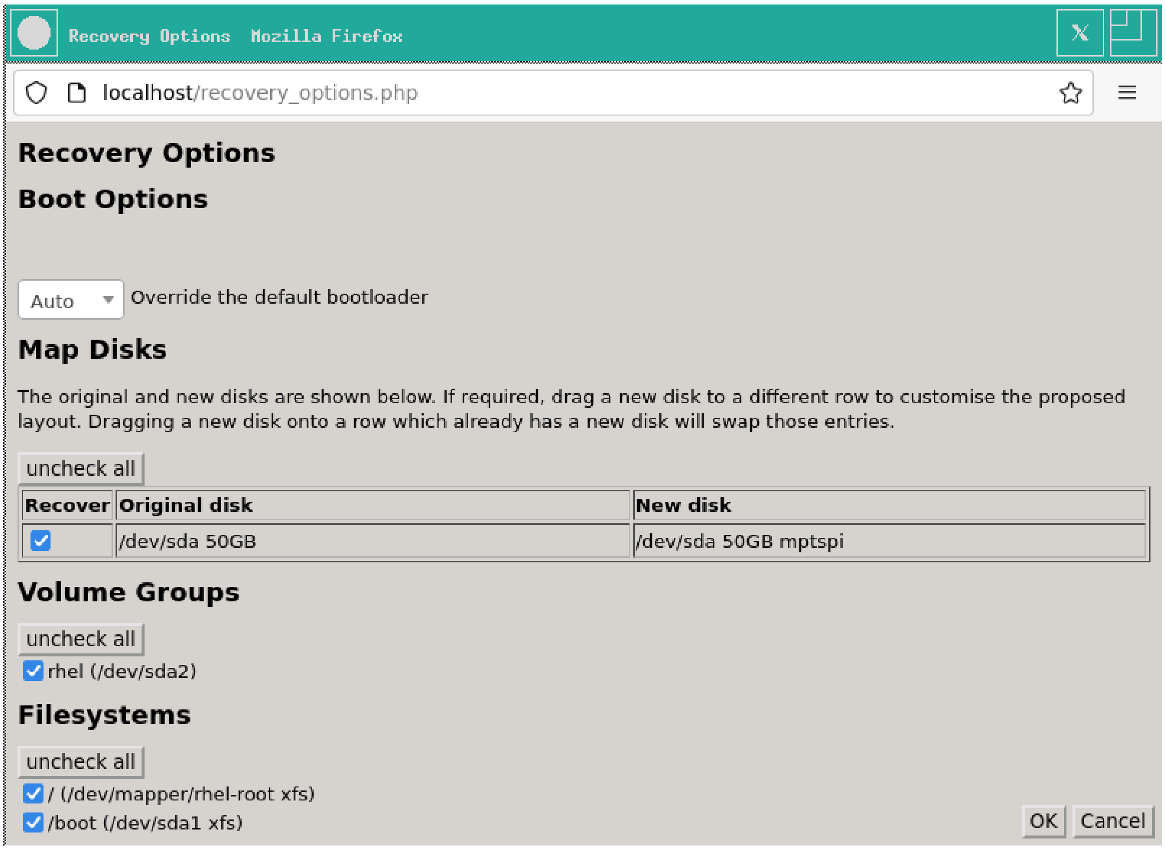
If you are recovering Multipath or PowerPath disks, you must **check** the tick-box for **Multipath/PowerPath Support**. Not doing so will cause the disks to be treated as non-Multipath/PowerPath disks. You can then select and customise your Multipath/PowerPath disk layout by clicking on the Multipath Options or PowerPath Options buttons as appropriate. Note the tick-box and buttons will only become active if such disks are actually present and recorded in the DR configuration.


Multipath Options - Mozilla Firefox
localhost/mpath_options.php

Multipath Options

Recover	Original device	New device
☑	boot 3600c0ff000d70ba1a95c0c5a01000000 20G /dev/sda,/dev/sdc	3600c0ff000d70ba16c7d0c5a01000000 20G /dev/sda,/dev/sdd
☑	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.

Recover	Original disk	New disk
☑	/dev/sda 50GB	/dev/sda 50GB mptspi

Volume Groups

☑ rhel (/dev/sda2)

Filesystems

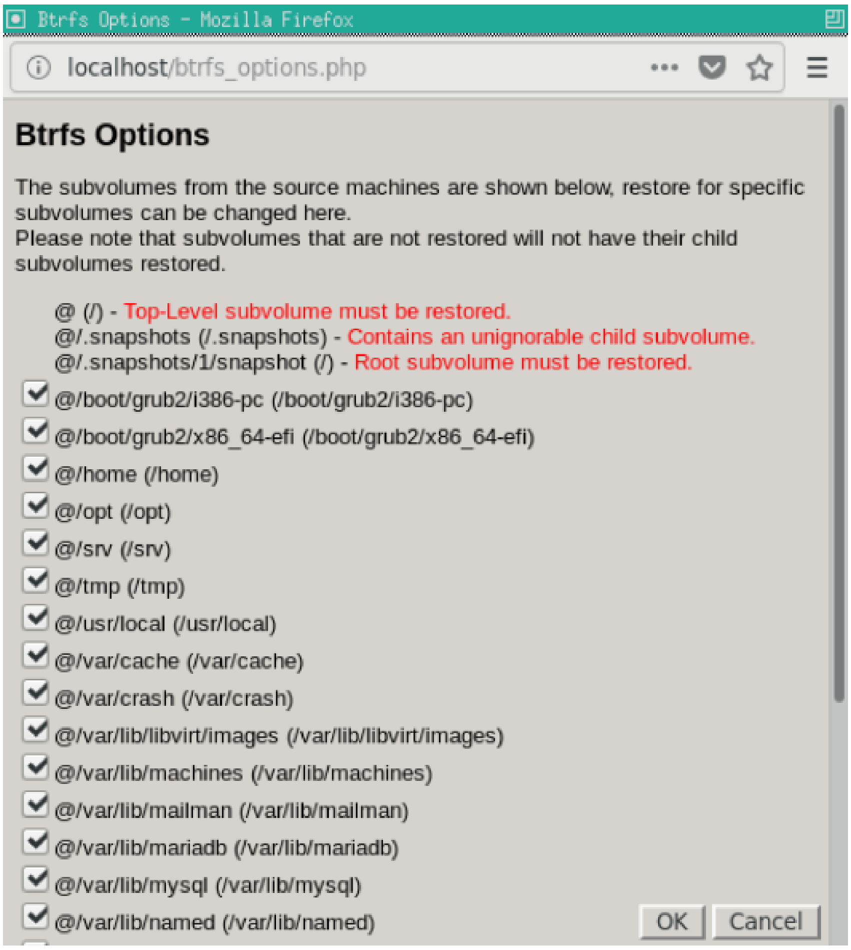
☑ / (/dev/mapper/rhel-root xfs)

☑ /boot (/dev/sda1 xfs)

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

Note 2: 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.



Btrfs Options

The subvolumes from the source machines are shown below, restore for specific subvolumes can be changed here.
Please note that subvolumes that are not restored will not have their child subvolumes restored.

