CBMR AIX

Bare Machine Recovery

Quick Start Guide

Version 9.1 released December 2022

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.*
- *CloneManager® 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) 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 About CBMR for AIX

This document provides a **Quick Start Guide** to **CBMR** for **AIX** and us such does not cover the full functionality of the product - just the essential features to get you started.

CBMR for AIX provides a file-based backup and disaster recovery (DR) system for AIX 7.1 to 7.3.

The process of backing up and recovering an AIX machine comprises three phases:

1. **Create a bootable recovery environment from the running machine**

2. **Perform the Disaster Recovery (DR) backup**

3. **Perform the recovery**

All of the above actions may be performed using the Graphical User Interface run from the command `cbmr`. Documentation describing command line tools with the same functionality is also included, allowing you to easily create scripted backups.

Use the command man cbmr to get an overview of CBMR functionality and the command line tools available.

> ***Note: CBMR must be installed and run by a user that has root access***

3 System Requirements

Please refer to this web page https://www.cristie.com/support/matrix/ to determine the latest OS support and minimum hardware requirements for CBMR Version 9.1.

> *Note: A minimum of 6 GB of RAM is required to boot and perform a recovery using the CBMR Disaster Recovery boot ISO.*

CBMR for AIX is suitable for all versions of AIX 7.1 to 7.3 and later.

SSL is a prerequisite for the Licensing Manager as it links `libcrypto` and `libssl`, both of which are supplied by SSL. These files are supplied as part of the installation.

Prerequisites

An appropriate version of the IBM Spectrum Protect agent should optionally be installed prior to the installation of CBMR.

Otherwise the CBMR distribution media includes everything you need. In particular the module `cristielibs-9.1.1-1.aix6.1.ppc64` contains all the prerequisites required.

You can then install CBMR for AIX via rpm;

```
rpm -ivh *.rpm
```

This installs the rpms in the correct sequence. If you wish to install them one at a time install in this order:

- `rpm -ivh cristielibs-9.1.1-1.aix6.1.ppc64.rpm`
- `rpm -ivh ncurses-6.1.3.aix6.1.ppc64.rpm`
- `rpm -ivh screen-4.6.2-1.aix6.1.ppc64.rpm`
- `rpm -ivh cbmr-9.1.1-1.aix6.1.ppc64.rpm`

You may be prompted should the install fail, to increase the filesystem size of `/opt` using;-

```
chfs -a size=+xxxxxxxxxx /opt
```

These are included with the installation and may also be downloaded from the IBM AIX Toolbox for Linux website:

http://www-03.ibm.com/systems/power/software/aix/linux/toolbox/download.html

4 CBMR for AIX Software

At the moment CBMR is supplied upon request. Please contact sales@cristie.com in the first instance. After successful evaluation you will then be provided with an FTP download link for the installation package.

5 Installation

The product installation media is supplied in **tar.gz** format typically in the form:

```
cbmr-9.1.3266.aix.tar.gz
```

Extract the contents of this file to (say) /tmp before proceeding with the installation.

CBMR can be installed via the **AIX System Management Interface** - smit or smitty - directly via RPM or from the archive. It is recommended that all installation files are installed using the same method.

The installation of CBMR requires the RPM package management tool: `fileset rpm.rte 3.0.5.20 or later`. This tool is installed by default on AIX 6.1 or later.

The version of this tool can be checked using the command `'lslpp -1 rpm.rte'`. If the fileset is at an earlier maintenance level, then the `rpm.rte` file can be downloaded individually from: http://www-933.ibm.com/support/fixcentral/

Depending on the size of the filesystems `chfs` may be required to increase the size of `/opt`

5.1 Install via Smit/Smitty

CBMR can be installed via smit or smitty by selecting the fastpath 'install', for example by running:

```
smitty install
```

The installation directory should be the `'/bffs'` directory on the CD or in the archive.

The prerequisites listed on the preceding page are contained in the directory alongside CBMR and are installed automatically.

> ***Note: the smitty installation delegates to RPM. Therefore, if some packages have already been installed via RPM then the latest version available is selected.***

5.2 Install via RPM

CBMR can also be installed using the RPM package management tool. The RPM packages are contained in the `'/rpms'` directory as part of the extracted tar archive.

Install the rpms using a command like this:

```
rpm -ivh *.rpm
```

As with the smitty installation, the open-source prerequisites are contained in this directory alongside CBMR.

The versions of prerequisites may be checked using a command like this:

```
rpm -q ncurses libxml2
```

5.3 License

Following the instructions in this section will result in a standard 30-day trial license being installed. **Cristie** provide a 30 day trial license so that the product can be fully evaluated before purchase.

If you have purchased a full license, you will have been sent a contract identifier and activation code, these can be used to activate the product with the `licmgr` tool as follows:

```
licmgr -p cbmr --act YU5ZQCSR-C962R6YD-PYKKTSA5-ZFHJ7FKN
```

Note the above codes are examples only - please use the activation codes sent to you. More information about the `licmgr` tool can be found by typing `'man licmgr'`.

5.4 Uninstall

To uninstall if installed via smit or smitty, run `'smit remove'` or `'smitty remove'`, then select the relevant packages for removal.

To uninstall the RPM package, enter:

```
rpm -e cbmr
```

Note: uninstalling does NOT remove the original installation directory with the extracted tar.gz files.

6 Product Licensing

When first installed, CBMR may be used for a trial period of 30 days. During that period CBMR is fully functional. If the software is subsequently un-installed and later re-installed on the same system, the 30 day period continues from the date of the first installation.

If you wish to use the software beyond the trial period, you must register and purchase a license from Cristie Software Ltd.. Alternatively, and in special circumstances, Cristie Software Ltd. may extend the license period if you wish to trial the software beyond that period.

If you purchase the product, then contract and license activation codes will be available on the Cristie Licensing Portal. Together these codes will enable you to fully activate the product.

The following sections discuss this in more detail.

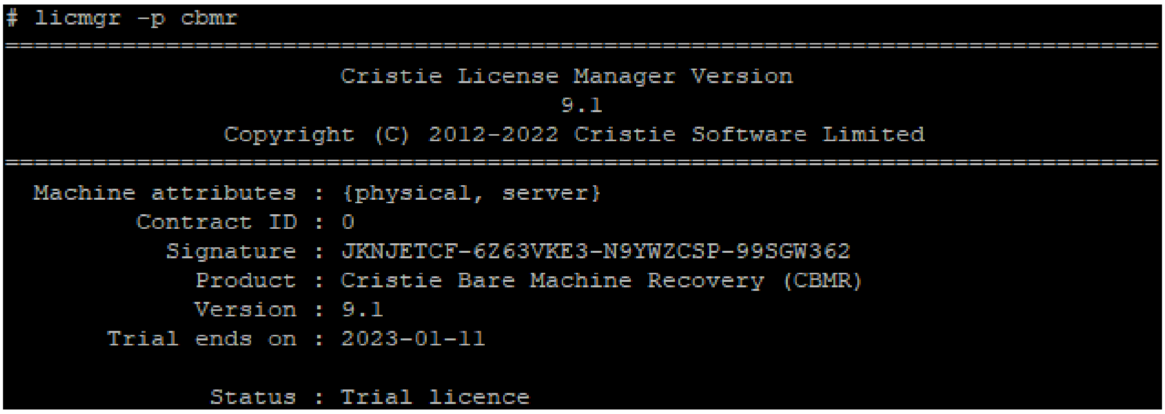
6.1 Trial License

A 30-day trial license commences from the date of installation. The CBMR configuration file generator cbmrcfg will not run after this period expires.

You may use the Cristie License Manager to add or inspect license details at any time. This is acheived by opening a terminal and entering:

```
licmgr -p cbmr
```

Entering this command, will display the Cristie License Manager. This shows Machine attributes, Contract ID. the installed host System signature, the current product, the product version, the trial end date and the current license Status.



```
# licmgr -p cbmr
==============================================================================
                       Cristie License Manager Version
                                     9.1
               Copyright (C) 2012-2022 Cristie Software Limited
==============================================================================
  Machine attributes : {physical, server}
         Contract ID : 0
           Signature : JKNJETCF-6Z63VKE3-N9YWZCSP-99SGW362
             Product : Cristie Bare Machine Recovery (CBMR)
             Version : 9.1
       Trial ends on : 2023-01-11

              Status : Trial licence
```

The CBMR configuration file generator will become active again as as a full license has been purchased from Cristie Software Ltd. and the new contract and activation code entered via the Cristie License Manager

6.2 Full License

A Full license entitles the Customer to product support and upgrades for the duration of the license period.

To upgrade from the trial license to a full license, you need to apply for a full license activation code via the Cristie Licensing Portal website. You will need to first register an account on the Cristie Licensing Portal (located at https://portal.cristie.com/login). A Contract ID will be created and provided to you when you purchase a license.

These are the various codes used in the Cristie licensing process:

Contract ID: A 4-digit number supplied by Cristie Software Ltd. Sales during the license purchase process.
Agreement Number: Same as *Contract ID* at the moment.
Contract Code: 35-character contract code obtained from the Cristie Licensing Portal
Activation Code: 35-character support activation code obtained from the Cristie Licensing Portal

In special circumstances a 'bulk license' may be issued by Cristie Software Ltd. for customers that order a significant number of product licenses. Please contact your Cristie sales representative if you wish to discuss this service.

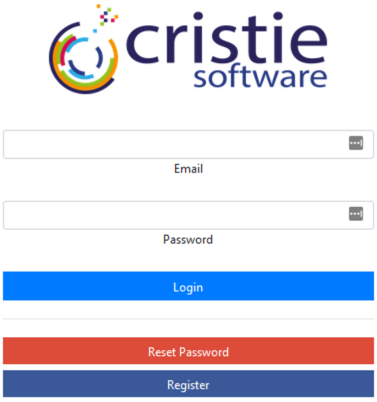
> ***Note this discussion assumes that CBMR is already installed on a Customer production machine.***

6.2.1 Setting up a Cristie Licensing Portal account

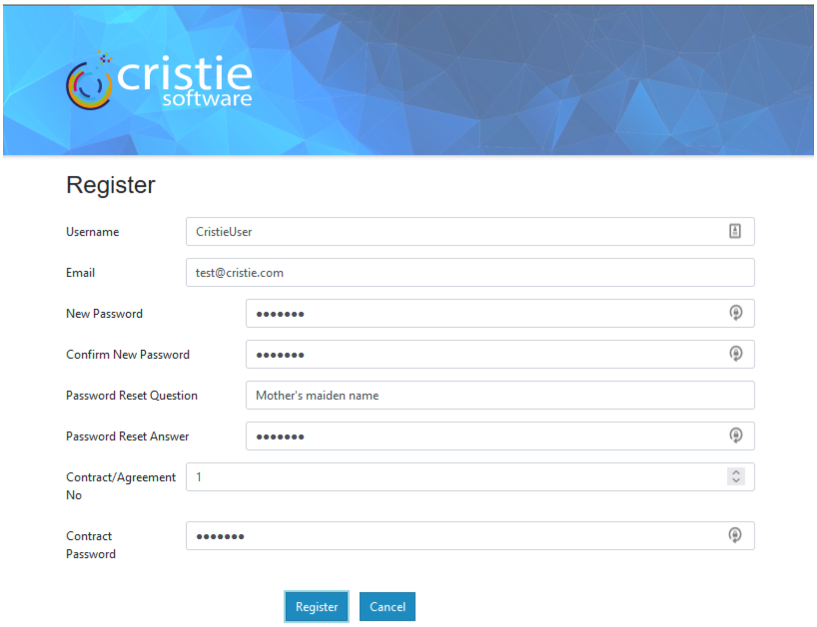
To setup a new account on the Cristie Licensing Portal follow the following steps. To do this you will need your 4-digit Contract ID and contract setup password. These will be provided by email from Cristie Software Ltd. when you purchase a product license.

> ***Note: Your Contract ID may have been supplied to you as your contract Agreement Number. In that case please use your Agreement number in place of the Contract ID throughout.***

1. On a suitable machine that has Internet access run a browser (such as Google Chrome) and navigate to the Cristie Licensing Portal web page at `https://portal.cristie.com/login`.



Select Register to create a new account. Enter your new account details (note this is an example):



Register

Username: CristieUser

Email: test@cristie.com

New Password: •••••••

Confirm New Password: •••••••

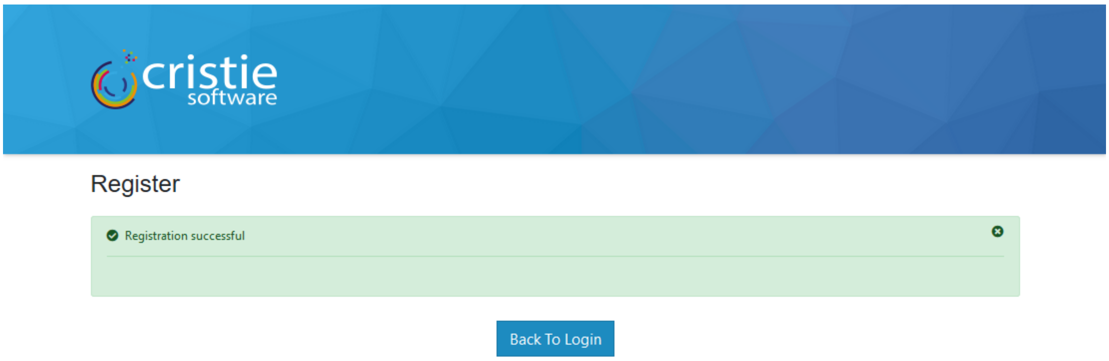
Password Reset Question: Mother's maiden name

Password Reset Answer: •••••••

Contract/Agreement No: 1

Contract Password: •••••••

Then click Register. If successful the following is shown.



Register

Registration successful

At this point you may now log in to the Cristie Licensing Portal using the E-mail ID and password setup in the previous steps.

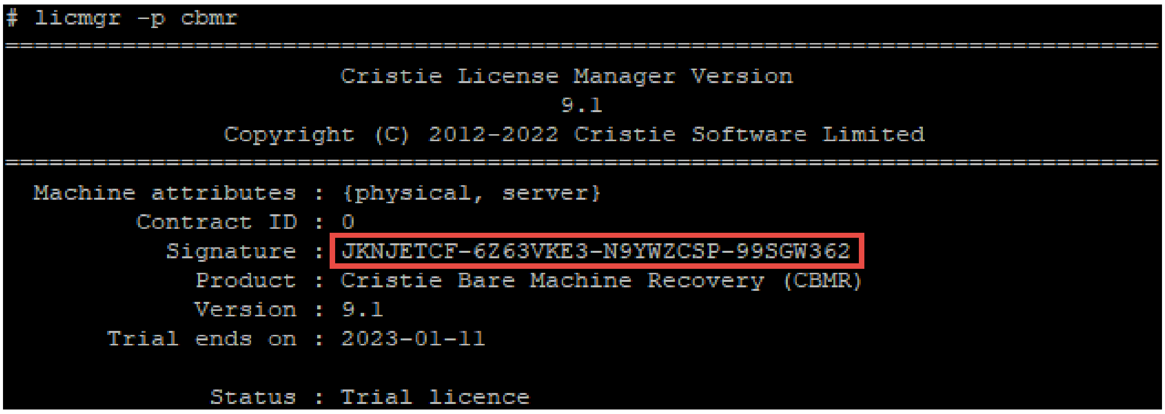
6.2.2 Manual Activation

This involves activating using the Cristie Licensing Portal are as follows. This discussion assumes your contract is already setup on the Cristie Licensing Portal

Assign your Activation code on the CBMR host machine by opening up a terminal and entering:

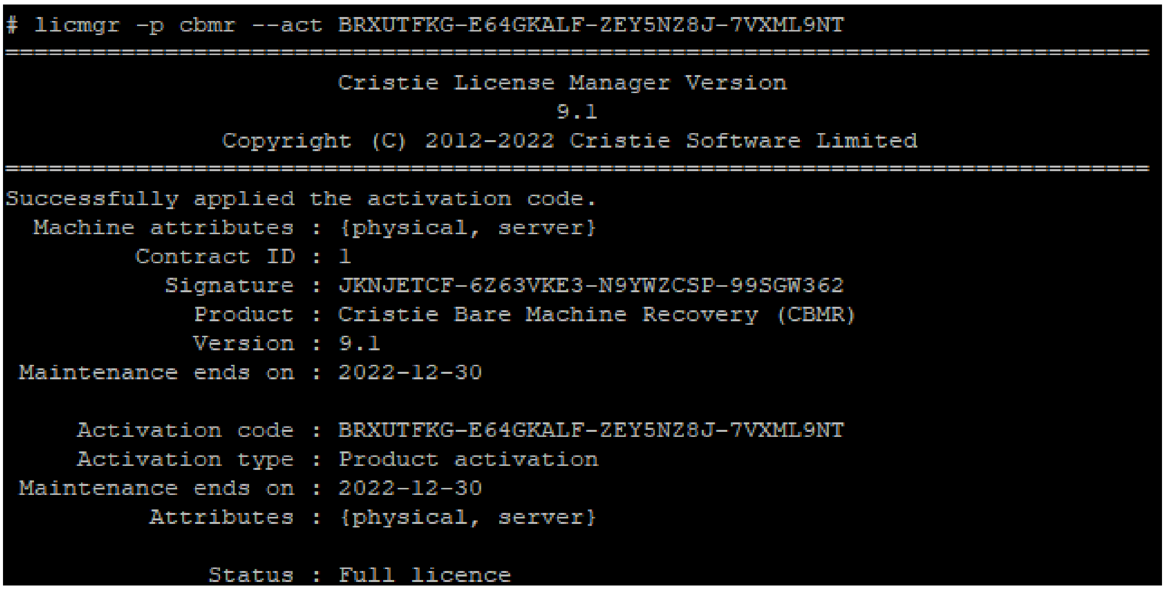
```
licmgr -p cbmr --act xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx
```