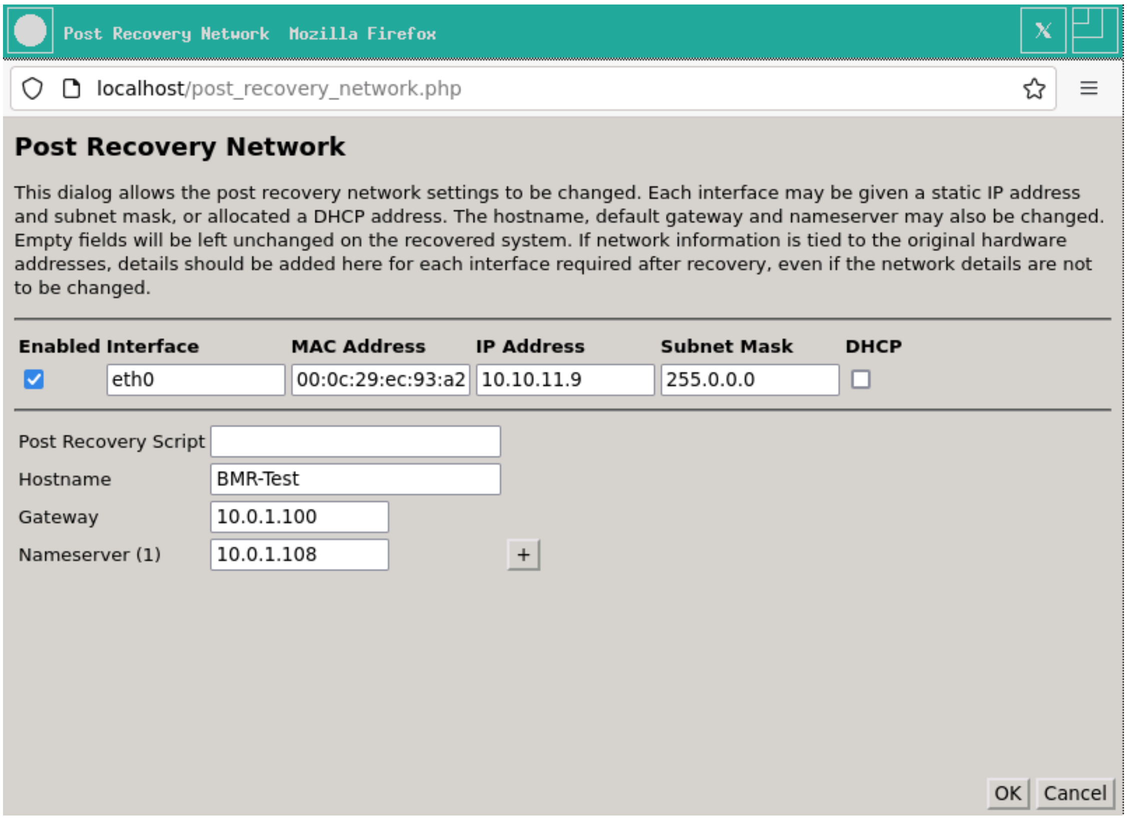
@ (/) - Top-Level subvolume must be restored.
@/.snapshots (/.snapshots) - Contains an unignorable child subvolume.
@/.snapshots/1/snapshot (/) - Root subvolume must be restored.

- ☑ @/boot/grub2/i386-pc (/boot/grub2/i386-pc)
- ☑ @/boot/grub2/x86_64-efi (/boot/grub2/x86_64-efi)
- ☑ @/home (/home)
- ☑ @/opt (/opt)
- ☑ @/srv (/srv)
- ☑ @/tmp (/tmp)
- ☑ @/usr/local (/usr/local)
- ☑ @/var/cache (/var/cache)
- ☑ @/var/crash (/var/crash)
- ☑ @/var/lib/libvirt/images (/var/lib/libvirt/images)
- ☑ @/var/lib/machines (/var/lib/machines)
- ☑ @/var/lib/mailman (/var/lib/mailman)
- ☑ @/var/lib/mariadb (/var/lib/mariadb)
- ☑ @/var/lib/mysql (/var/lib/mysql)
- ☑ @/var/lib/named (/var/lib/named)

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 SUSE 11and Red Hat 6 or later.


Post Recovery Network Mozilla Firefox
localhost/post_recovery_network.php

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.

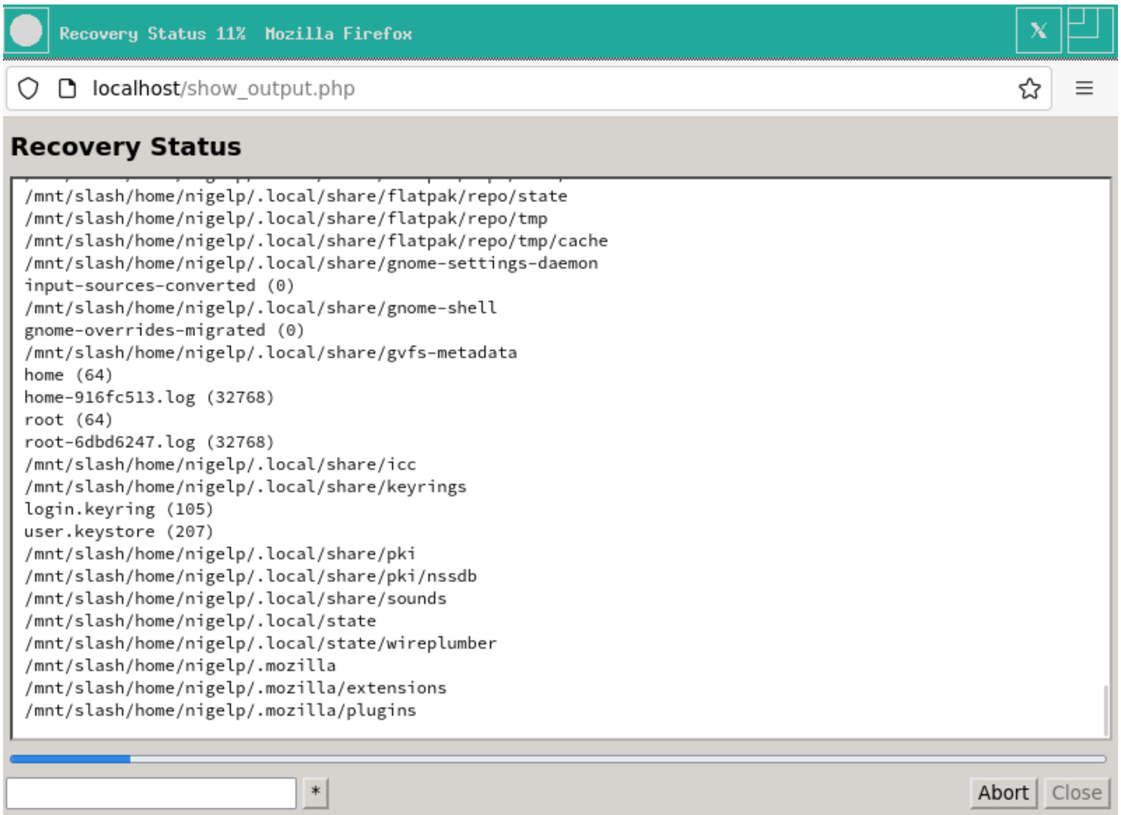
Enabled	Interface	MAC Address	IP Address	Subnet Mask	DHCP
☑	eth0	00:0c:29:ec:93:a2	10.10.11.9	255.0.0.0	□

Post Recovery Script	
Hostname	BMR-Test
Gateway	10.0.1.100
Nameserver (1)	10.0.1.108

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.

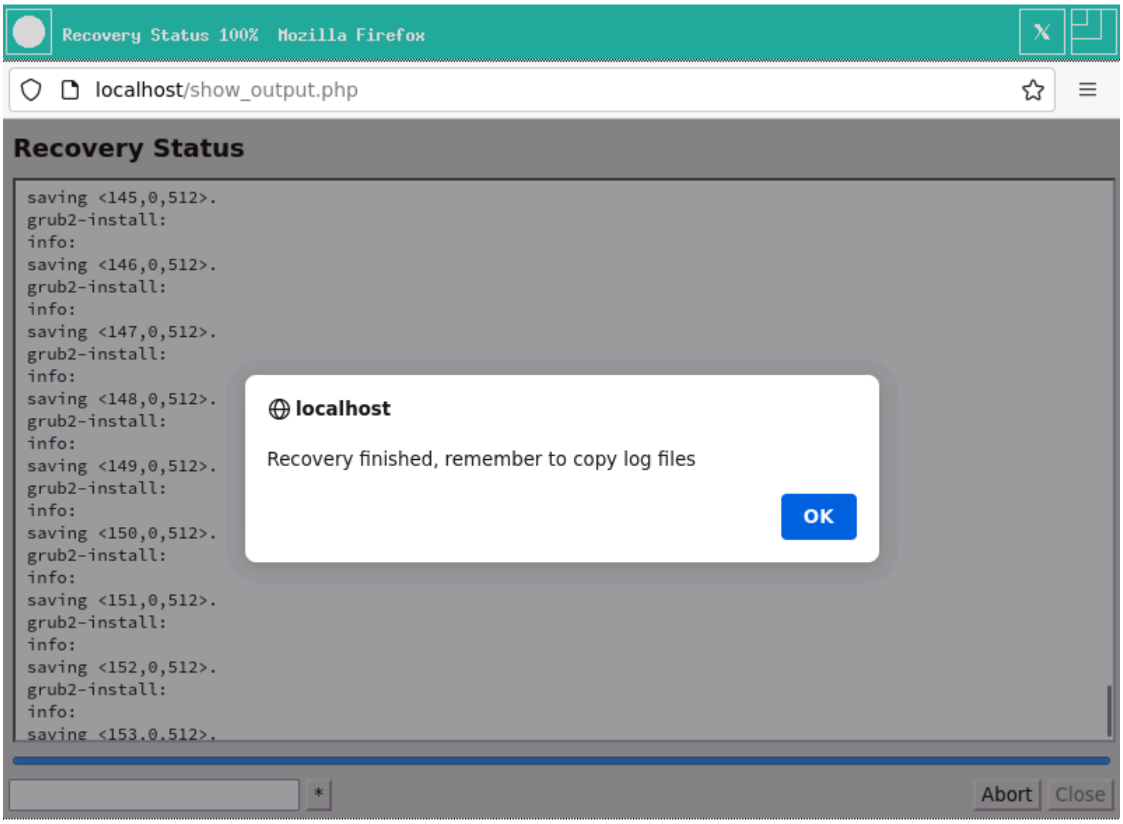
To begin your recovery, click Next> on the **Start Recovery** menu. The recovery will commence with the disk configuration step.


Recovery Status 11% Mozilla Firefox
localhost/show_output.php
Abort
Close

Recovery Status

```
/mnt/slash/home/nigelp/.local/share/flatpak/repo/state
/mnt/slash/home/nigelp/.local/share/flatpak/repo/tmp
/mnt/slash/home/nigelp/.local/share/flatpak/repo/tmp/cache
/mnt/slash/home/nigelp/.local/share/gnome-settings-daemon
input-sources-converted (0)
/mnt/slash/home/nigelp/.local/share/gnome-shell
gnome-overrides-migrated (0)
/mnt/slash/home/nigelp/.local/share/gvfs-metadata
home (64)
home-916fc513.log (32768)
root (64)
root-6dbd6247.log (32768)
/mnt/slash/home/nigelp/.local/share/icc
/mnt/slash/home/nigelp/.local/share/keyrings
login.keyring (105)
user.keystore (207)
/mnt/slash/home/nigelp/.local/share/pki
/mnt/slash/home/nigelp/.local/share/pki/nssdb
/mnt/slash/home/nigelp/.local/share/sounds
/mnt/slash/home/nigelp/.local/state
/mnt/slash/home/nigelp/.local/state/wireplumber
/mnt/slash/home/nigelp/.mozilla
/mnt/slash/home/nigelp/.mozilla/extensions
/mnt/slash/home/nigelp/.mozilla/plugins
```

When the recovery has completed, it will prompt you to copy the log files:


Recovery Status 100% Mozilla Firefox
localhost/show_output.php
Abort
Close

Recovery Status

```
saving <145,0,512>.
grub2-install:
info:
saving <146,0,512>.
grub2-install:
info:
saving <147,0,512>.
grub2-install:
info:
saving <148,0,512>.
grub2-install:
info:
saving <149,0,512>.
grub2-install:
info:
saving <150,0,512>.
grub2-install:
info:
saving <151,0,512>.
grub2-install:
info:
saving <152,0,512>.
grub2-install:
info:
saving <153,0,512>.
```

localhost

Recovery finished, remember to copy log files

OK

Select OK, followed by Close to return to the Main Recovery menu.

Copyright © 2003-2024 Cristie Software Ltd.