(where xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx is your Activation code, which can be obtained by signing into the Cristie Licensing Portal) and use the Activate Licenses option. You will need your host's IP address, hostname and license signature. The latter can be obtained from the licmgr -p cbmr output.



```
# licmgr -p cbmr
===============================================================================
                       Cristie License Manager Version
                                     9.1
                   Copyright (C) 2012-2022 Cristie Software Limited
===============================================================================
  Machine attributes : {physical, server}
         Contract ID : 0
           Signature : JKNJETCF-6Z63VKE3-N9YWZCSP-99SGW362
             Product : Cristie Bare Machine Recovery (CBMR)
             Version : 9.1
       Trial ends on : 2023-01-11

              Status : Trial licence
```

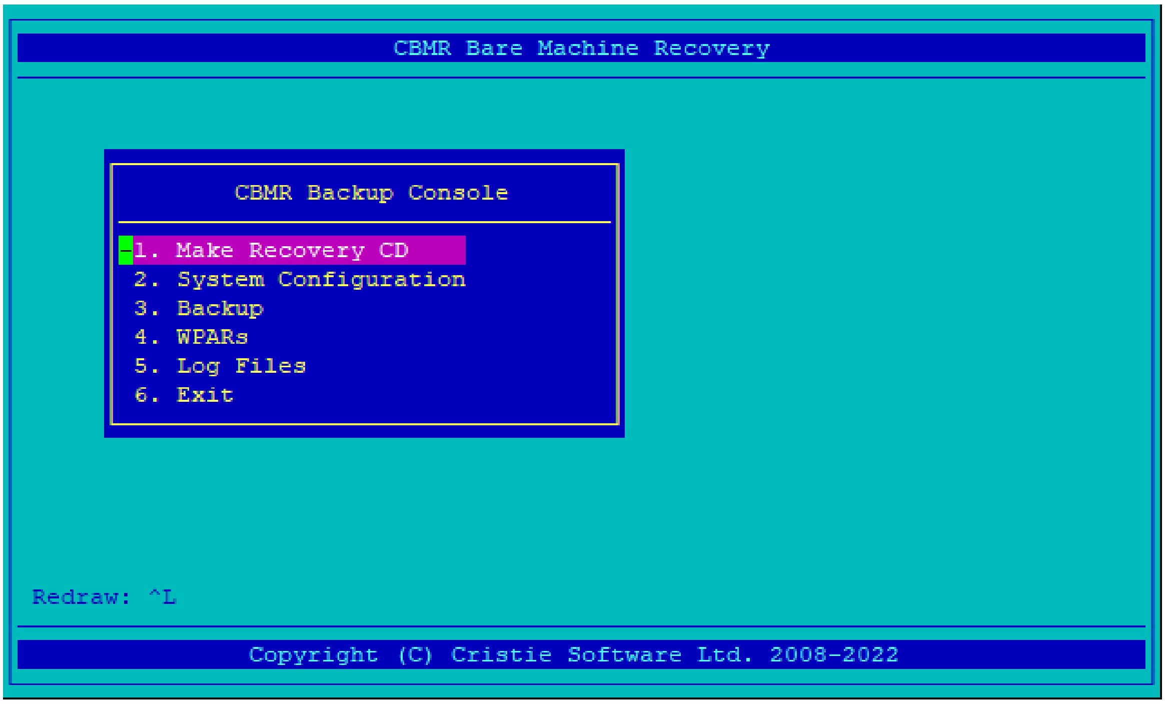
After activation the Cristie License Manager will be refreshed showing your Contract ID, the new Activation code and your contract support end date.



```
# licmgr -p cbmr --act BRXUTFKG-E64GKALF-ZEY5NZ8J-7VXML9NT
===============================================================================
                       Cristie License Manager Version
                                     9.1
                   Copyright (C) 2012-2022 Cristie Software Limited
===============================================================================
Successfully applied the activation code.
  Machine attributes : {physical, server}
         Contract ID : 1
           Signature : JKNJETCF-6Z63VKE3-N9YWZCSP-99SGW362
             Product : Cristie Bare Machine Recovery (CBMR)
             Version : 9.1
 Maintenance ends on : 2022-12-30

     Activation code : BRXUTFKG-E64GKALF-ZEY5NZ8J-7VXML9NT
     Activation type : Product activation
 Maintenance ends on : 2022-12-30
          Attributes : {physical, server}

              Status : Full licence
```

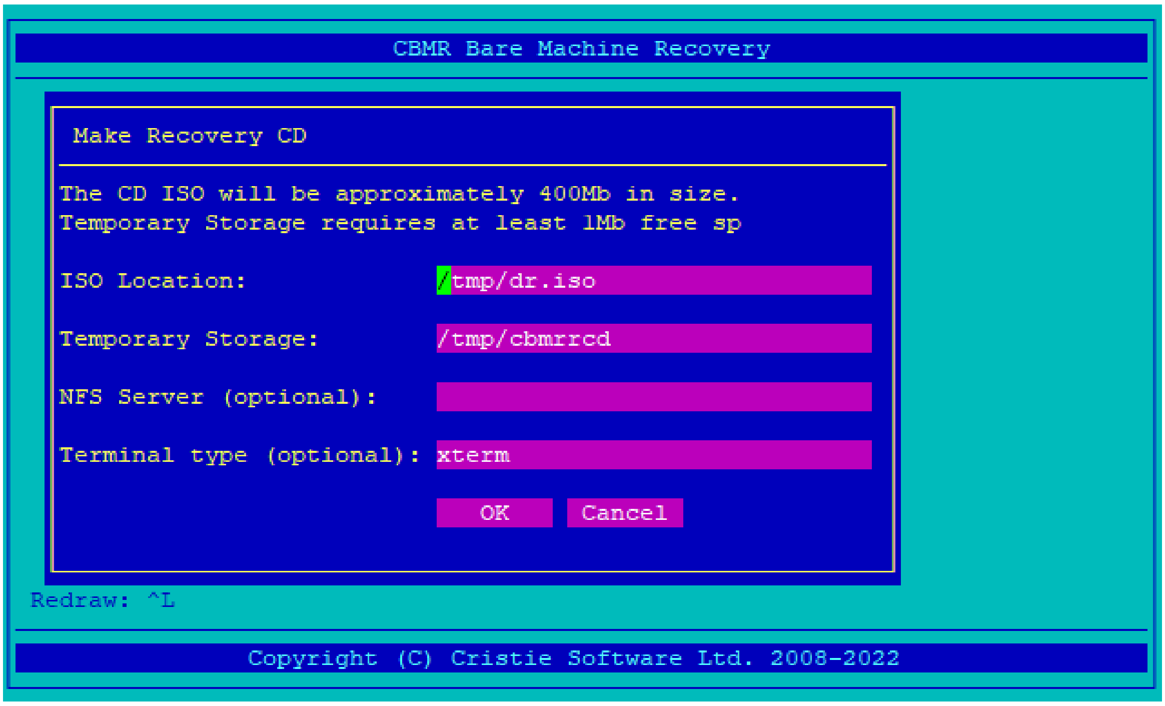
7 Creating a Recovery Image

As mentioned previously, all functionality can be accessed through the CBMR Graphical User Interface. After entering the command 'cbmr', the CBMR Console menu is presented:



```
CBMR Bare Machine Recovery

CBMR Backup Console

1. Make Recovery CD
2. System Configuration
3. Backup
4. WPARs
5. Log Files
6. Exit

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

The first step is to create a recovery CD or PXE/NIM bootable image. This is an iso image that can be used directly, burned to CD or extracted to create a network boot environment.



```
CBMR Bare Machine Recovery

Make Recovery CD

The CD ISO will be approximately 400Mb in size.
Temporary Storage requires at least 1Mb free sp

ISO Location:                /tmp/dr.iso

Temporary Storage:           /tmp/cbmrrcd

NFS Server (optional):

Terminal type (optional):    xterm

                                OK       Cancel

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

The terminal type can be specified here if a different terminal is desired on boot up. xterm is recommended as it is compatible with most terminal emulation programs on Windows and UNIX.

The temporary directory is used to create the structure of the CD, which consequently is converted to a file. The GUI creates an iso file which may be burned to a CD using an iso burning tool such as `burn_cd`:

```
burn_cd -d /dev/cd0 recovery_cd.iso
```

Note: the output log for CD creation is saved in '/var/log/cristie/mkdrcd.log'

7.1 PXE Booting

Alternatively, the CD can be extracted to create a PXE bootable environment. If the CD is extracted to the directory `'/recoverycd'` then the PXE environment can be setup as follows:

- **Copy** the file `'ppc/chrp/bootfile.exe'` to the TFTP sever directory
- **Export** `'/recoverycd'` over NFS
- **Create** a DHCP/BOOTP entry for the machine with option 151 specifying the NFS server IP address and 152 specifying the NFS server path

This is an example using ISC dhcpd under RedHat linux (`/etc/dhcp/dhcp.conf`):

```
option aix-server code 151 = ip-address;
option aix-path code 152 = text;

host aix  {
   filename "/bootfile.exe";
   option aix-server 192.168.1.100;
   option aix-path "/recoverycd";
}
```

On an AIX NIM Master, the DHCP configuration itself (`'/etc/dhcpsd.cnf'`) contains detailed instructions to set up a host in the manner detailed above.

This is an example section of `/etc/dhcpsd.cnf` used to enable NIM booting of the recovery environment for the machine with MAC address `'01:02:03:04:05:06:07:08'`:

```
supportBOOTP   yes

client 6 01:02:03:04:05:06:07:08 192.168.1.199 {
  option sa 192.168.1.100
  option hd /recoverycd/
  option bf bootfile.exe
}
```

The attributes for the NFS server address and directory are set in a similar manner.

Alternatively, the NFS server and directory may be set statically for the image by entering the full address (ie. 10.10.14.90:/mnt/SPOT) or just a path (ie. /mnt/SPOT) into the **NFS**

Server dialogue.

> *Note: if this option is used, then the recovery environment attempts to boot from the NFS server and directory given. If only a path is supplied then the recovery environment attempts to use the boot server (either BOOTP or DHCP) and the path supplied. See the auxilliary document "AIXBootingProcedures.pdf" for a more complete explanation"*

8 Performing a DR backup

Performing a DR backup is split into two stages:

1. **Record** system information.

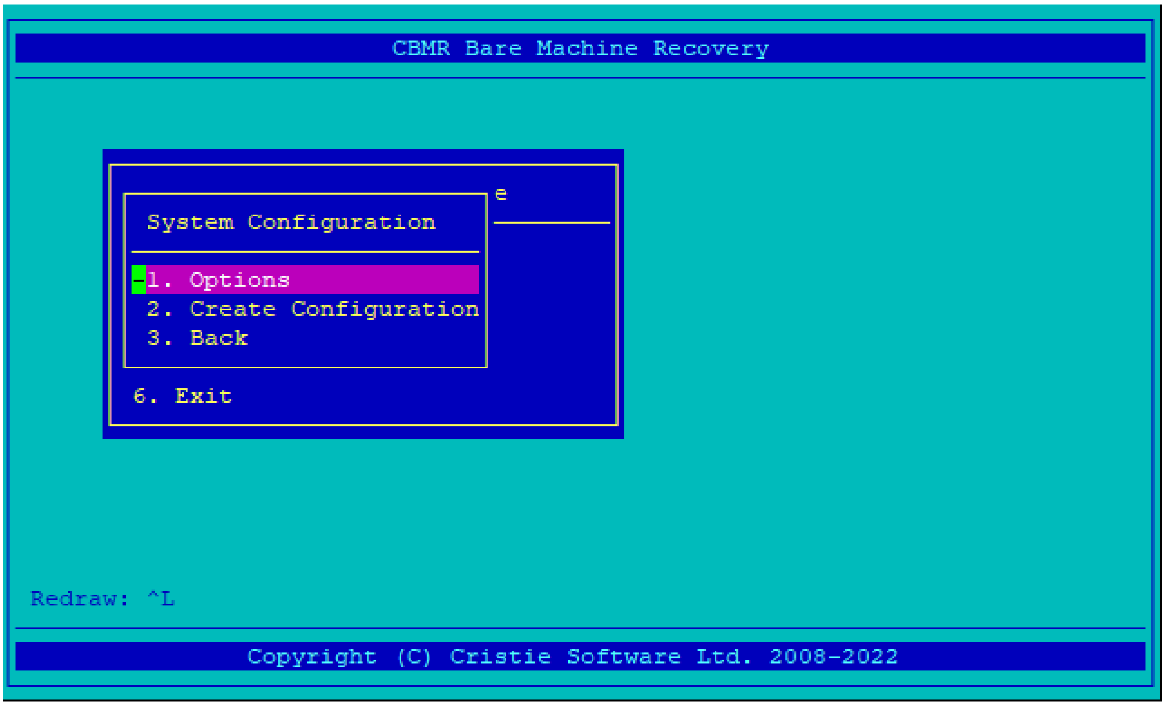
2. **Perform** the system backup using a VTD or IBM Spectrum Protect node backup location.

The system information is recorded to allow the recovery environment to recreate the original system environment. This includes drive and file-system information, as well as information about essential packages for rebuilding the system (for example, to provide file encryption at recovery time).

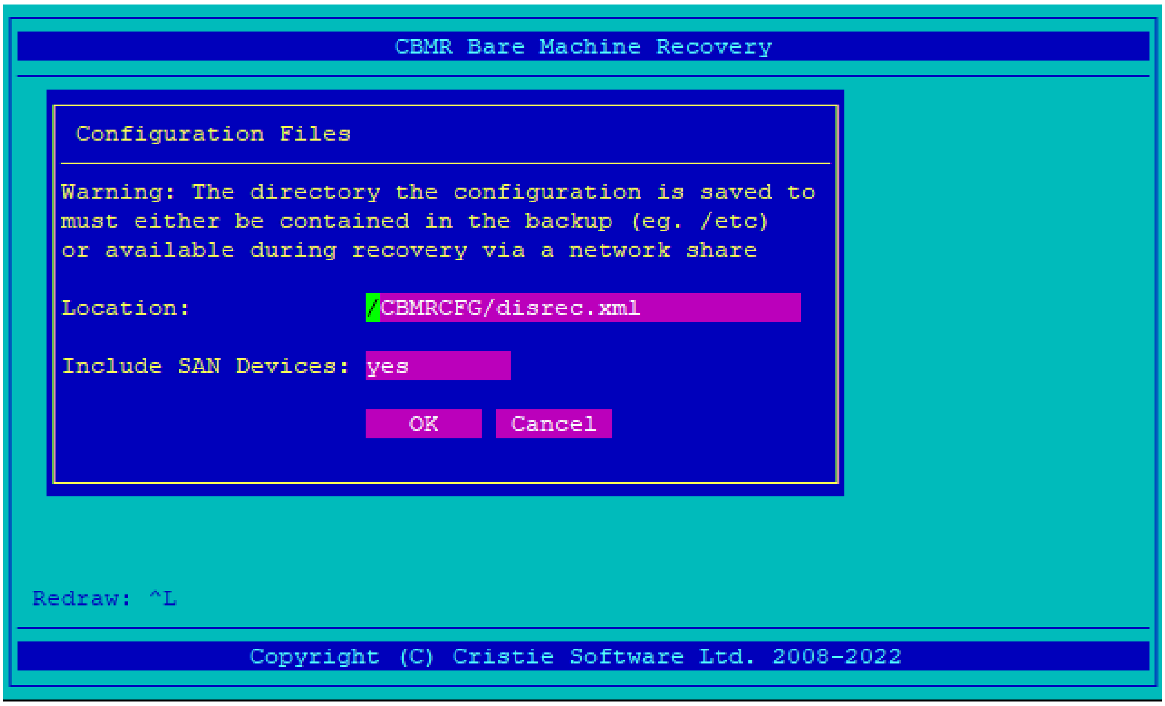
8.1 Recording System Information

The system information must be recorded and stored so that the system can be rebuilt at recovery time. This is performed using the `cbmrcfg` tool, available through the **System Configuration** option of the Graphical User Interface.

Selecting **System Configuration** from the main menu opens a sub-menu containing options for creating the configuration:


```
CBMR Bare Machine Recovery

                                   e
   System Configuration
   1. Options
   2. Create Configuration
   3. Back

  6. Exit

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

The **Options** menu item allows a choice of where to create the configuration file and to include/exclude any SAN devices attached to the host



```
CBMR Bare Machine Recovery

Configuration Files

Warning: The directory the configuration is saved to
must either be contained in the backup (eg. /etc)
or available during recovery via a network share

Location:            /CBMRCFG/disrec.xml

Include SAN Devices: yes

                     OK    Cancel

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

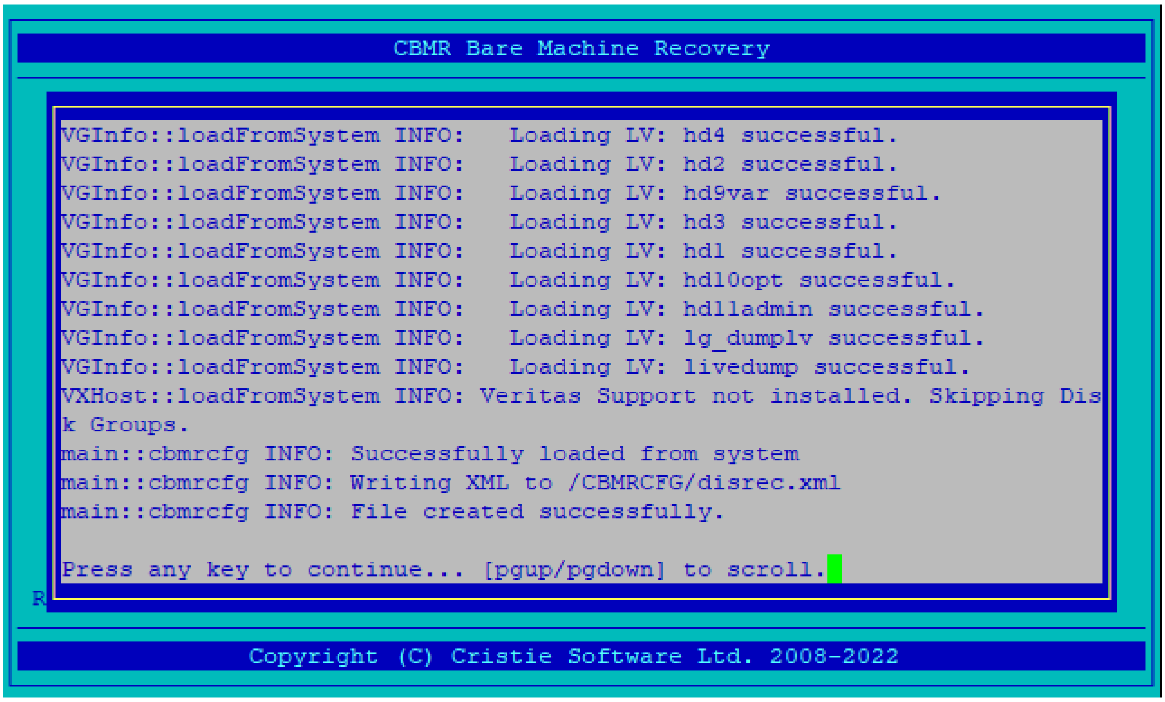
Location

The default location for the configuration file is `/CBMRCFG/disrec.xml`. Cristie recommends leaving the location at this default value.

Include SAN Devices: Yes/No.

If this option is set to **Yes** then all disks (including SAN attached disks) are parsed for inclusion in the configuration files. Only set this options to **No** if you are certain that no volumes that you wish to recover are on SAN.

When running the configuration tool information, the current operations are displayed:

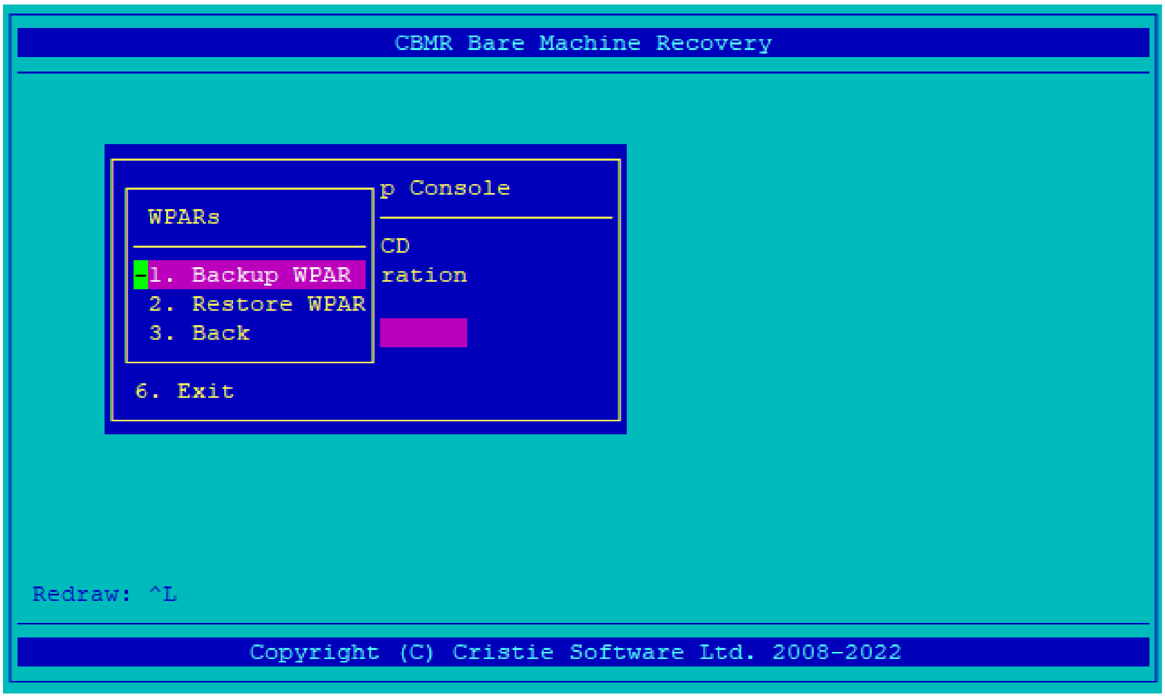

CBMR Bare Machine Recovery
Copyright (C) Cristie Software Ltd. 2008-2022

```
VGInfo::loadFromSystem INFO:   Loading LV: hd4 successful.
VGInfo::loadFromSystem INFO:   Loading LV: hd2 successful.
VGInfo::loadFromSystem INFO:   Loading LV: hd9var successful.
VGInfo::loadFromSystem INFO:   Loading LV: hd3 successful.
VGInfo::loadFromSystem INFO:   Loading LV: hd1 successful.
VGInfo::loadFromSystem INFO:   Loading LV: hd10opt successful.
VGInfo::loadFromSystem INFO:   Loading LV: hd11admin successful.
VGInfo::loadFromSystem INFO:   Loading LV: lg_dumplv successful.
VGInfo::loadFromSystem INFO:   Loading LV: livedump successful.
VXHost::loadFromSystem INFO: Veritas Support not installed. Skipping Dis
k Groups.
main::cbmrcfg INFO: Successfully loaded from system
main::cbmrcfg INFO: Writing XML to /CBMRCFG/disrec.xml
main::cbmrcfg INFO: File created successfully.

Press any key to continue... [pgup/pgdown] to scroll.
```

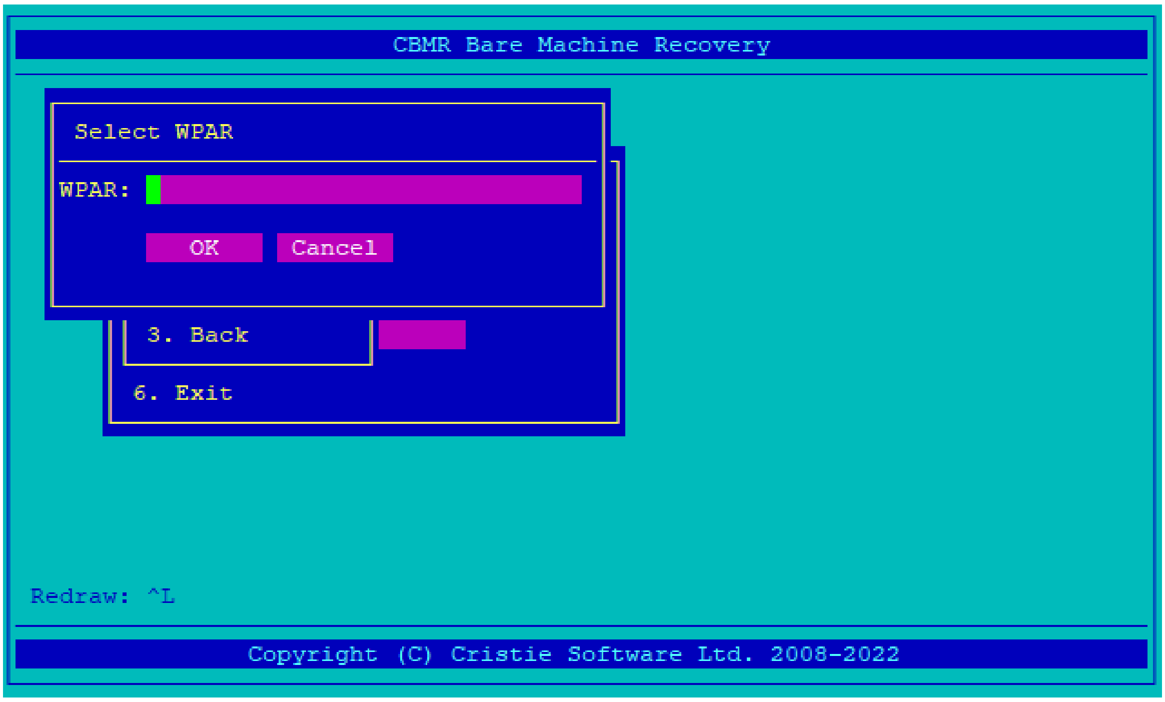
Once this operation is complete, the log fine can be found in `/var/log/cristie/cbmrcfg.log`. This may also be viewed using the **Log Files** submenu.

8.2 WPARs

It is also possible to backup and restore individual WPARs using the CBMR GUI.



Selecting **Backup** or **Restore** presents a list of WPARs that may be recovered.



```
CBMR Bare Machine Recovery

Select WPAR

WPAR:

OK   Cancel

3. Back

6. Exit

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

8.3 Configure the Backup Location

A **Backup Location** is a definition of the entity to which you backup data. CBMR can backup to tape drives, tape libraries, files as a virtual tape drive (VTD), IBM Spectrum Protect nodes and cascaded locations.

All backup functionality may be accessed via the **Backup** option from the main menu. This provides functionality to change the location of the backup (ie. file (VTD), tape, IBM Spectrum Protect server), change the selection of file to backup and perform the backup. However, it is also possible to create definitions using a text editor.

When performing a VTD backup with CBMR it can fail with "**couldn't write buffer: SMERR_PHYSICAL_END_OF_MEDIA**"

This can be remedied by modifying /etc/security/limits and setting:-

```
fsize = -1
```

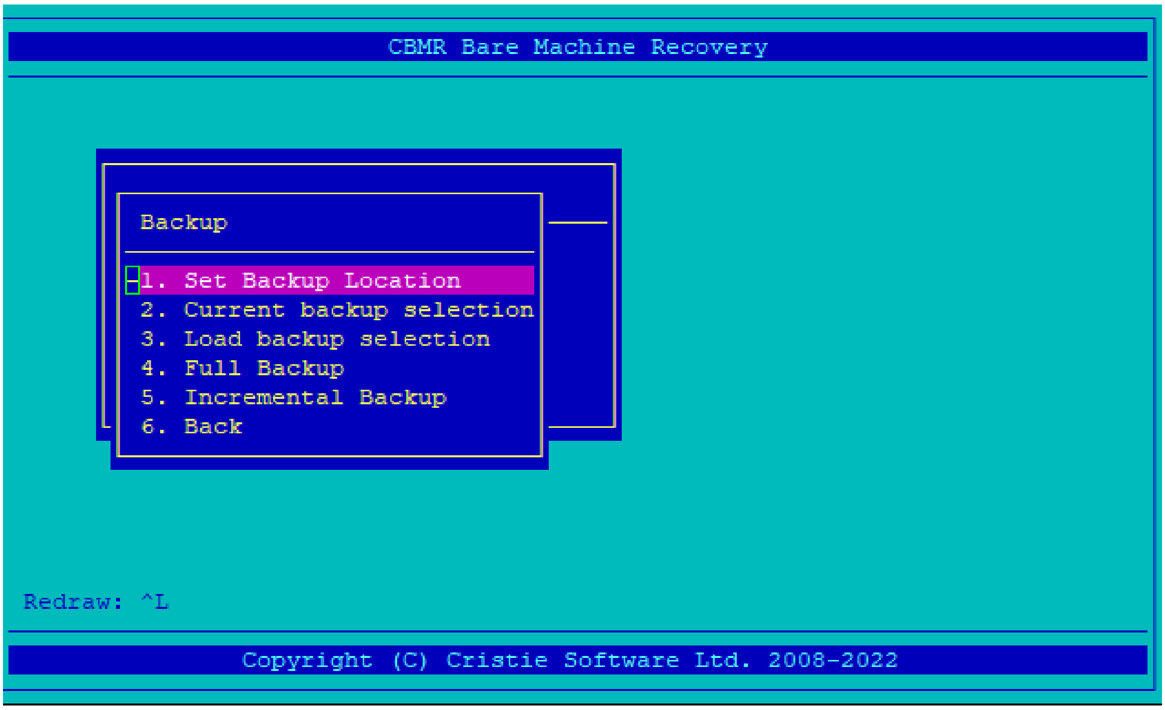
Another cause of this error is a low value of `ulimit`. Change it like this:

```
ulimit -f 16000000
```

Note: a backup location MUST be configured before starting a DR backup

8.3.1 Configuring a Backup Location using the Graphical User Interface

The **Graphical User Interface**, GUBAX, can be accessed either by selecting **Set Backup Location** from the CBMR tool or by running gubax at the command prompt.

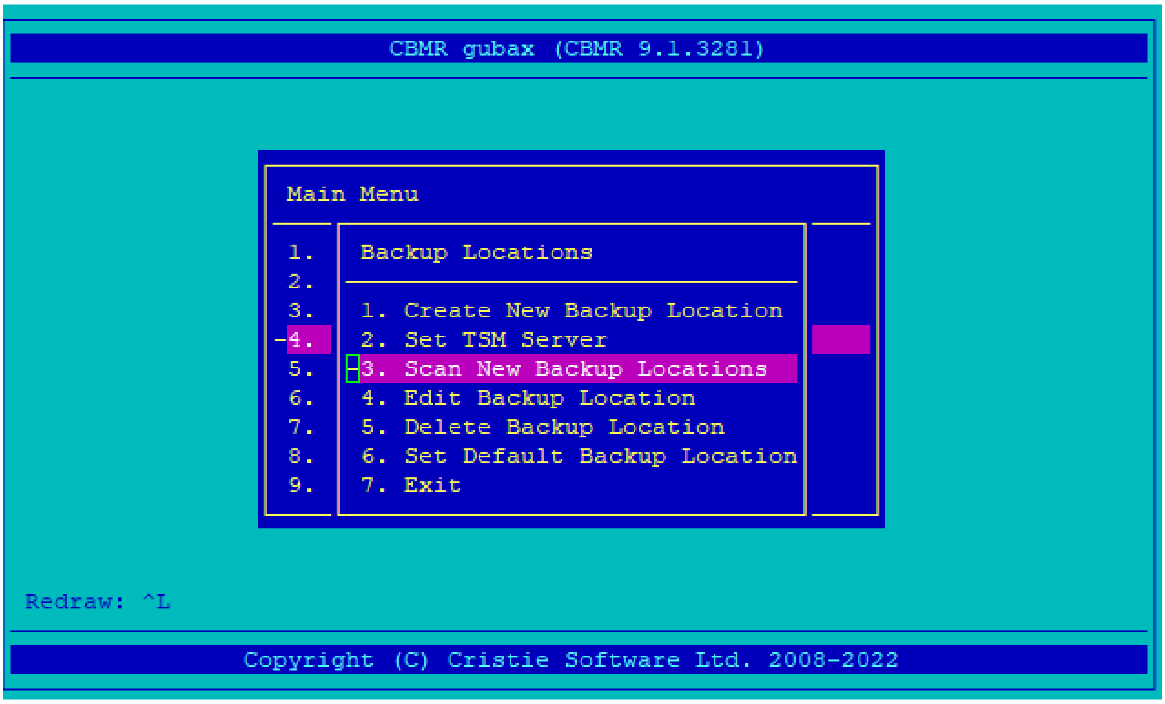


```
CBMR Bare Machine Recovery

Backup

1. Set Backup Location
2. Current backup selection
3. Load backup selection
4. Full Backup
5. Incremental Backup
6. Back

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

The GUBAX menu provides the ability to create, modify and delete file (VTD), tape and IBM Spectrum Protect backup locations.