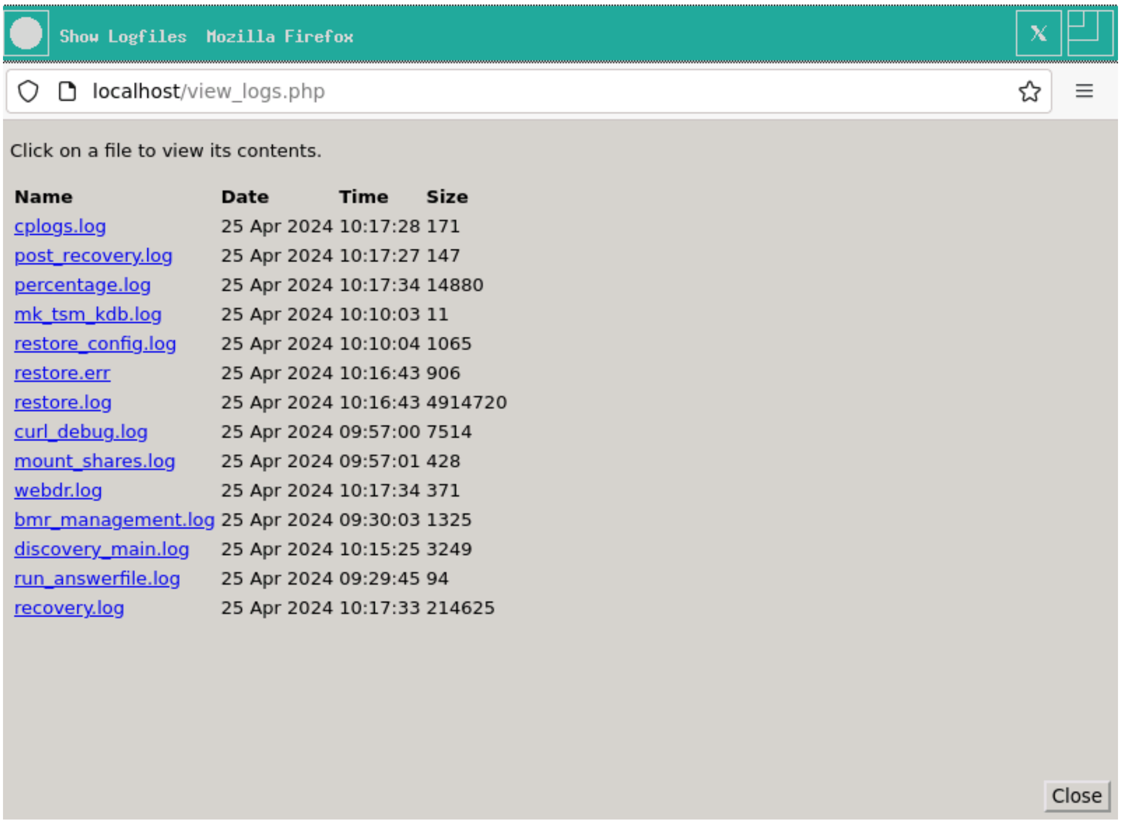
8.4 Post Recovery Options

After performing a recovery (and before booting the recovered system), it is possible to undertake the following actions:

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

8.4.1 Show Log Files

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



Click on a file to view its contents.

Name	Date	Time	Size
cplogs.log	25 Apr 2024	10:17:28	171
post_recovery.log	25 Apr 2024	10:17:27	147
percentage.log	25 Apr 2024	10:17:34	14880
mk_tsm_kdb.log	25 Apr 2024	10:10:03	11
restore_config.log	25 Apr 2024	10:10:04	1065
restore.err	25 Apr 2024	10:16:43	906
restore.log	25 Apr 2024	10:16:43	4914720
curl_debug.log	25 Apr 2024	09:57:00	7514
mount_shares.log	25 Apr 2024	09:57:01	428
webdr.log	25 Apr 2024	10:17:34	371
bmr_management.log	25 Apr 2024	09:30:03	1325
discovery_main.log	25 Apr 2024	10:15:25	3249
run_answerfile.log	25 Apr 2024	09:29:45	94
recovery.log	25 Apr 2024	10:17:33	214625

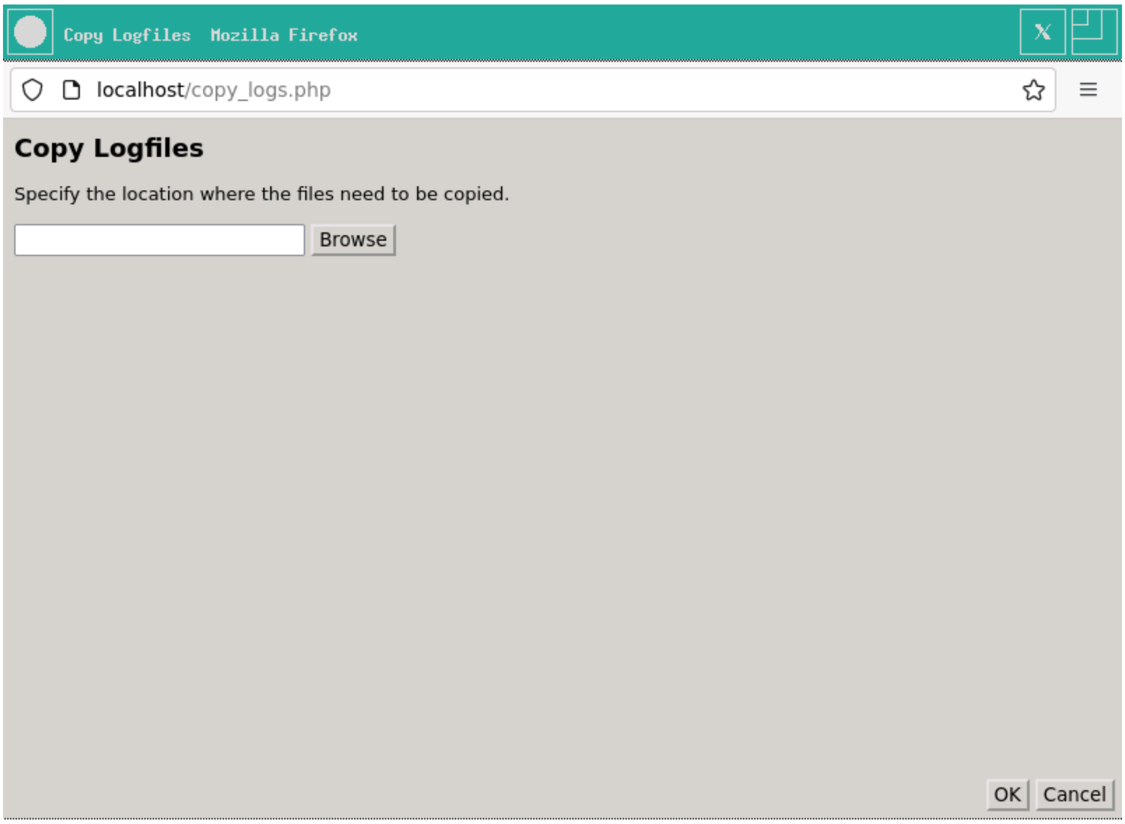
Click on the log you wish to view. Check the summary information at the bottom of the recovery status report for any errors.

Click Close to finish.