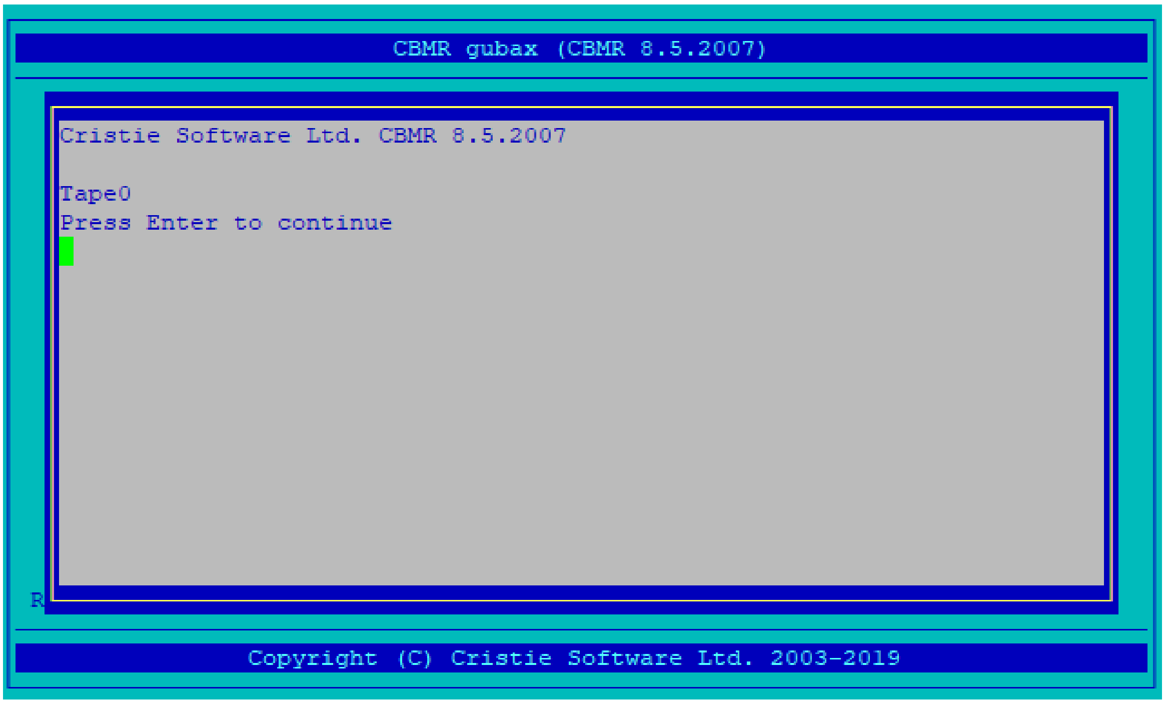
Tape Drives

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.



```
CBMR gubax (CBMR 9.1.3281)

Main Menu

1.   Backup Locations
2.
3.   1. Create New Backup Location
4.   2. Set TSM 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. 2008-2022
```

Any new devices found are listed and are then be available to choose as the default device. In the following example, the new Backup Location is named `Tape0`:



```
CBMR gubax (CBMR 8.5.2007)

Cristie Software Ltd. CBMR 8.5.2007

Tape0
Press Enter to continue

Copyright (C) Cristie Software Ltd. 2003-2019
```

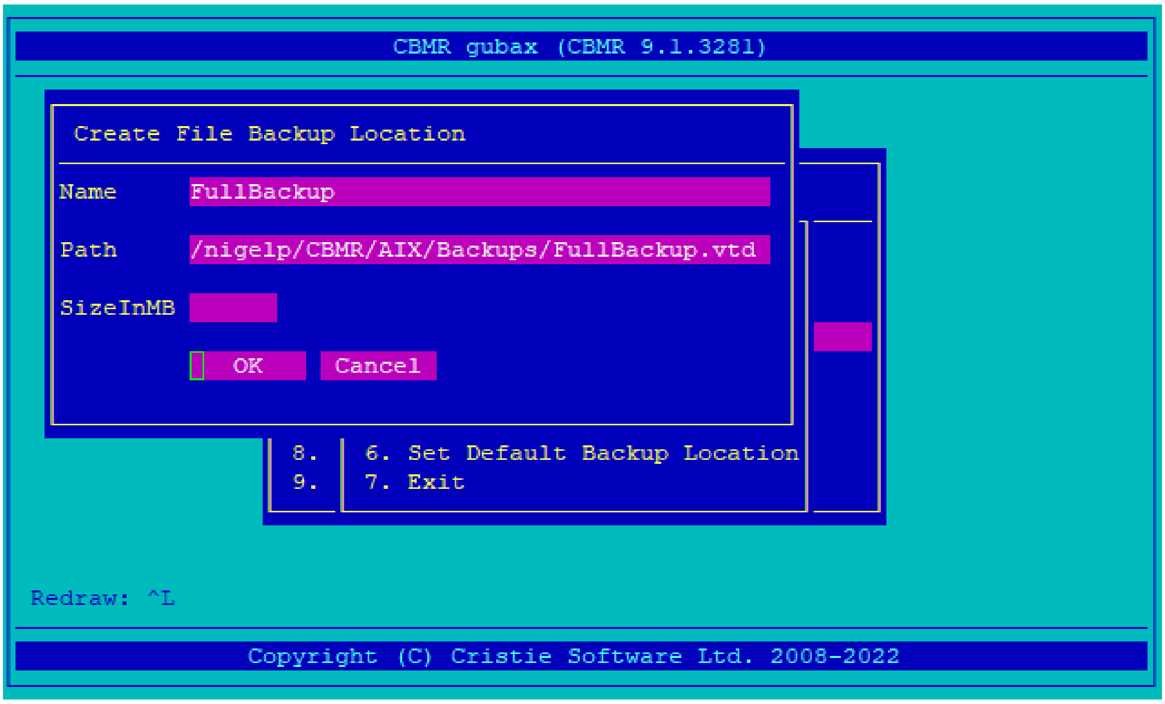
Other types of device should be configured manually by selecting **Create New Backup Location** from the device menu.

The menu presented allows creation of File (VTD), IBM Spectrum Protect, Tape Library and cascaded devices.

File Backup Locations

A File (VTD) backup Location is a file that is formatted like a tape. If you wish to backup to a file, usually located on a network share, choose **File Backup Location** from the Backup Location Type menu:

The Path,which is case sensitive, specifies the full path to the VTD file.

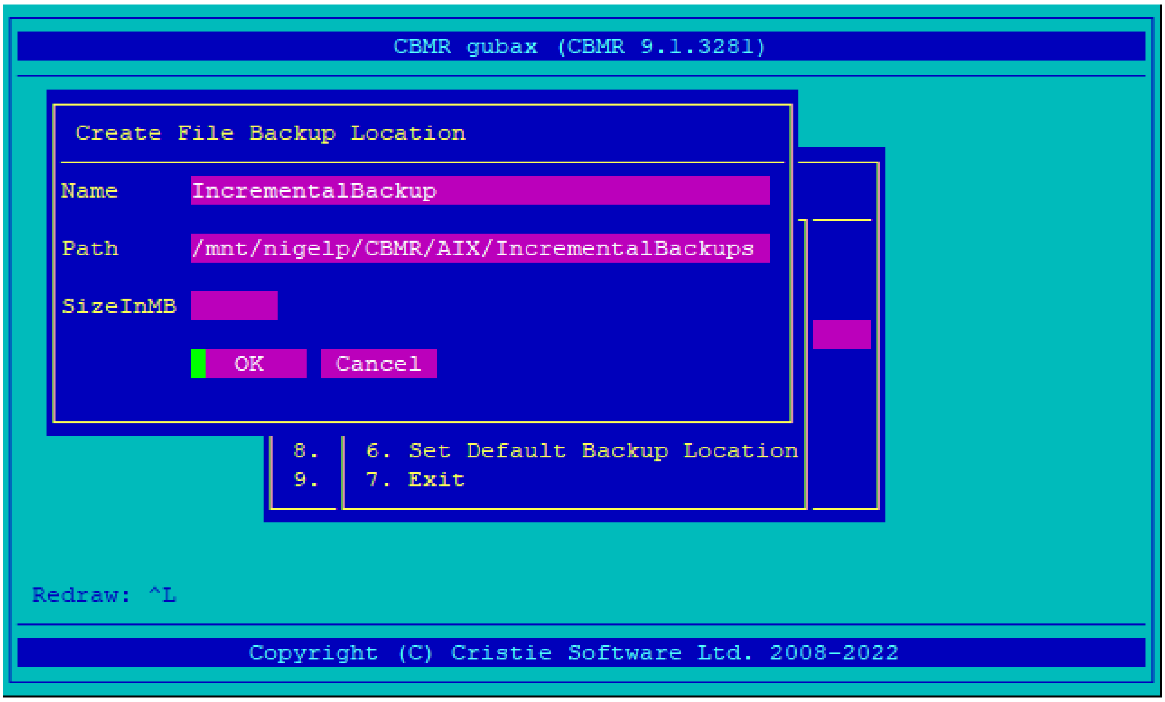


```
CBMR gubax (CBMR 9.1.3281)

Create File Backup Location

Name      FullBackup
Path      /nigelp/CBMR/AIX/Backups/FullBackup.vtd
SizeInMB
          OK   Cancel

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

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

It is recommended that you leave the **SizeInMB** field blank or set to zero. **SizeInMB** sets a maximum size for the file - by leaving this blank it allows it to expand until the backup is complete or there is no more space on the disk.

Incremental File Backup Locations

An Incremental File backup Location is a folder that contains a series of incremental backups. This uses 'forward incremental' backup algorithms to allow recoveries to be made to a specific point-in-time. To create an incremental backup location, usually located on a network share, first choose **File Backup Location** from the Backup Location Type menu:



```
CBMR gubax (CBMR 9.1.3281)

Create File Backup Location

Name      IncrementalBackup
Path      /mnt/nigelp/CBMR/AIX/IncrementalBackups
SizeInMB
          OK   Cancel

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

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

The Path, which is case sensitive, specifies the full path to the **directory** used to contain the incremental backups. Leave the **SizeInMB** field blank when specifying an incremental backup location directory path.

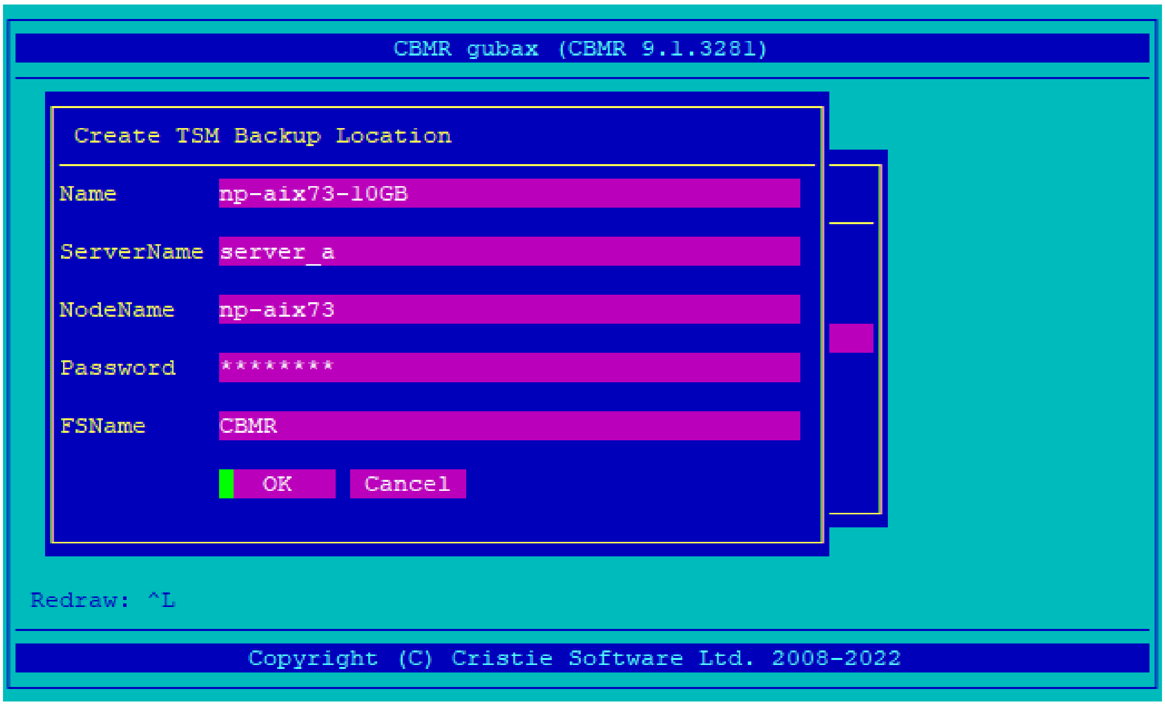
IBM Spectrum Protect Backup Location

A IBM Spectrum Protect node is a port to a network storage system. Currently, 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.

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 following 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 server, choose **IBM Spectrum Protect Backup Location** from the Backup Location Type menu. Complete the form presented with values that apply to your environment. The following form is an example only:



CBMR gubax (CBMR 9.1.3281)

Create TSM Backup Location

Name np-aix73-10GB

ServerName server_a

NodeName np-aix73

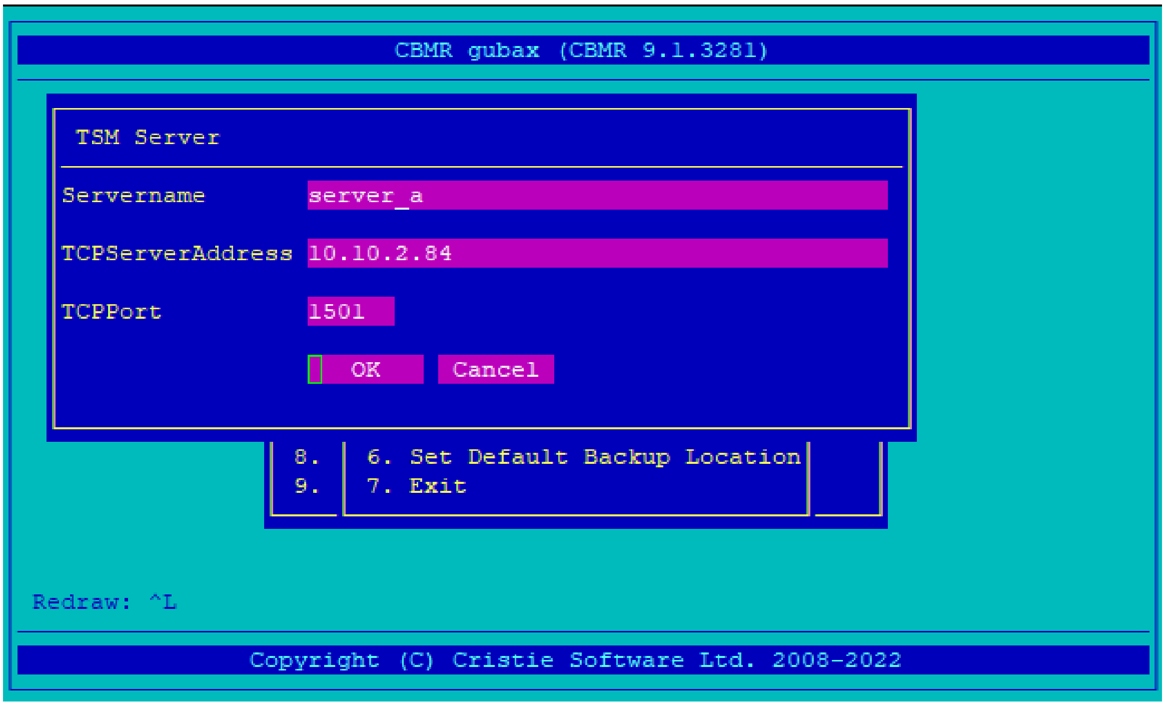
Password ********

FSName CBMR

Copyright (C) Cristie Software Ltd. 2008-2022

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

For a IBM Spectrum Protect Backup Location, you also need to provide connection information for the IBM Spectrum Protect Server. This may be performed by selecting **Set IBM Spectrum Protect Server** from the menu.



```
                    CBMR gubax (CBMR 9.1.3281)

   TSM Server

  Servername        server_a
  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. 2008-2022
```

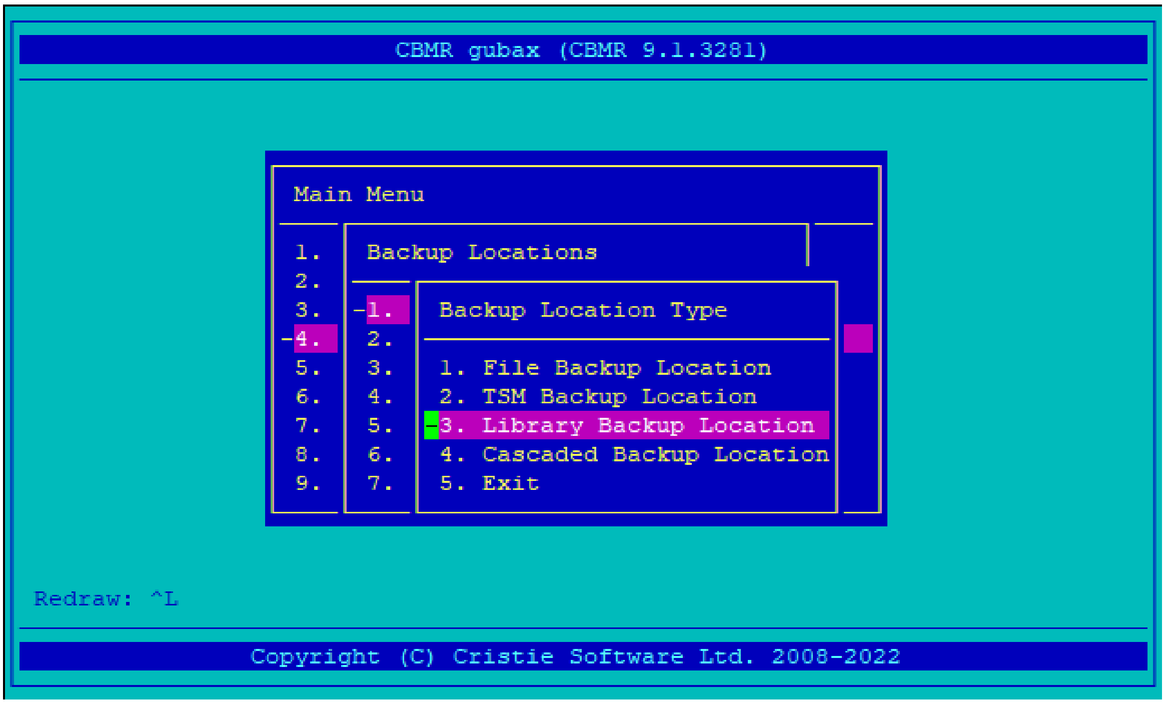
The data is specified in the `dsm.sys` file. If you have already created the file, you may skip this step. If you do use this function, it overwrites any existing `dsm.sys` file. The file is created in the directory configured by the `DSMI_DIR` environment variable, usually `/usr/tivoli/tsm/client/api/bin/`.

The displayed form allows you to specify the basic parameters for connecting to the IBM Spectrum Protect server over TCP/IP. Ensure that you use the same server name as you used on the IBM Spectrum Protect Backup Location form.

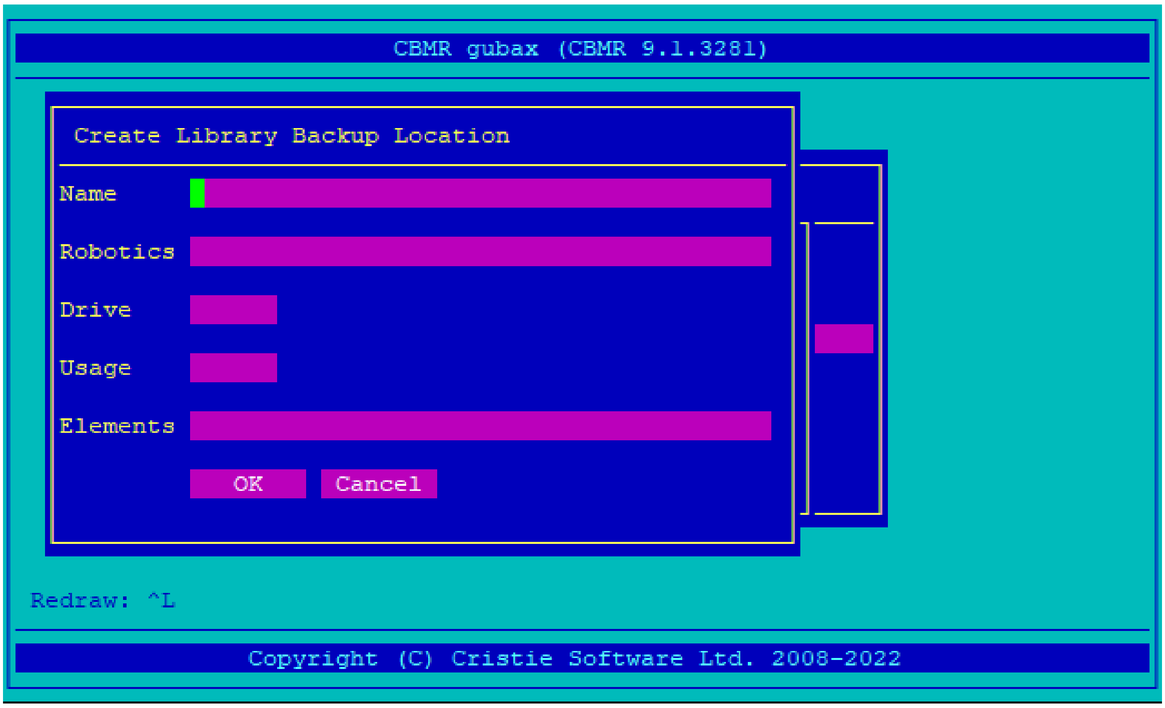
> ***Note: For server versions later than 8.1.12 you may need to configure SSL access to the server using an appropriate server certificate. Use*** `dsmcert` ***manually to do this prior to running the backup.***

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.



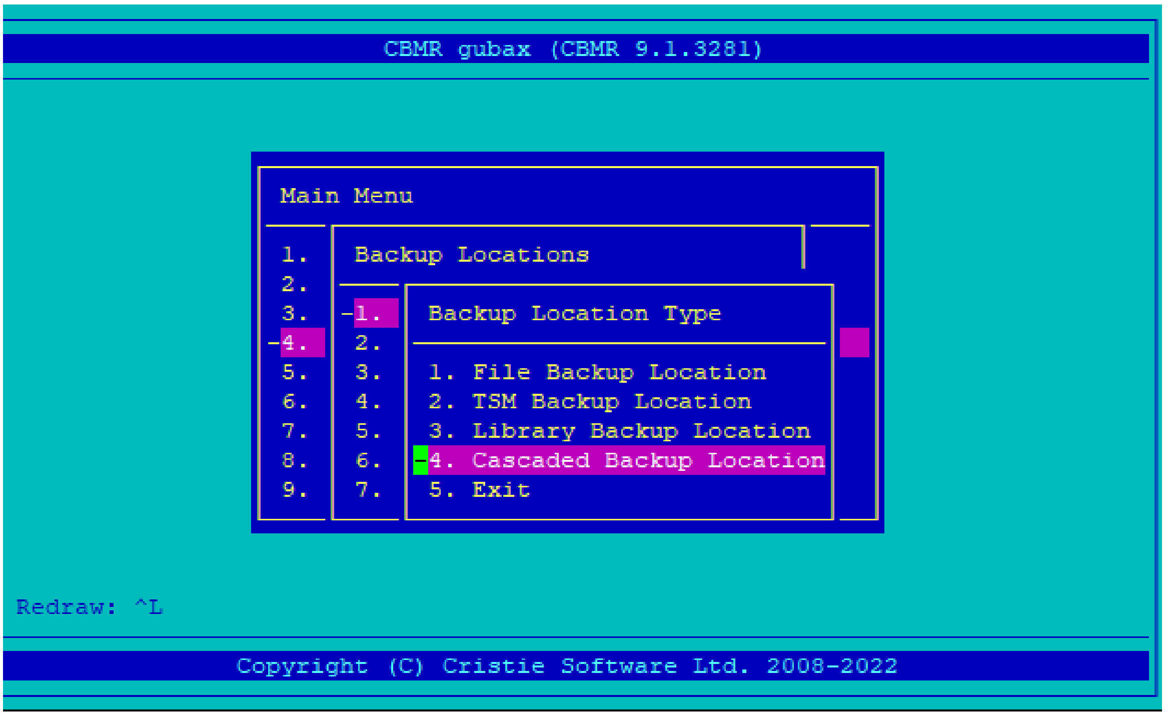
```
CBMR gubax (CBMR 9.1.3281)

Main Menu

1.   Backup Locations
2.
3.  -1.  Backup Location Type
-4.  2.
5.   3.  1. File Backup Location
6.   4.  2. TSM 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. 2008-2022
```



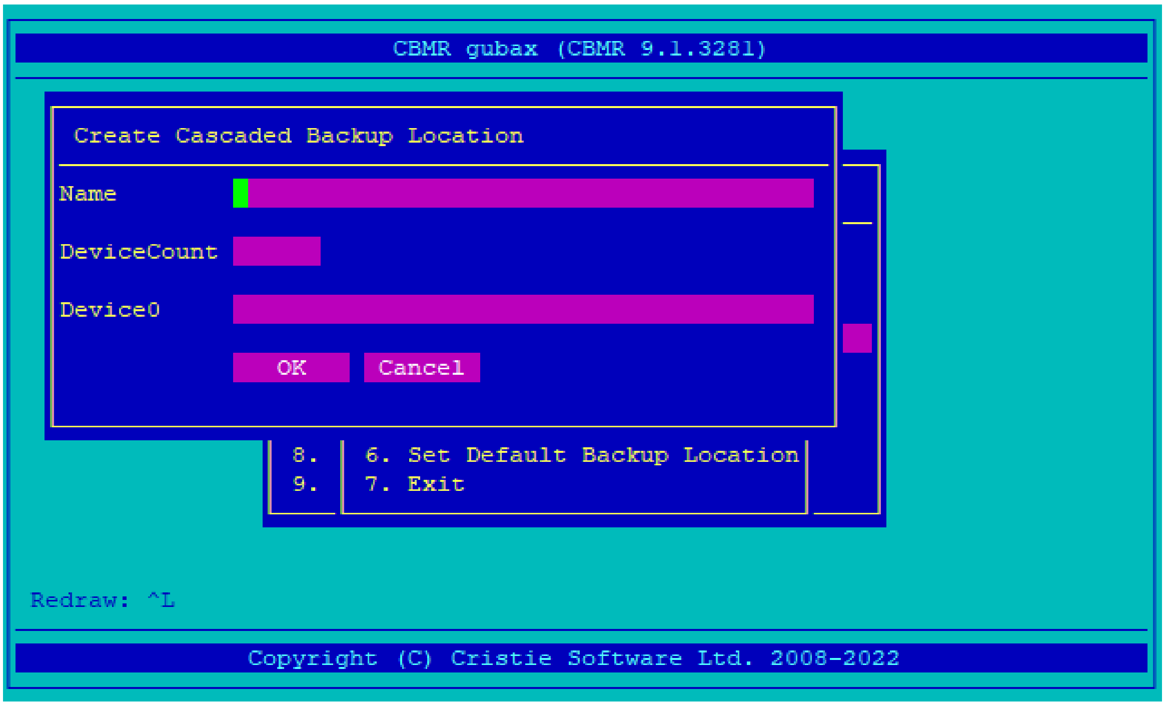
```
CBMR gubax (CBMR 9.1.3281)

Create Library Backup Location

Name
Robotics
Drive
Usage
Elements

         OK     Cancel

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

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.



```
                    CBMR gubax (CBMR 9.1.3281)

          Main Menu

          1.   Backup Locations
          2.
          3.  -1.   Backup Location Type
         -4.   2.
          5.   3.   1. File Backup Location
          6.   4.   2. TSM 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. 2008-2022
```



```
                    CBMR gubax (CBMR 9.1.3281)

   Create Cascaded Backup Location

  Name

  DeviceCount

  Device0

                OK       Cancel

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

Redraw: ^L

              Copyright (C) Cristie Software Ltd. 2008-2022
```

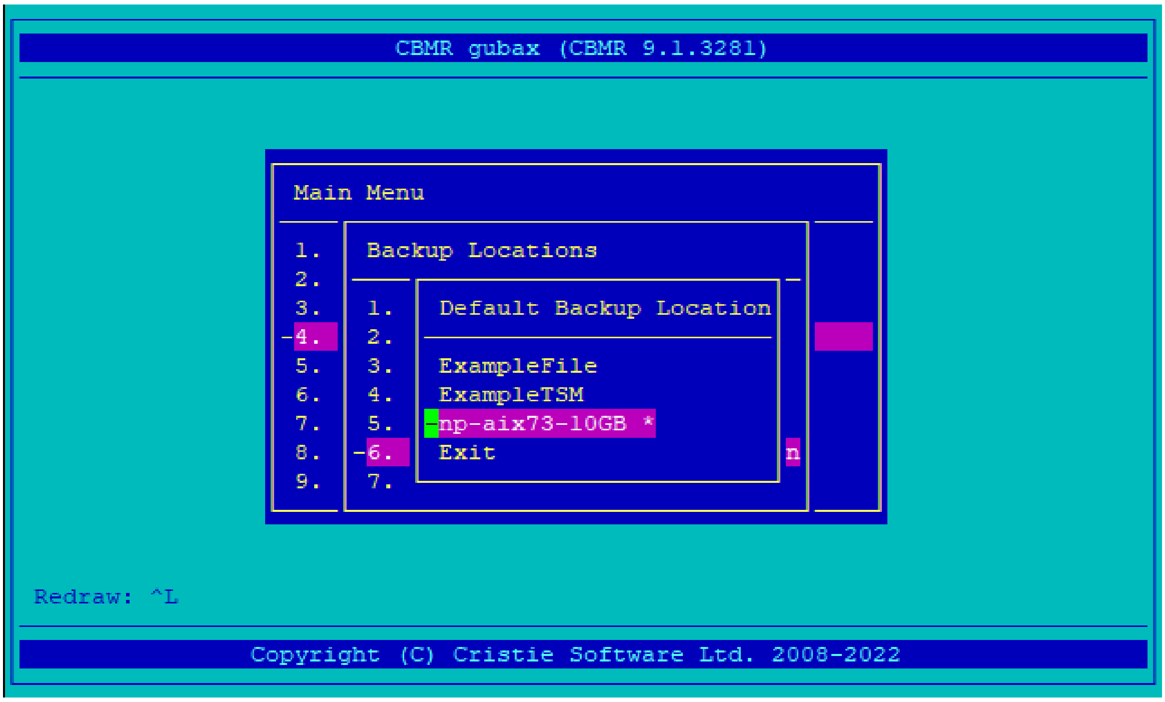
Typically, you could use this on tape drives or virtual tape drives. In order to create a Cascaded Backup Location, you need first to create individual backup locations that you can then cascade.

> *Note: this type of backup location is not particularly useful in a CBMR context where speed of recovery is important*

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. 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. You may check that the selection has taken effect by selecting the Set Default Backup Location menu again.



```
                    CBMR gubax (CBMR 9.1.3281)

            Main Menu

             1.  Backup Locations
             2.
             3.   1.  Default Backup Location
            -4.   2.
             5.   3.  ExampleFile
             6.   4.  ExampleTSM
             7.   5. -np-aix73-10GB *
             8.  -6.  Exit                    n
             9.   7.

 Redraw: ^L

           Copyright (C) Cristie Software Ltd. 2008-2022
```

8.3.2 Configuring a Backup Location using the 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 and File Backup Locations can be handled in this way. The `devices.ini` file which is located in `/etc/cristie` could be amended or created with entries such as the following:

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

If you wish to know more about these file formats, the UBAX main page - type `man ubax` - has more detailed information.

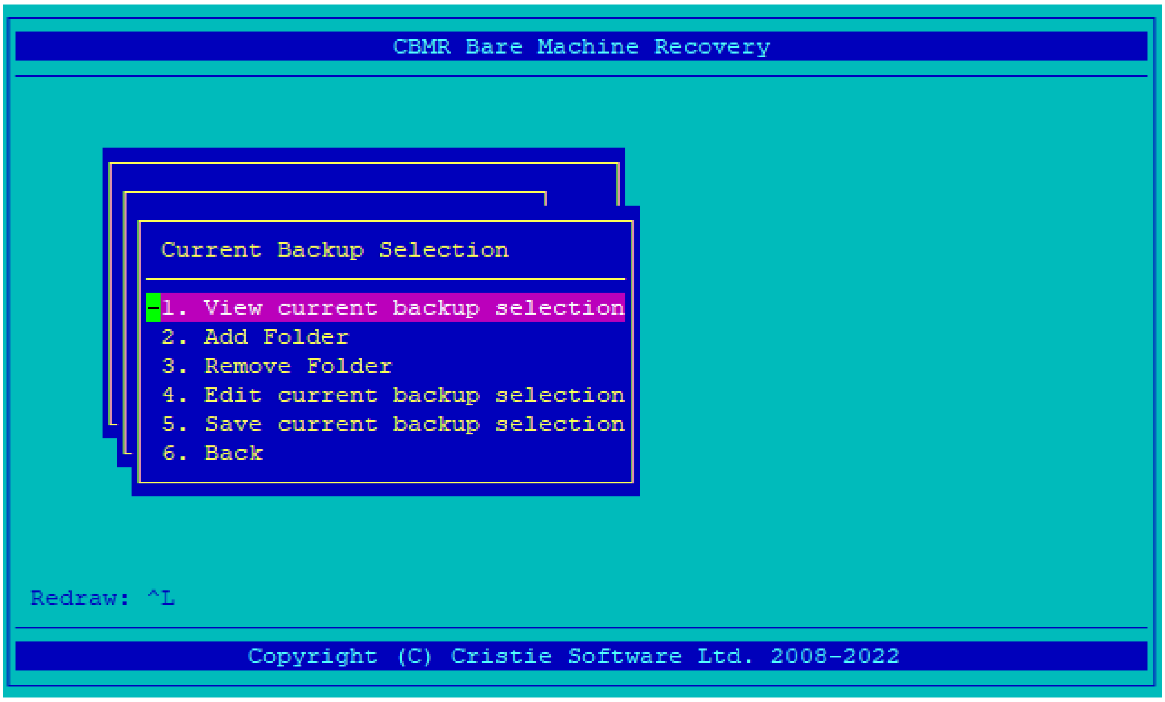
However, it is not recommended that this be done with an editor. Backup Locations are best defined using the GUI.

8.3.3 Select the Directories to be backed up

The selection of directories to be backed up is called a 'Backup Selection'. Each backup selection is stored in a backup script in the folder `/etc/cristie/scripts/`, with the default being `cbmr.scp`. On the first run of CBMR for AIX, all **mounted** volumes will be selected for backup.

8.3.3.1 Viewing the current backup selection

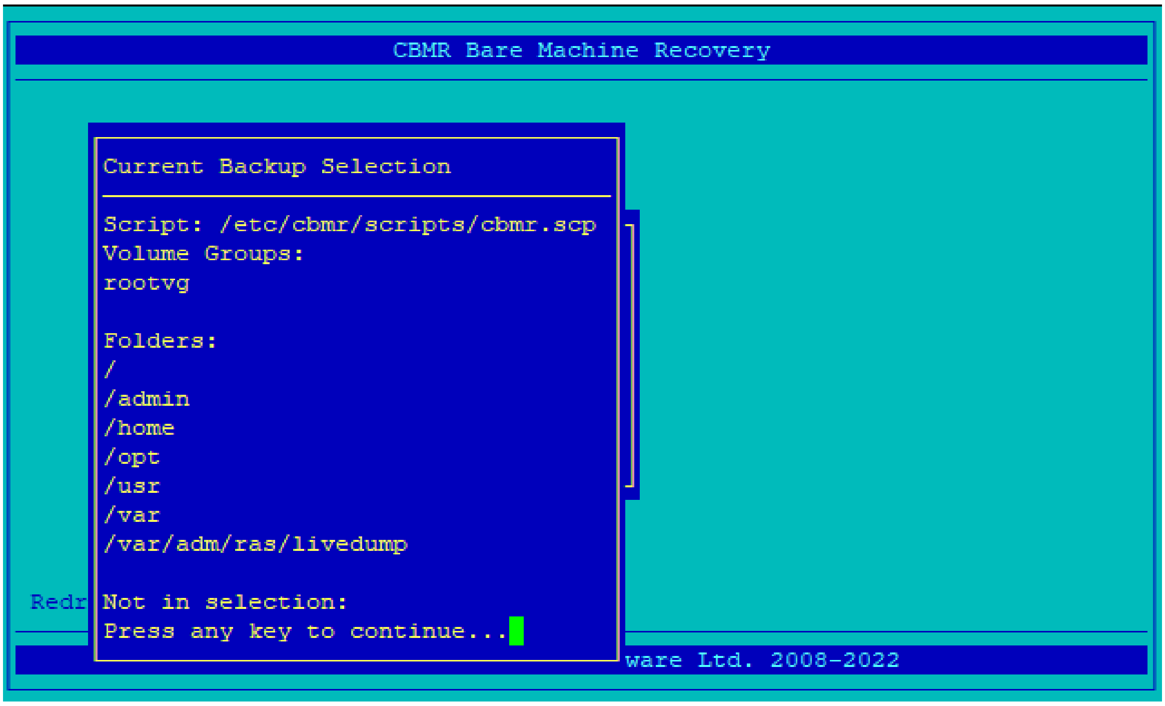
The current backup selection can be viewed and modified via the **View current backup selection** menu, accessed via the Backup Menu.