8.4.2 Copy Log Files

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

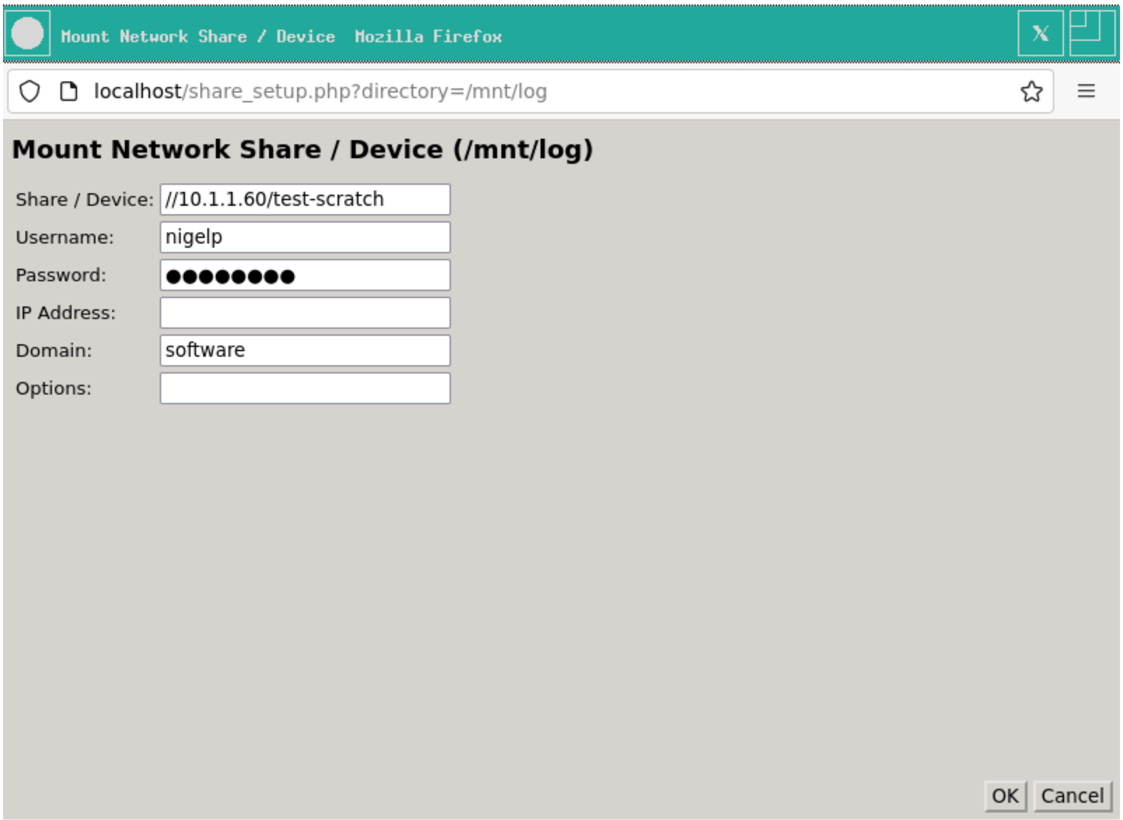
Click Browse to select a location to copy the log files to.



Copy Logfiles

Specify the location where the files need to be copied.

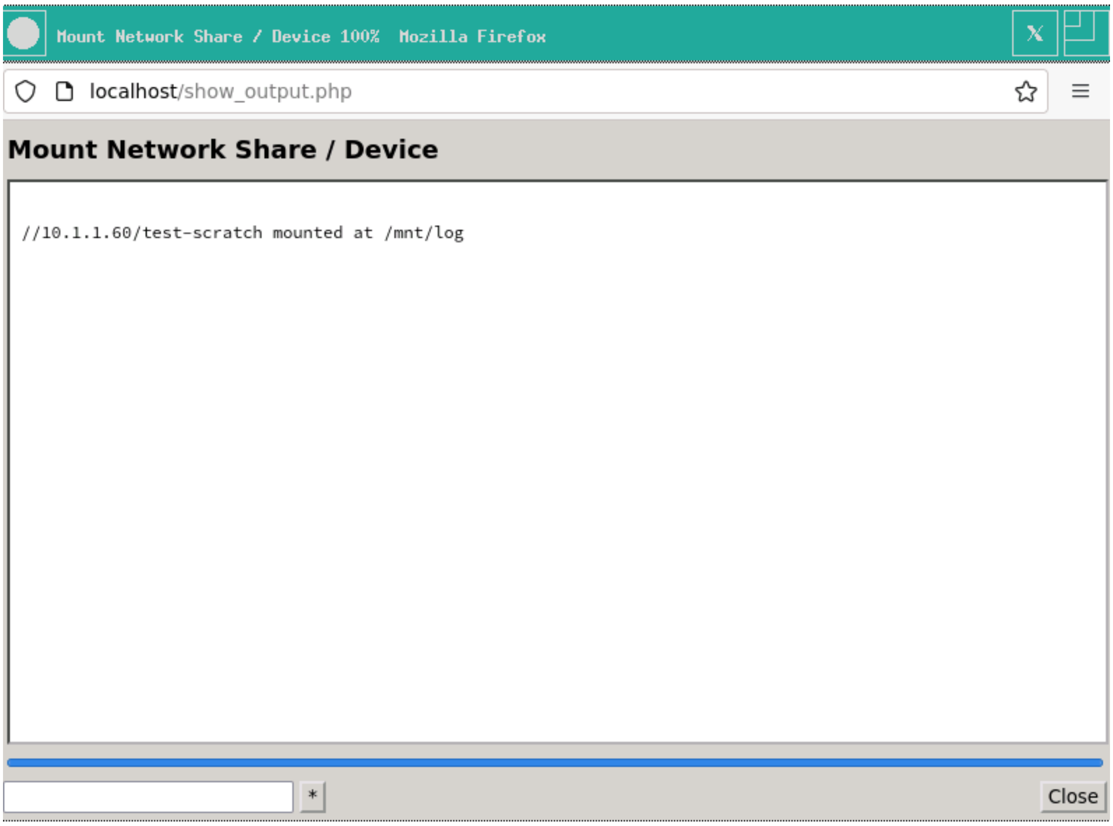
Select Browse to mount a network drive.


Mount Network Share / Device Mozilla Firefox
localhost/share_setup.php?directory=/mnt/log

Mount Network Share / Device (/mnt/log)

Share / Device:	//10.1.1.60/test-scratch
Username:	nigelp
Password:	●●●●●●●●
IP Address:	
Domain:	software
Options:	

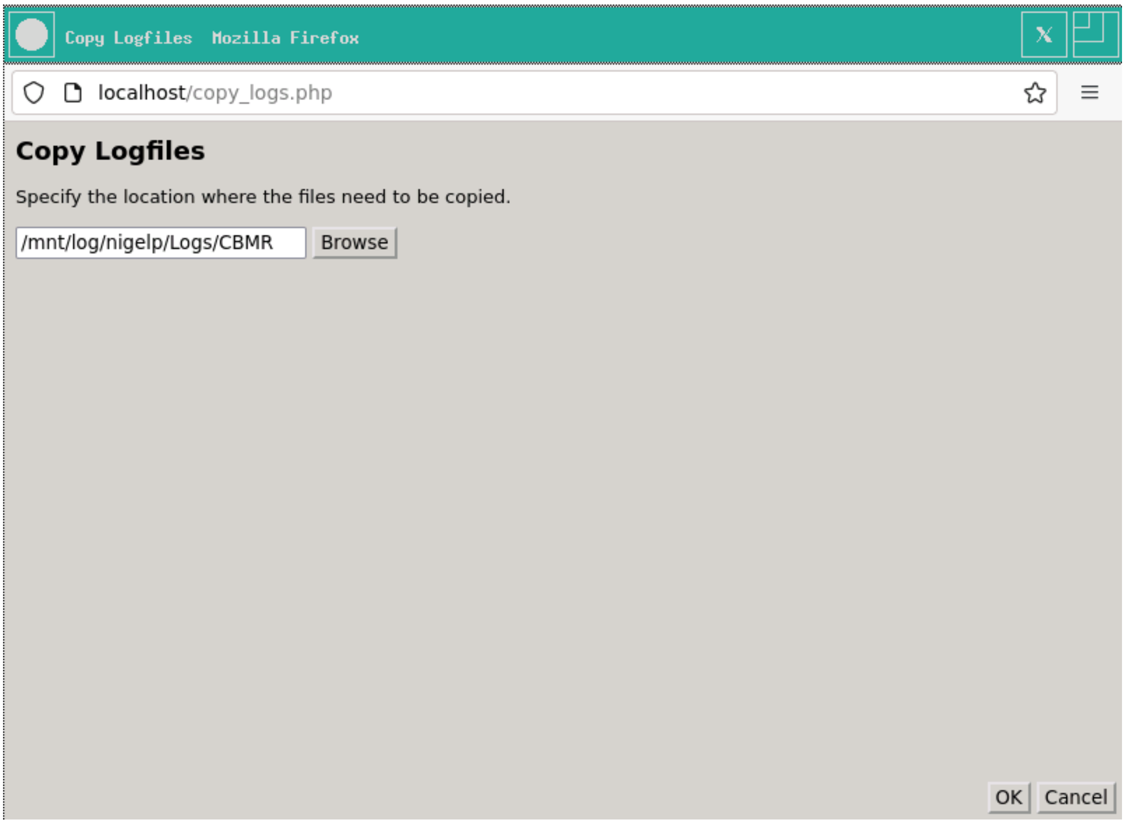
A successful mount is signified by:



Mount Network Share / Device 100% Mozilla Firefox
localhost/show_output.php
Mount Network Share / Device

```
//10.1.1.60/test-scratch mounted at /mnt/log
```

Select a directory on the mounted share:

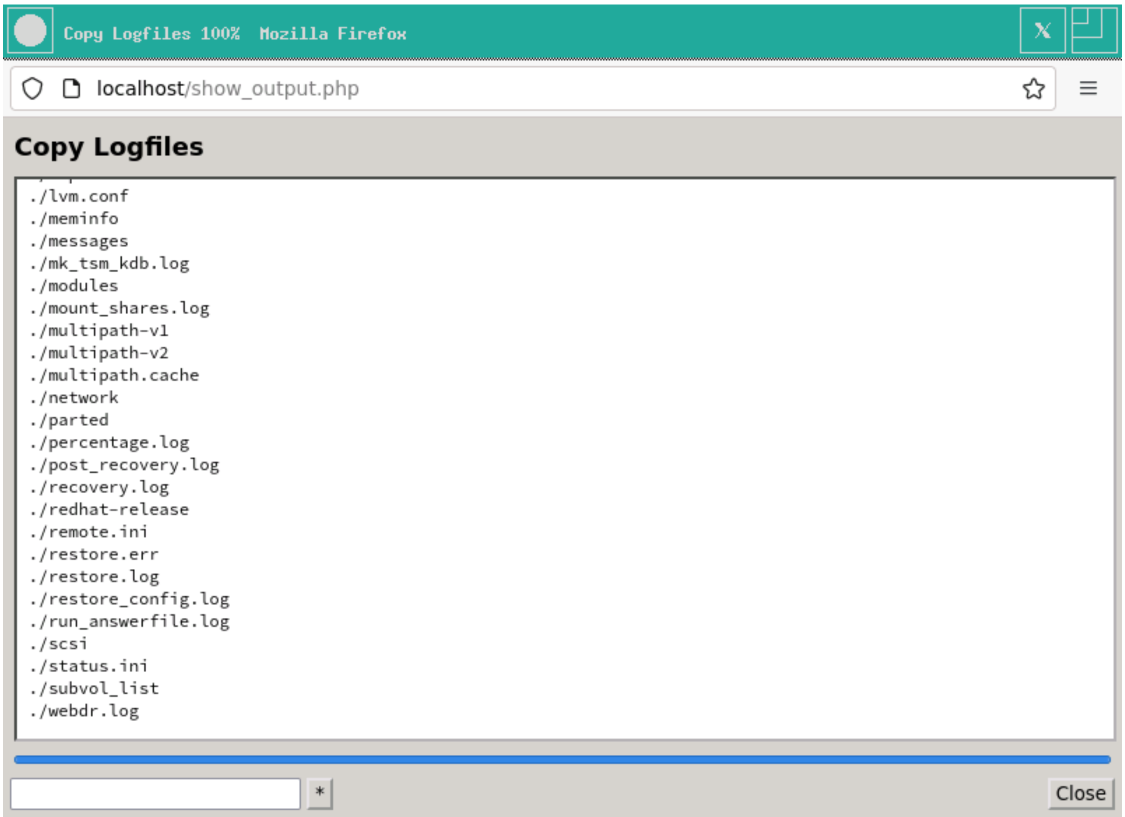


Copy Logfiles

Specify the location where the files need to be copied.

/mnt/log/nigelp/Logs/CBMR

Click OK to copy the logfiles.


Copy Logfiles 100% Mozilla Firefox
localhost/show_output.php
Copy Logfiles
Close

```
./lvm.conf
./meminfo
./messages
./mk_tsm_kdb.log
./modules
./mount_shares.log
./multipath-v1
./multipath-v2
./multipath.cache
./network
./parted
./percentage.log
./post_recovery.log
./recovery.log
./redhat-release
./remote.ini
./restore.err
./restore.log
./restore_config.log
./run_answerfile.log
./scsi
./status.ini
./subvol_list
./webdr.log
```

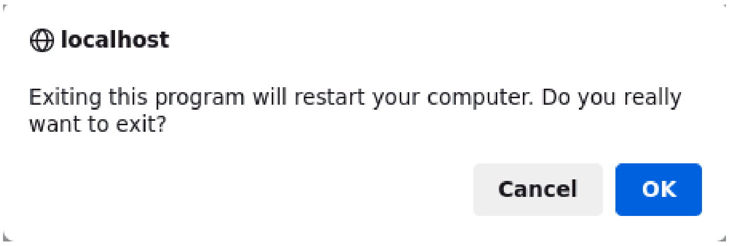
Ensure this is a location which can be easily accessed in case there is a need to email the log files to Cristie for support purposes.

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.*

8.5 Boot Recovered System

You should now restart the recovered machine by clicking 🖥 on the **Cristie Recovery Environment** menu. You will then have the option to confirm reboot or return to the main menu.



Exiting this program will restart your computer. Do you really want to exit?

8.6 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 CBMR DR principles and procedures.