```
CBMR Bare Machine Recovery

Current Backup Selection

1. View current backup selection
2. Add Folder
3. Remove Folder
4. Edit current backup selection
5. Save current backup selection
6. Back

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

This will display the following information:

- **Script**:- the location of the script file
- **Volume Groups** - the volume that the data spans
- **Directories** - the directories that will be backed up

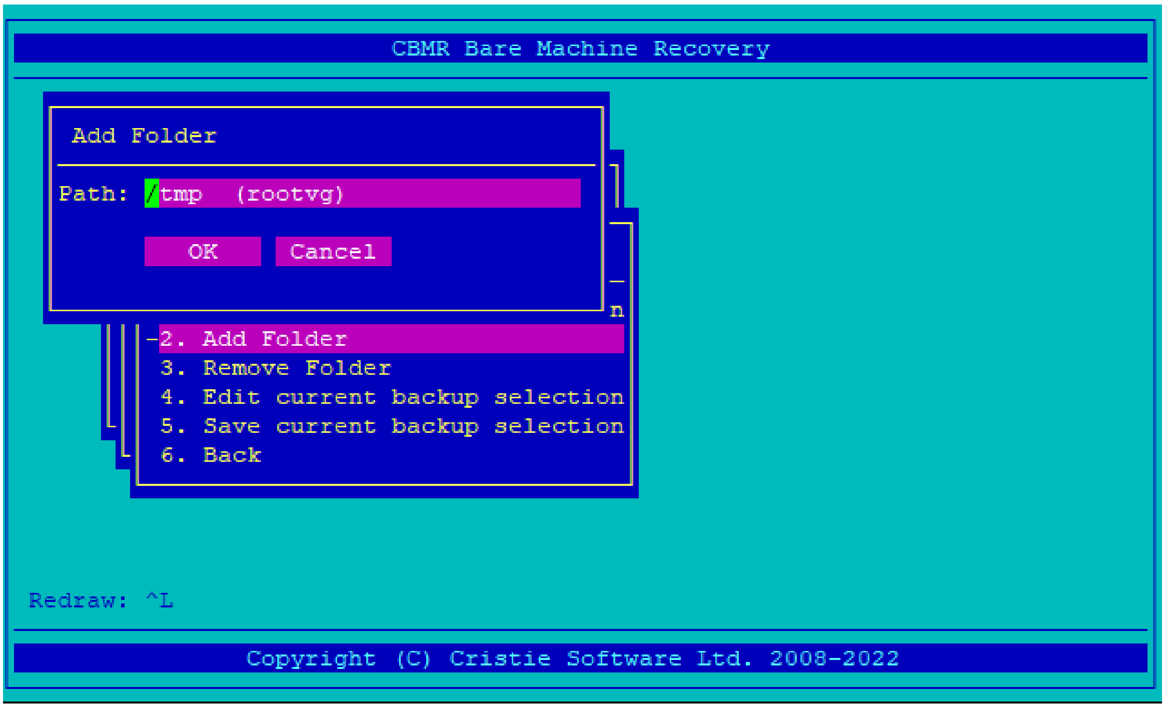


```
                        CBMR Bare Machine Recovery

        Current Backup Selection
        ────────────────────────────────────
        Script: /etc/cbmr/scripts/cbmr.scp
        Volume Groups:
        rootvg

        Folders:
        /
        /admin
        /home
        /opt
        /usr
        /var
        /var/adm/ras/livedump

  Redr  Not in selection:
        Press any key to continue...
                                          ware Ltd. 2008-2022
```

8.3.3.2 Editing the current backup selection

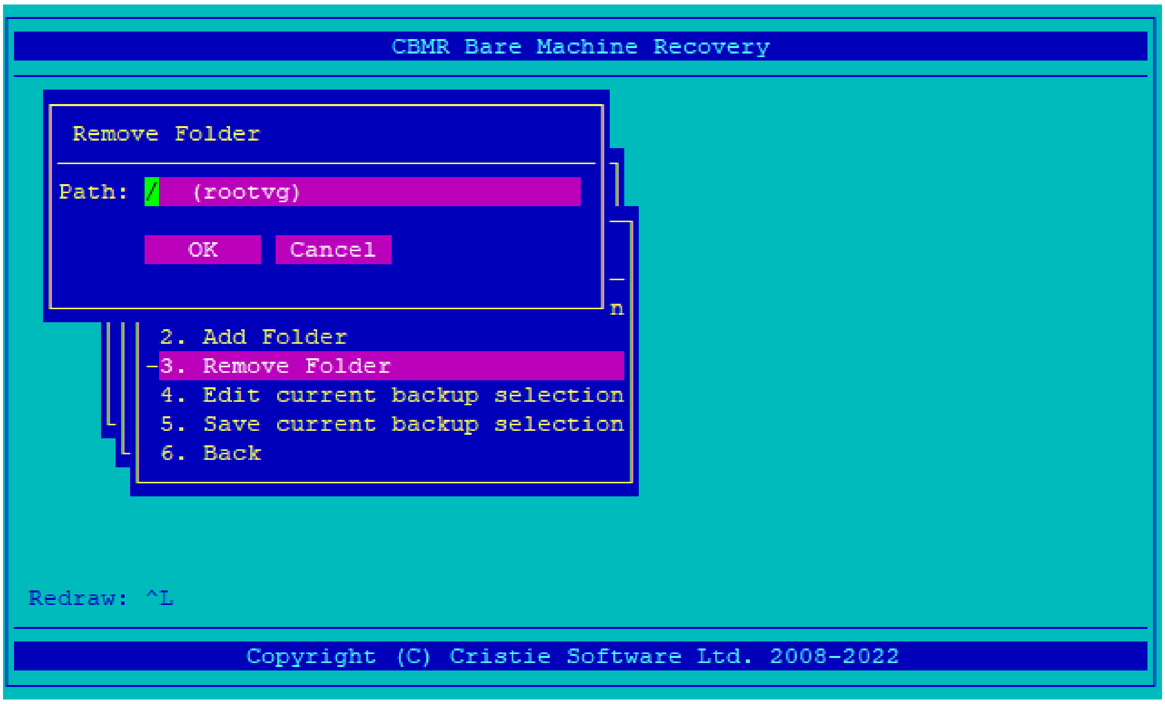
The current backup selection can be edited either by adding or removing directories using the Graphical User Interface or by directly editing the file itself. In the latter case, the main page for UBAX describes the format of the files in detail.

The directories listed in the selection are the mount-points of local file-systems on the system, or directories included explicitly in the current script.



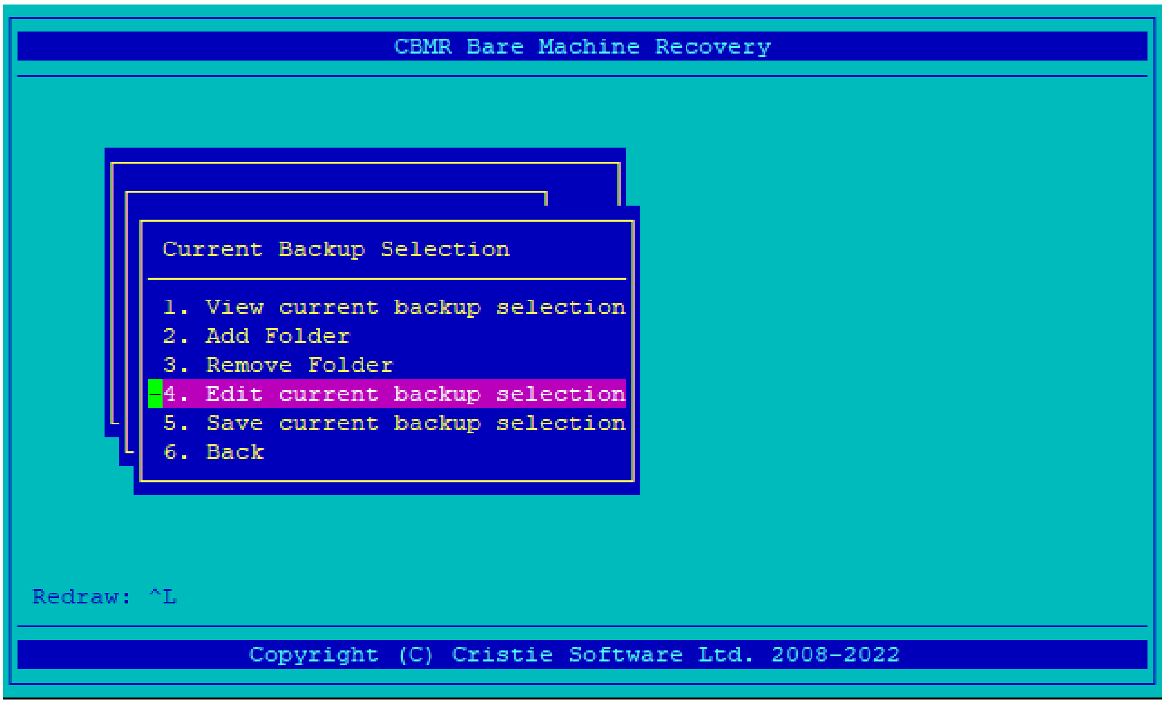
```
                        CBMR Bare Machine Recovery

     Add Folder
    ─────────────────────────────────────
    Path: /tmp  (rootvg)

          OK     Cancel

              2. Add Folder
              3. Remove Folder
              4. Edit current backup selection
              5. Save current backup selection
              6. Back

  Redraw: ^L

              Copyright (C) Cristie Software Ltd. 2008-2022
```

Each directory to be added or removed will have the volume group it resides on in brackets. If all directories for a given Volume Group are removed using Remove Folder, then it will not be necessary (but still possible) to recreate the volume group at recovery time.

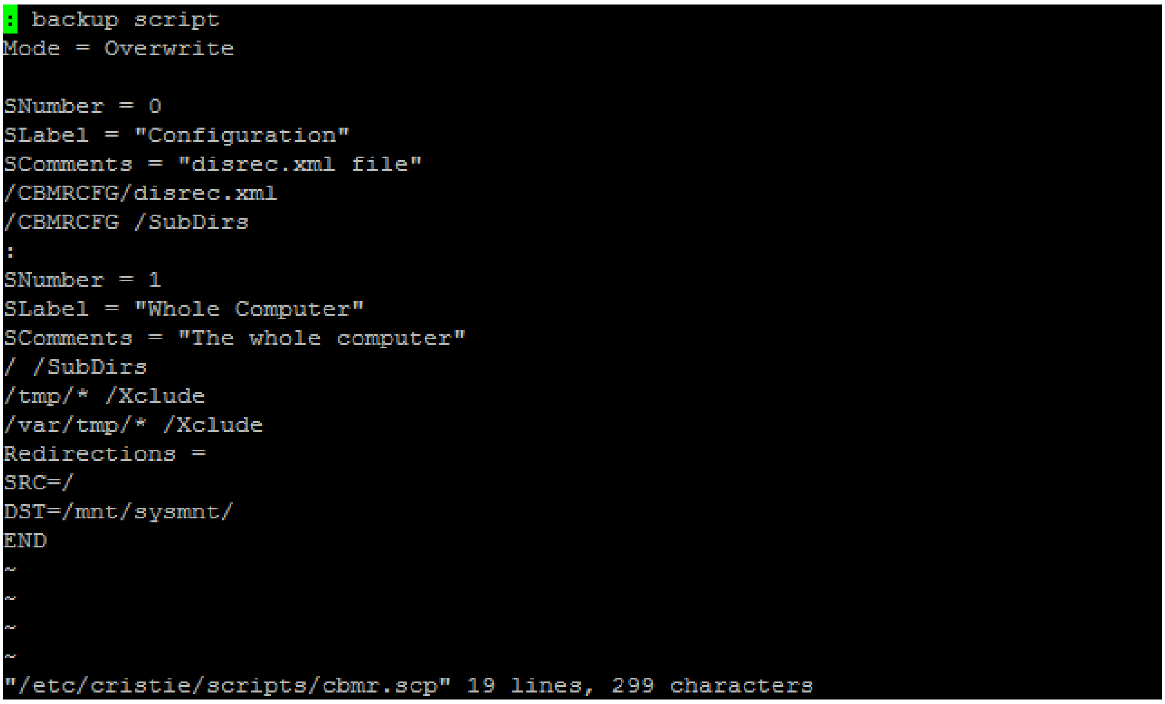


```
CBMR Bare Machine Recovery

Remove Folder

Path: /  (rootvg)

OK    Cancel

2. Add Folder
3. Remove Folder
4. Edit current backup selection
5. Save current backup selection
6. Back

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

The script file can be edited directly either be navigating to /etc/cristie/scripts or selecting **edit current backup selection**.



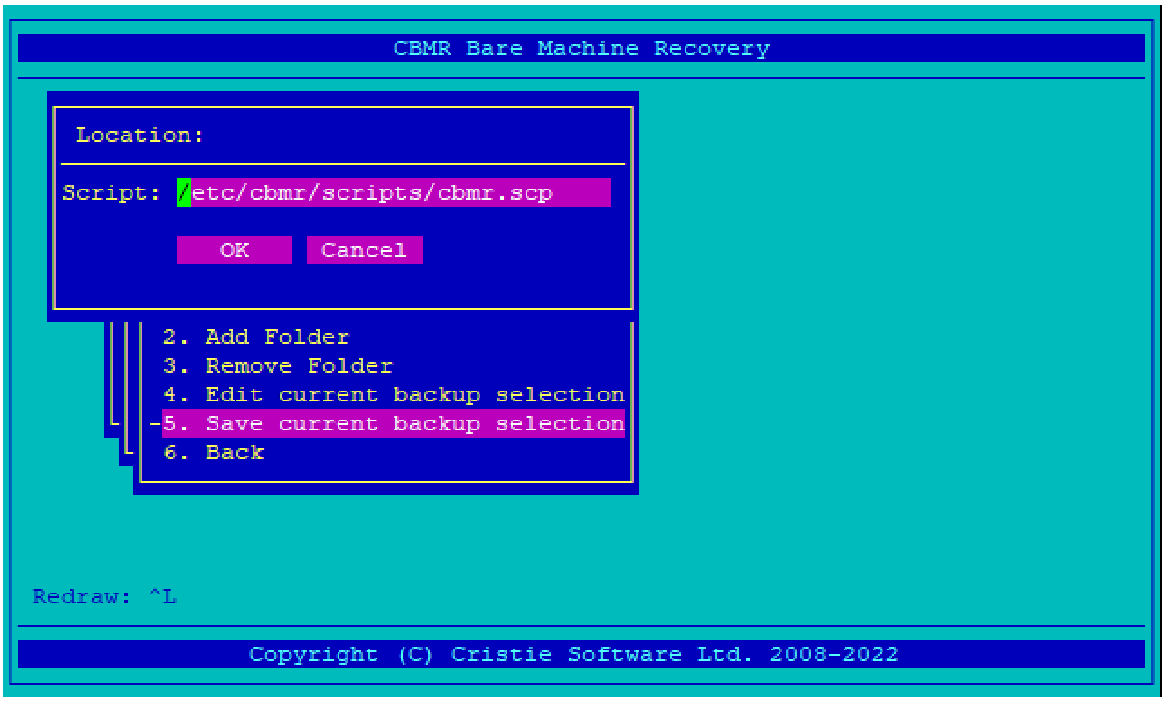
```
CBMR Bare Machine Recovery

Current Backup Selection

1. View current backup selection
2. Add Folder
3. Remove Folder
4. Edit current backup selection
5. Save current backup selection
6. Back

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```



```
: backup script
Mode = Overwrite

SNumber = 0
SLabel = "Configuration"
SComments = "disrec.xml file"
/CBMRCFG/disrec.xml
/CBMRCFG /SubDirs
:
SNumber = 1
SLabel = "Whole Computer"
SComments = "The whole computer"
/ /SubDirs
/tmp/* /Xclude
/var/tmp/* /Xclude
Redirections =
SRC=/
DST=/mnt/sysmnt/
END
~
~
~
~
"/etc/cristie/scripts/cbmr.scp" 19 lines, 299 characters
```

8.3.3.3 Saving the current backup selection

The backup selection must be saved before the backup is performed. To do this, select **Save current backup selection** from the Current Backup Selection menu.