The command line parameters supplied to the script are divided into 4 groups, **Network**, **Mount, File (VTD), IBM Spectrum Protect (TSM)** 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

File (VTD) options:

--cbmr_vtd=<path>	Set path to VTD file

IBM Spectrum Protect (TSM) options:

--tsm_ip_address=<ip_address>	Set TSM server IP address
--tsm_port=<number>	Set TSM server port number
--tsm_node=<string>	Set TSM server node name
--tsm_passwd=<string>	Set TSM server password
--tsm_certificate=<path>	Set TSM certificate path
--cbmr_tsm_node=<string>	Set TSM node name
--cbmr_tsm_passwd=<string>	Set TSM node password
--cbmr_tsm_filespace=<string>	Set TSM node filespace name
	forces a tar backup of /boot - this is needed for block based backups to work

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, rbmr or tbmr

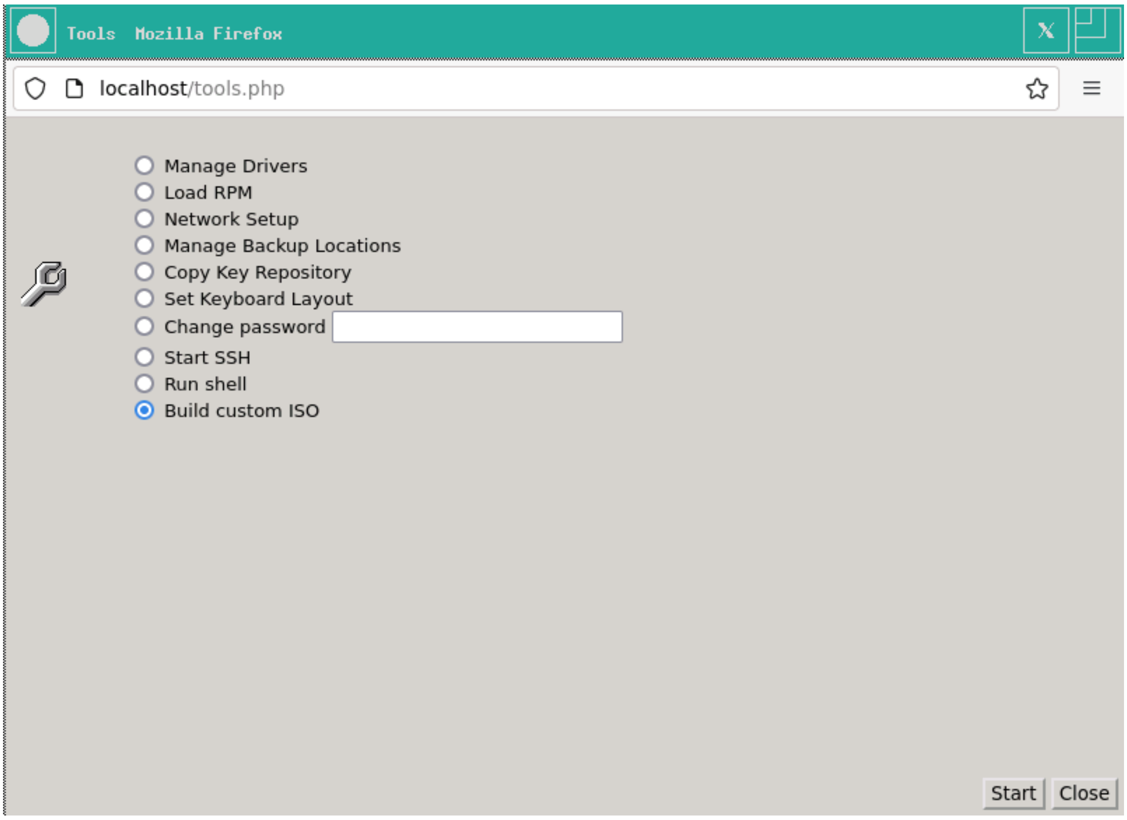
Example (a TBMR recovery)

```
restore --product=tbmr --reload="ibmveth old_large_send=1" --ethtool="-K eth0 tso on"
        --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.

8.7 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.

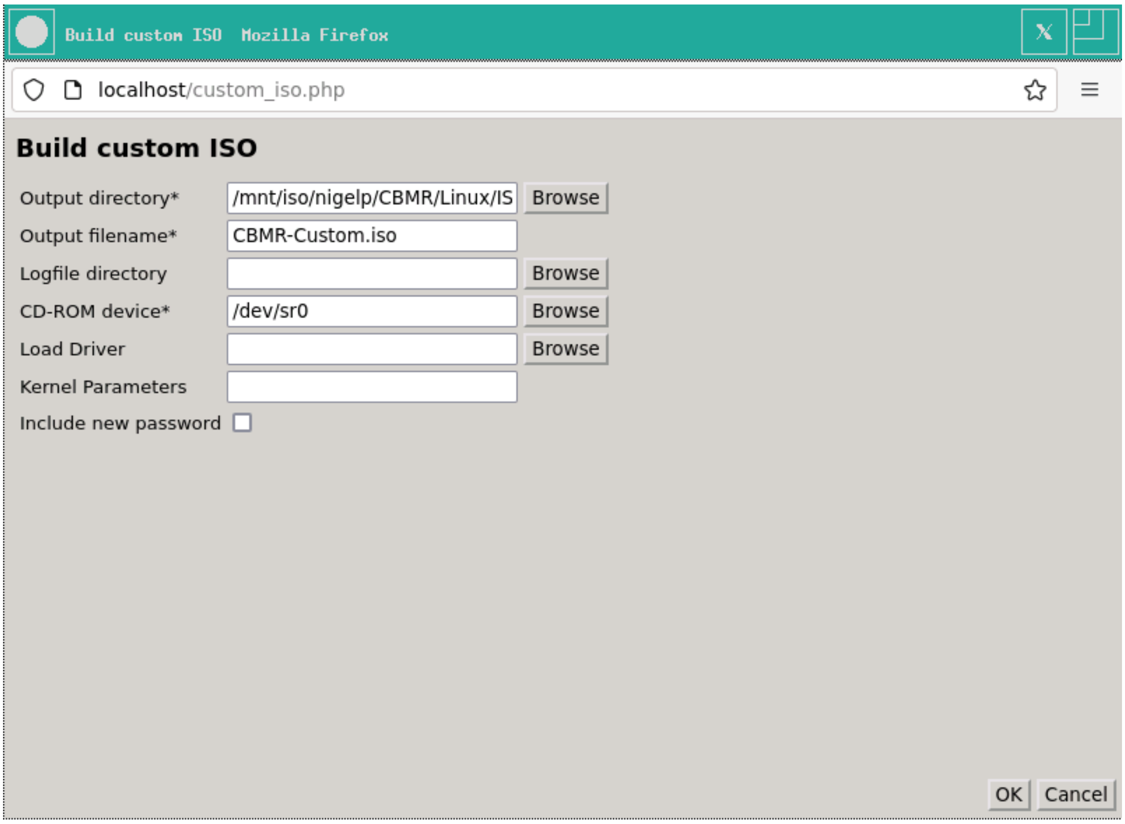


Tools Mozilla Firefox

localhost/tools.php

- ○ Manage Drivers
- ○ Load RPM
- ○ Network Setup
- ○ Manage Backup Locations
- ○ Copy Key Repository
- ○ Set Keyboard Layout
- ○ Change password
- ○ Start SSH
- ○ Run shell
- ● Build custom ISO

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



Build custom ISO

Output directory* /mnt/iso/nigelp/CBMR/Linux/IS

Output filename* CBMR-Custom.iso

Logfile directory

CD-ROM device* /dev/sr0

Load Driver

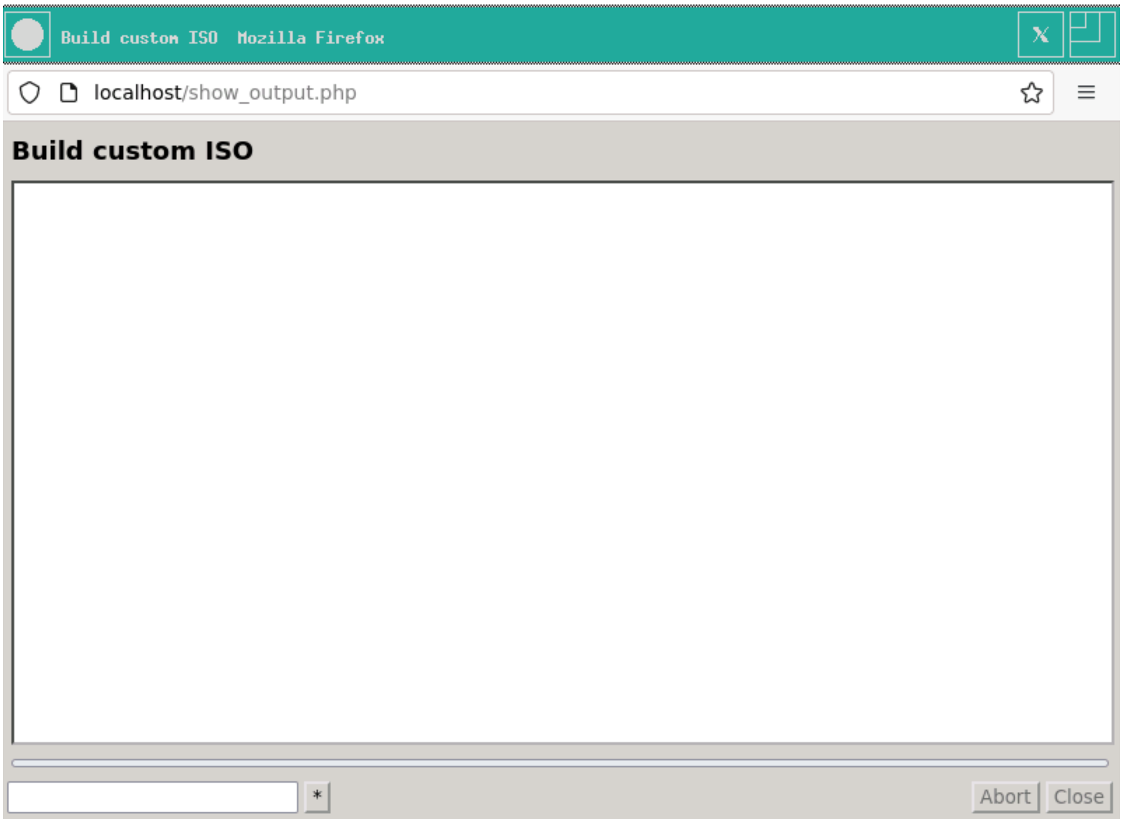
Kernel Parameters

Include new password □

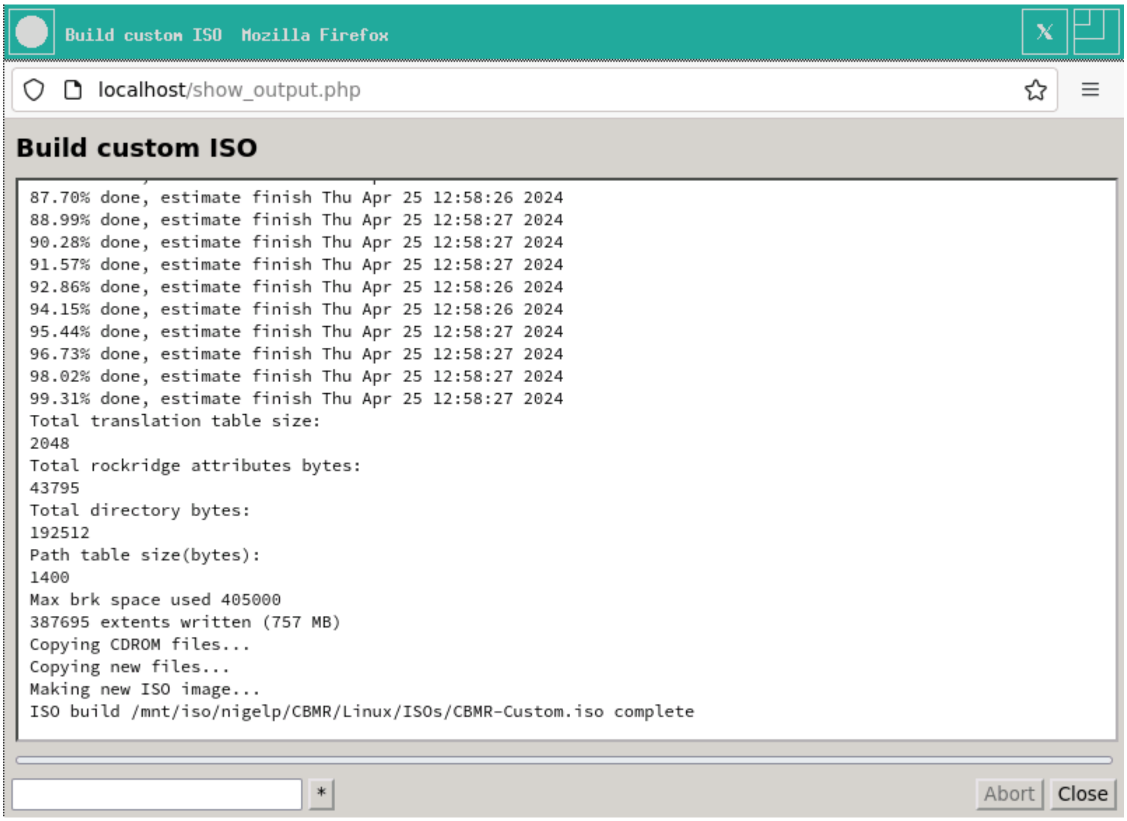
You will need to configure the following fields:

- **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.



```
87.70% done, estimate finish Thu Apr 25 12:58:26 2024
88.99% done, estimate finish Thu Apr 25 12:58:27 2024
90.28% done, estimate finish Thu Apr 25 12:58:27 2024
91.57% done, estimate finish Thu Apr 25 12:58:27 2024
92.86% done, estimate finish Thu Apr 25 12:58:26 2024
94.15% done, estimate finish Thu Apr 25 12:58:26 2024
95.44% done, estimate finish Thu Apr 25 12:58:27 2024
96.73% done, estimate finish Thu Apr 25 12:58:27 2024
98.02% done, estimate finish Thu Apr 25 12:58:27 2024
99.31% done, estimate finish Thu Apr 25 12:58:27 2024
Total translation table size:
2048
Total rockridge attributes bytes:
43795
Total directory bytes:
192512
Path table size(bytes):
1400
Max brk space used 405000
387695 extents written (757 MB)
Copying CDROM files...
Copying new files...
Making new ISO image...
ISO build /mnt/iso/nigelp/CBMR/Linux/ISOs/CBMR-Custom.iso complete
```

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 Cristie Technical Support

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

- CBMR 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.