CBMR Bare Machine Recovery
Location:
OK
Cancel
2. Add Folder
3. Remove Folder
4. Edit current backup selection
5. Save current backup selection
6. Back
Redraw: ^L

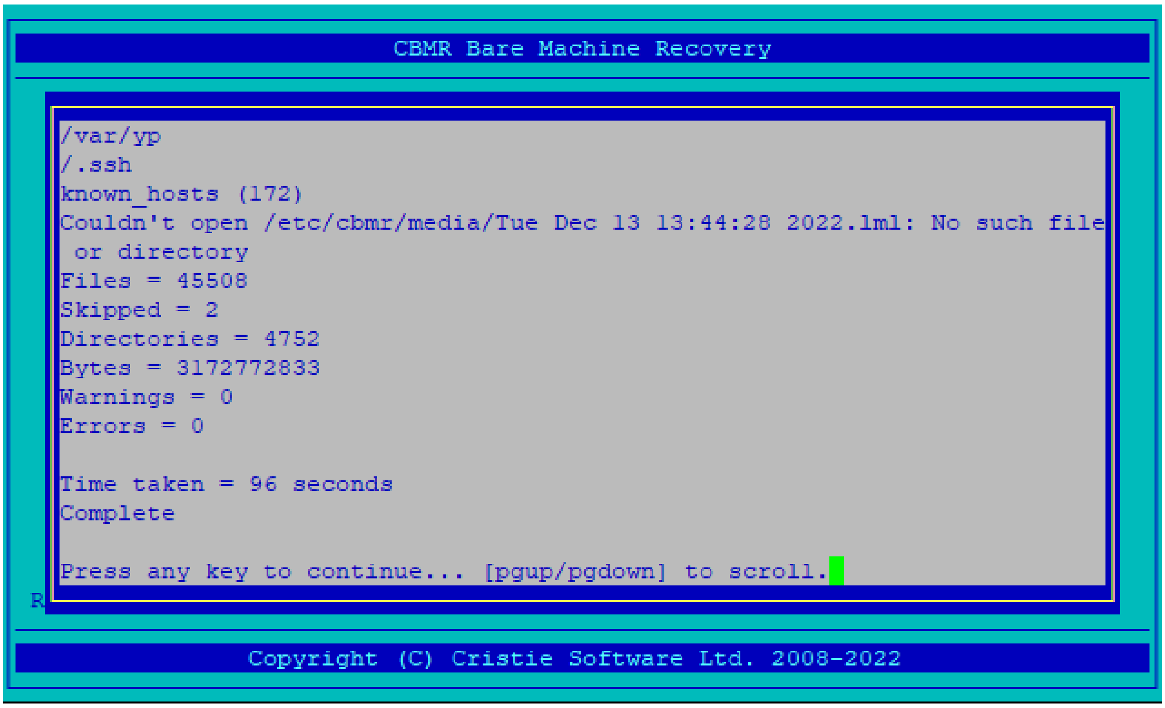
Script: /etc/cbmr/scripts/cbmr.scp

Copyright (C) Cristie Software Ltd. 2008-2022

8.4 Performing the backup

A DR backup can be performed by selecting **Full** or **Incremental Backup** from the **Backup** menu.

If mount points **explicitly** mentioned in the backup script are not mounted, then an error will be given at this point. Otherwise, the backup will proceed.



CBMR Bare Machine Recovery

```
/var/yp
/.ssh
known_hosts (172)
Couldn't open /etc/cbmr/media/Tue Dec 13 13:44:28 2022.lml: No such file
 or directory
Files = 45508
Skipped = 2
Directories = 4752
Bytes = 3172772833
Warnings = 0
Errors = 0

Time taken = 96 seconds
Complete

Press any key to continue... [pgup/pgdown] to scroll.
```

R
Copyright (C) Cristie Software Ltd. 2008-2022

9 Performing a Disaster Recovery

Recovery is divided into six stages:

1. **VolumeGroups** - create the required volume groups

2. **LogicalVolumes** - create the required logical volumes

3. **FileSystems** - create file-systems on the logical volumes created in the previous step

4. **Mounting** - mount the file-systems

5. **Recovery** - recover files from the backup

6. **Make bootable** - make the system bootable

Additional steps are required when Veritas Volume Manager is installed and Veritas Volume Groups must be recovered, these are:

1. **VXDisks** - make disks available for use with Veritas.

2. **VXGroups** - create Veritas Volume Groups.

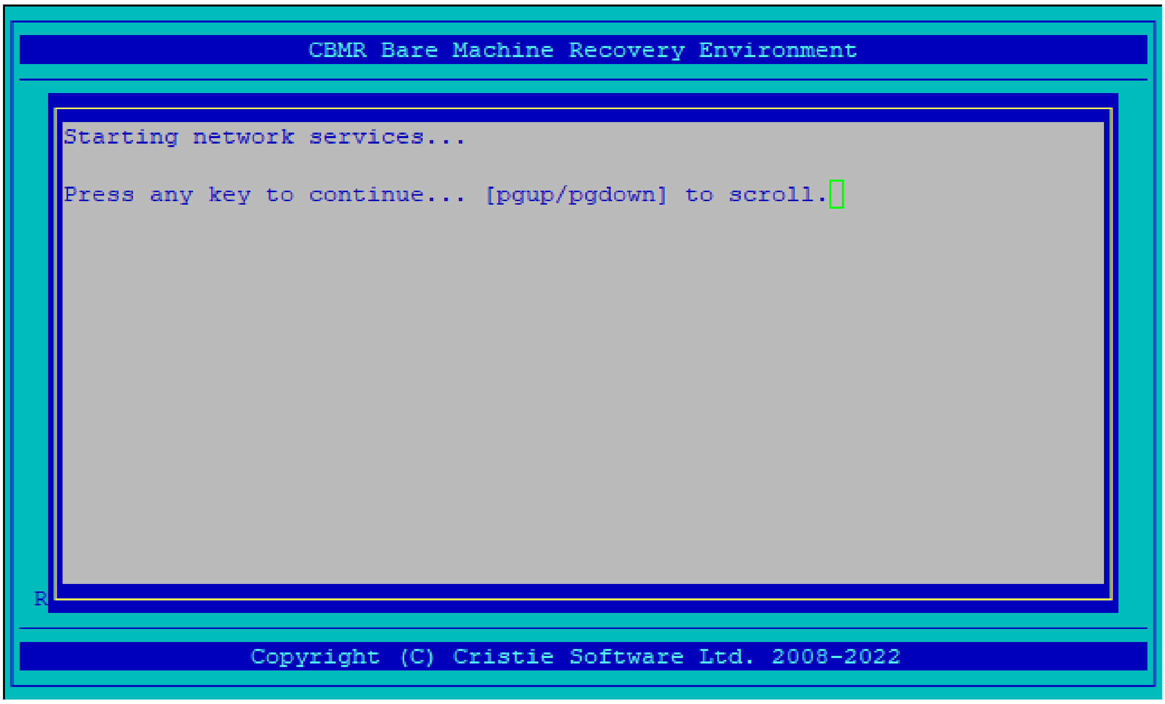
3. **VXVolumes** - create Veritas Volumes.

All stages are run though in order - consequently this can take a long time dependent upon the speed of disks and network interfaces. Once the recovery is complete, the system can be rebooted into its original state.

Before re-boot, however, it is very useful to make a copy of the log files generated during the recovery as shown in Copying Log Files.

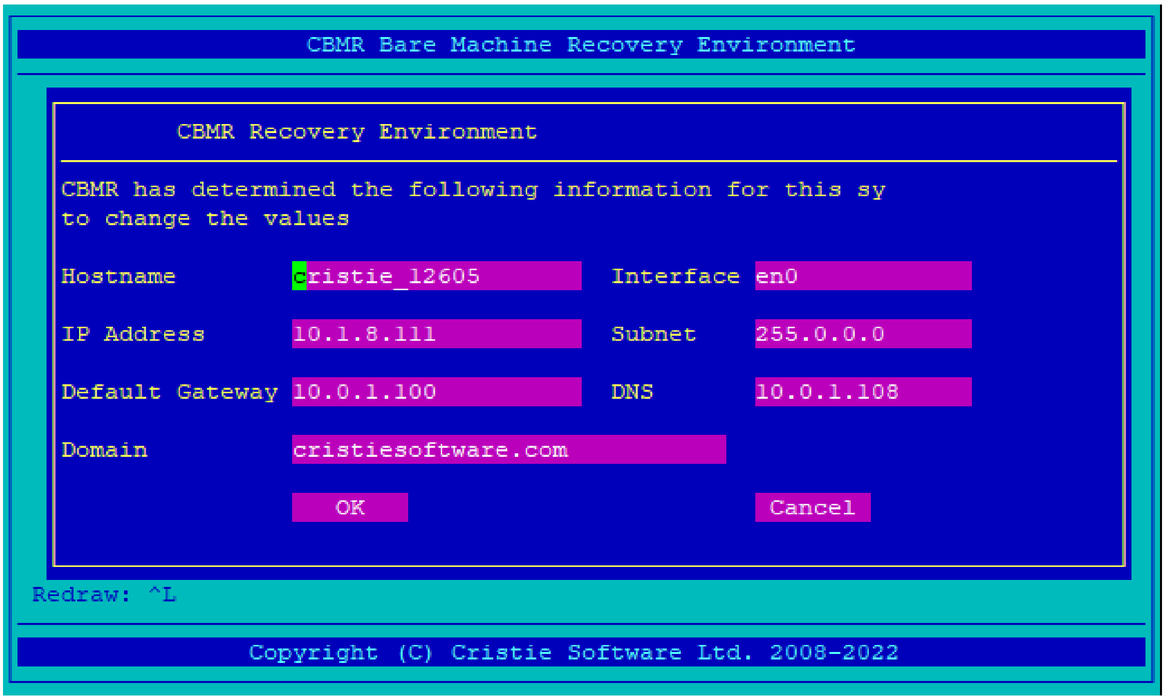
9.1 Starting the Recovery Environment

A recovery may be performed by booting into the recovery console from the recovery CD or CD image created earlier. The environment initialises by attempting to acquire a network address via **DHCP.**



```
CBMR Bare Machine Recovery Environment

Starting network services...

Press any key to continue... [pgup/pgdown] to scroll.

R

Copyright (C) Cristie Software Ltd. 2008-2022
```

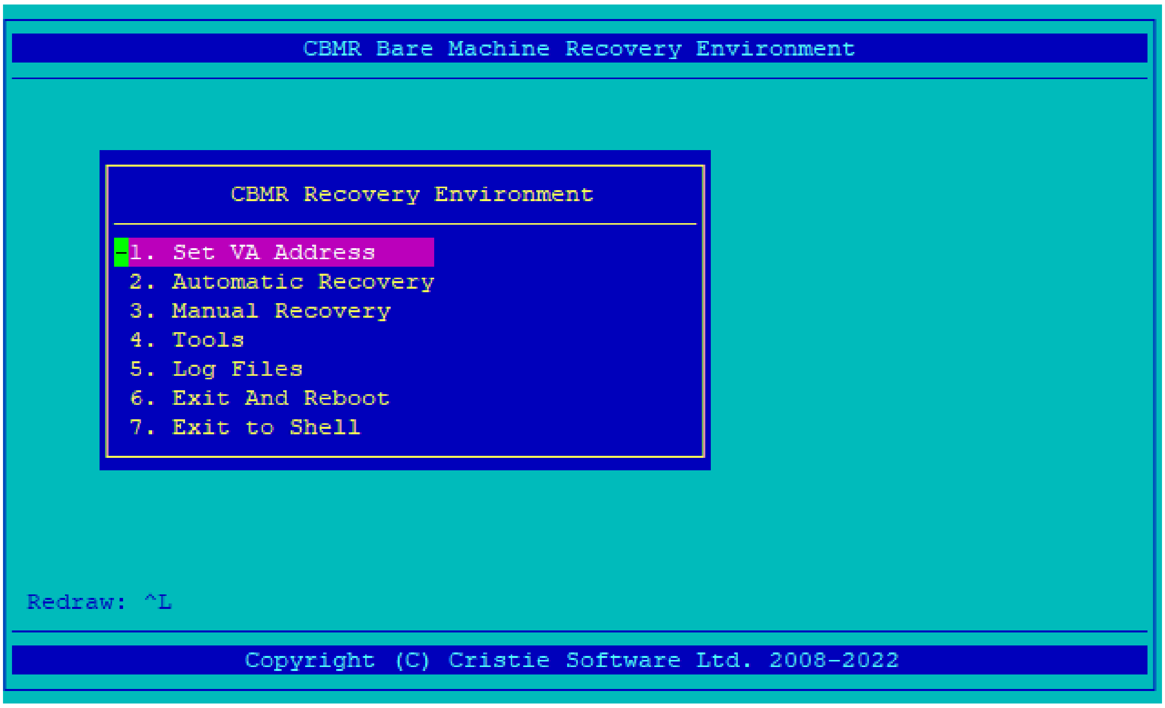
Next you should configure the recovery environment hostname and network details.



```
CBMR Bare Machine Recovery Environment

CBMR Recovery Environment

CBMR has determined the following information for this sy
to change the values

Hostname          cristie_12605        Interface  en0

IP Address        10.1.8.111           Subnet     255.0.0.0

Default Gateway   10.0.1.100           DNS        10.0.1.108

Domain            cristiesoftware.com

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

> *Note: if no DNS entry is given, then all subsequent addresses MUST be given in dotted decimal form*

Once the network is setup, the **Recovery Main Menu** is presented:



```
CBMR Bare Machine Recovery Environment

          CBMR Recovery Environment

        1. Set VA Address
        2. Automatic Recovery
        3. Manual Recovery
        4. Tools
        5. Log Files
        6. Exit And Reboot
        7. Exit to Shell

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

If you wish to monitor the recovery operation in the Cristie VA Console product use the **Set VA Address** option to set the IP address of the VA. If this is not set or set incorrectly the recovery will not be shown on the VA console.

This presents two recovery styles - automatic and manual - as well as tools for managing the recovery environment and log files.

- The **Automatic Recovery** runs through all stages of the recovery and only provides options to recover just the root volume group or the whole machine

- The **Manual Recovery** allows the option of recovering only selected volume groups and running selected phases of the recovery individually

> *Note: if the graphical environment is unusable at this stage, for example if the currently selected item appears to change unexpectedly, then the terminal type should be changed. See the Troubleshooting section for further details*

9.1.1 Automatic Recovery

The **Automatic Recovery** should be performed in this order:

1. **Setup Network** - if initial setup was unsatisfactory

2. **Backup Location** - specify the attributes of the location containing the backup

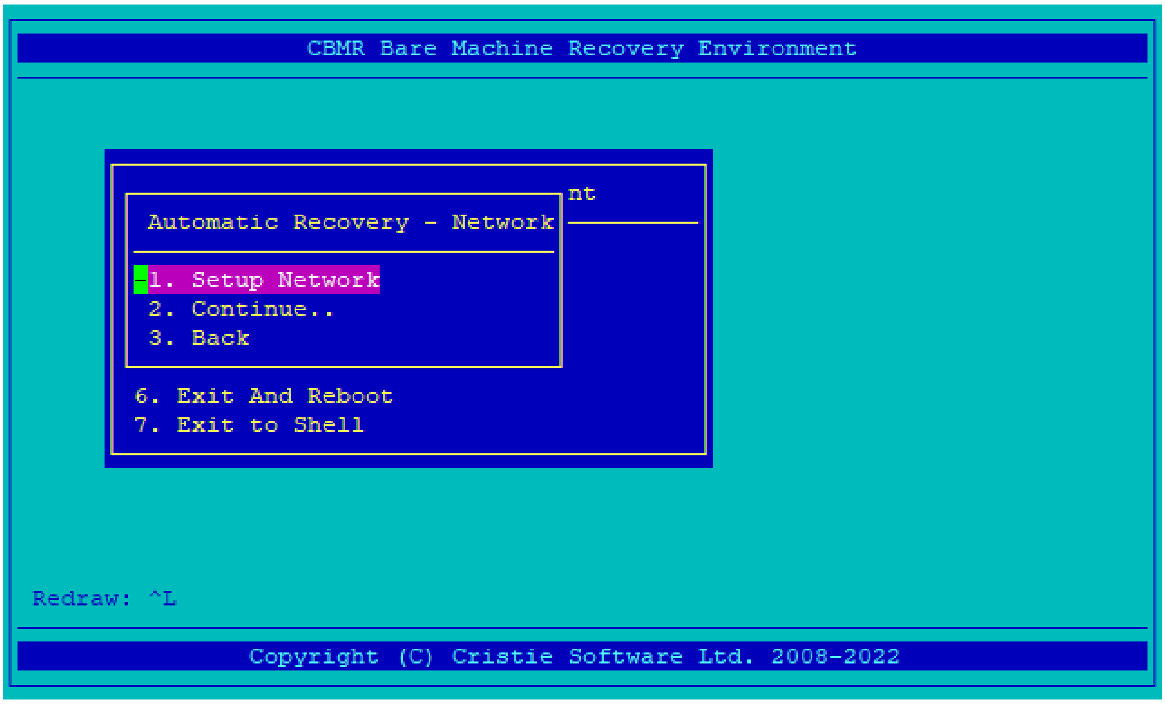
3. **Configuration** - read machine configuration information and set applicable options

4. **Perform Recovery** - start the recovery procedure

5. **Copy Log Files** - copy the log files generated by the recovery

Firstly select **Setup Network** if initial setup was unsatisfactory. Otherwise select **Continue**.

The network can be setup for any interfaces found using wither DHCP (Dynamic Host Configuration Protocol) or manual configuration.

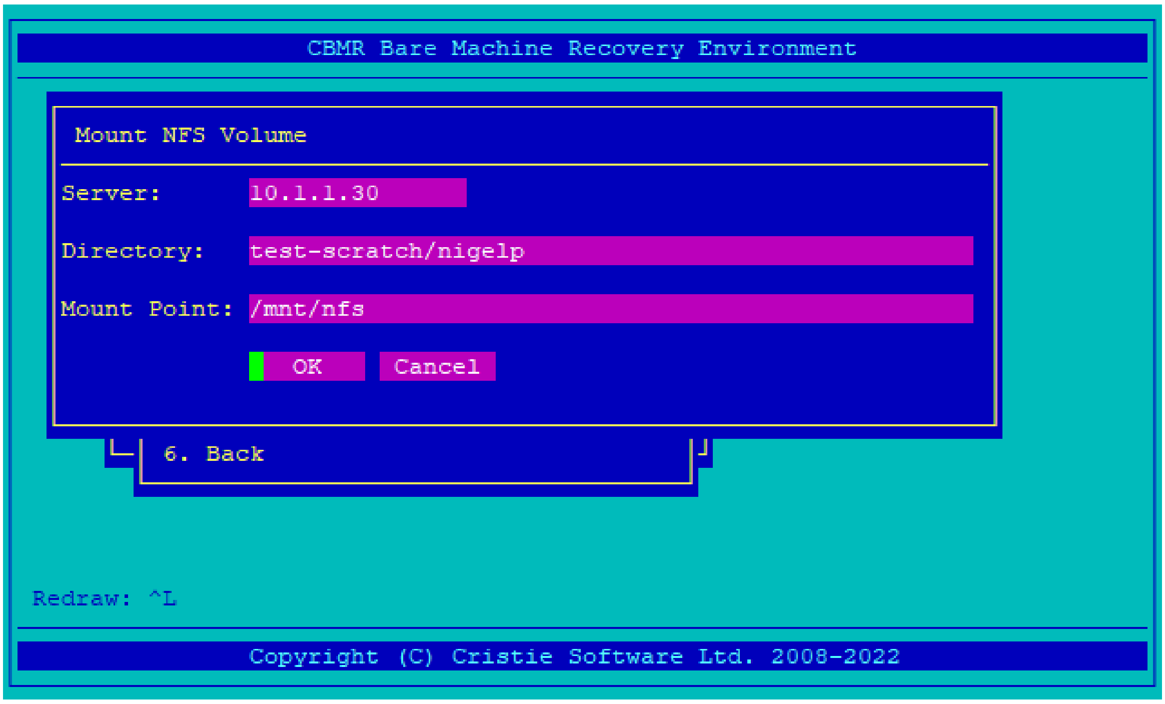


```
                    CBMR Bare Machine Recovery Environment

           nt
 Automatic Recovery - Network
 
 1. Setup Network
 2. Continue..
 3. Back

6. Exit And Reboot
7. Exit to Shell

Redraw: ^L

               Copyright (C) Cristie Software Ltd. 2008-2022
```

The manual configuration step is exactly the same as the initial network setup in Starting the Recovery Environment. The DHCP setup will attempt to start a DHCP server (if one is not already started) and check for an IP address.

> *Note: it is common to see warning messages during a DHCP setup, as interfaces may be polled whilst they are in uncertain states. The DHCP setup will fail if an IP address is not received in ten seconds. Therefore, if DHCP fails initially, it may succeed on subsequent attempts after more time will have elapsed*

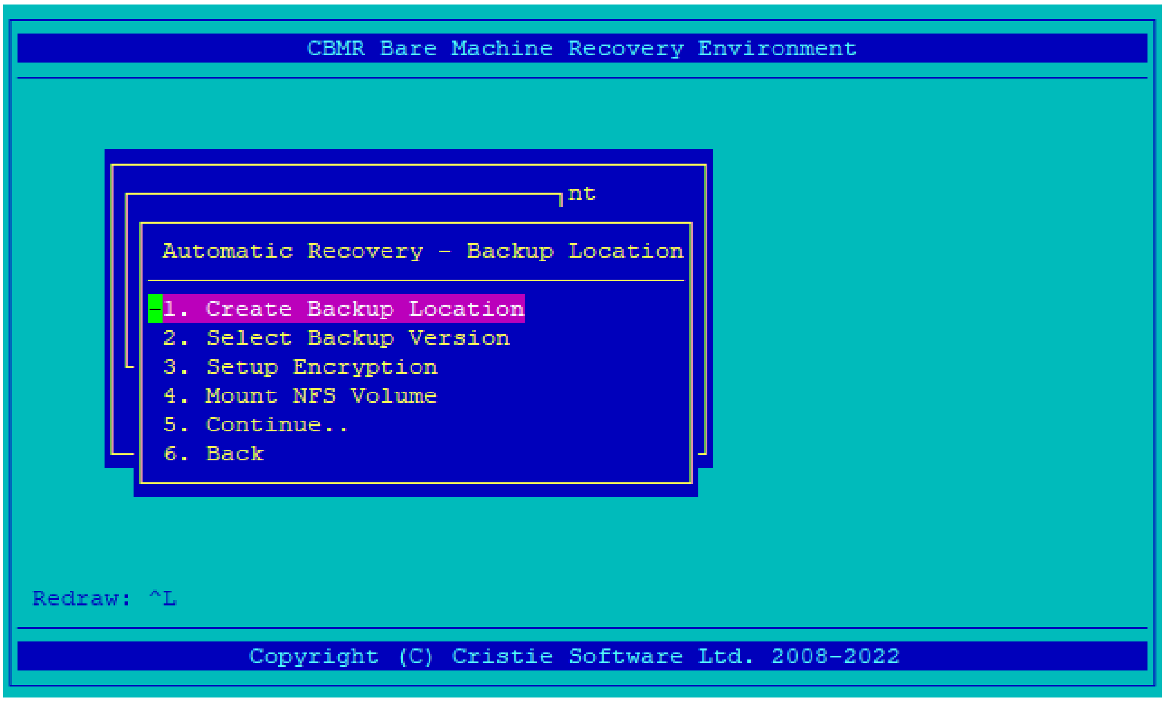
Now setup any required network share details required (e.g. a VTD backup location).



```
CBMR Bare Machine Recovery Environment

Mount NFS Volume

Server:       10.1.1.30
Directory:    test-scratch/nigelp
Mount Point:  /mnt/nfs

              OK    Cancel

6. Back

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

Backup Location

The Backup Location menu allows the user to setup the backup location in the same manner.



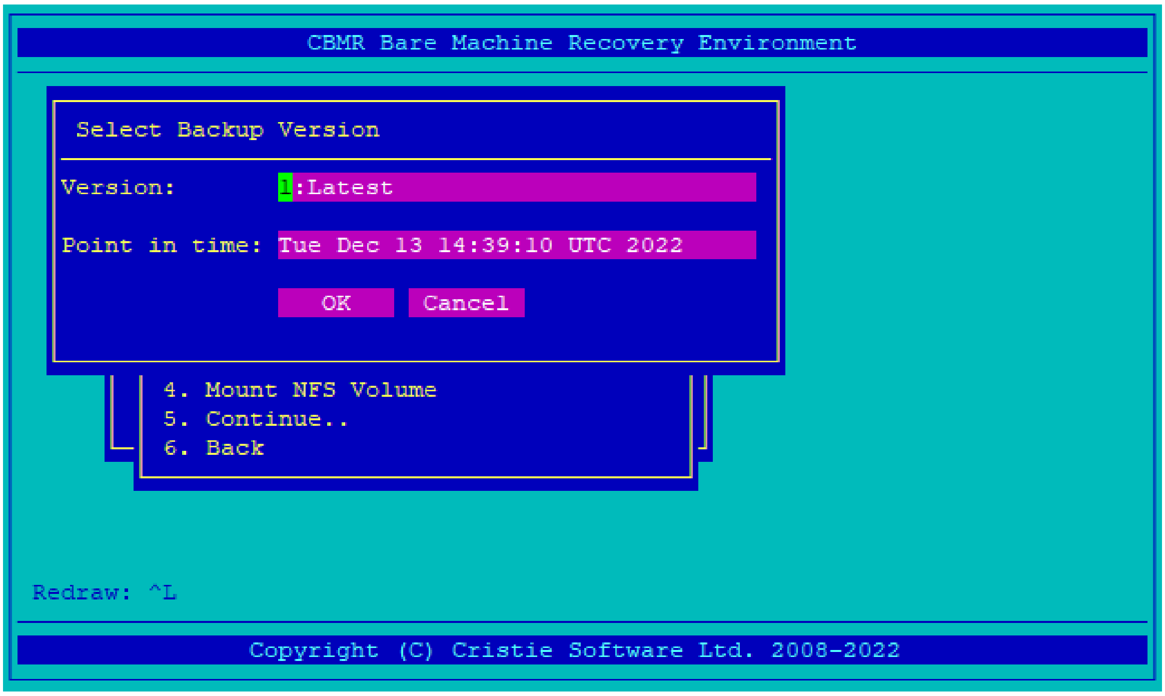
```
CBMR Bare Machine Recovery Environment

                                          nt
Automatic Recovery - Backup Location

1. Create Backup Location
2. Select Backup Version
3. Setup Encryption
4. Mount NFS Volume
5. Continue..
6. Back

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

A backup location must be specified before the backup version is chosen, as the location is queried to find the versions that are available.

> *Note: Select the backup version for a point-in-time recovery if the backup is maintained in an incremental file backup location.*

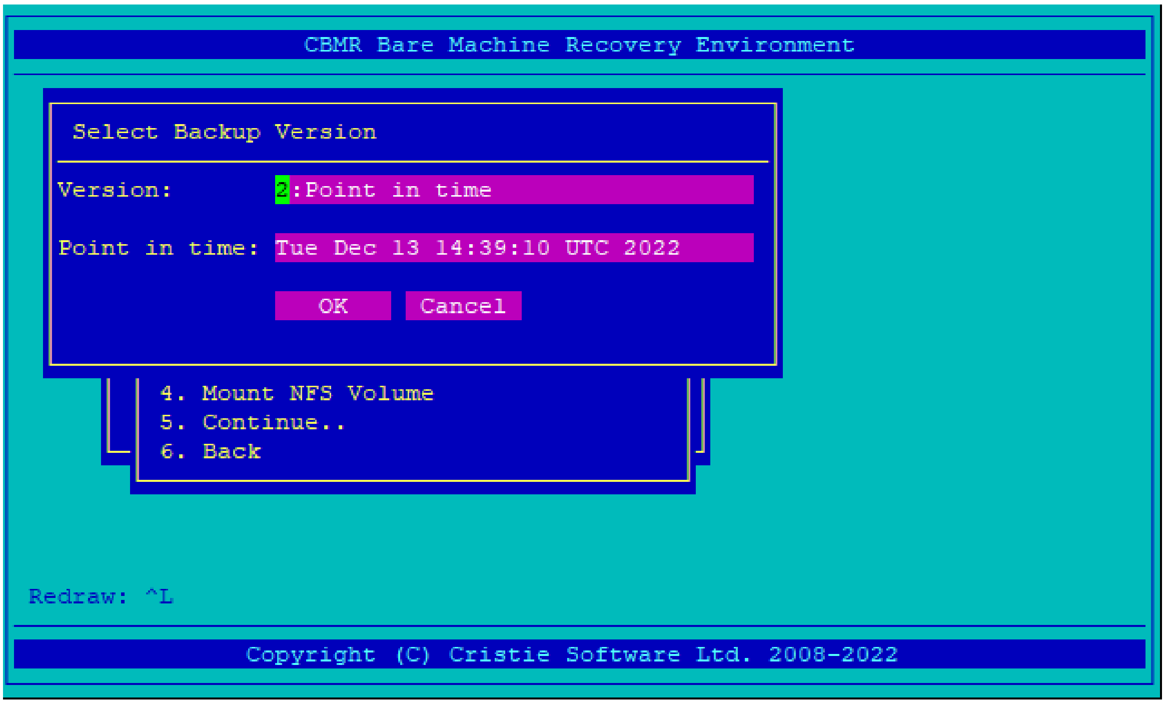
> *Note 2: If your backup exists on a Network Share, or the IBM Spectrum Protect server requires a SSL Certificate, you must first mount an NFS Volume using the 'Mount NFS*

Volume' option.



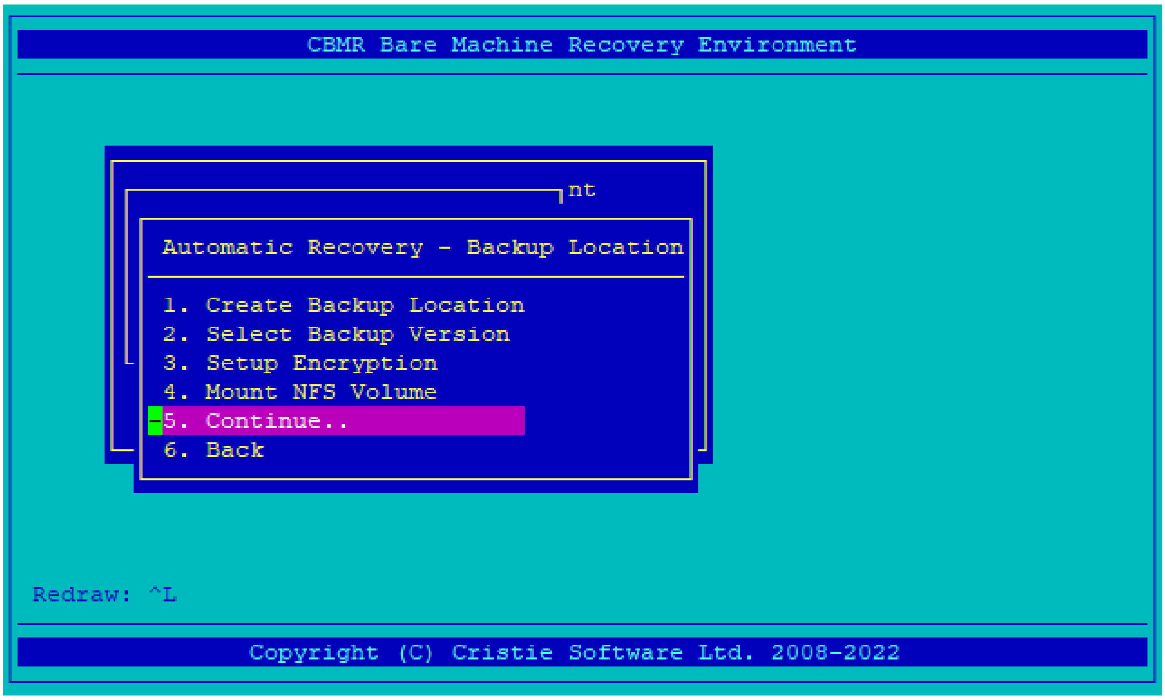
```
                  CBMR Bare Machine Recovery Environment

   Select Backup Version
  Version:        1:Latest

  Point in time: Tue Dec 13 14:39:10 UTC 2022

                   OK     Cancel

        4. Mount NFS Volume
        5. Continue..
        6. Back

 Redraw: ^L
               Copyright (C) Cristie Software Ltd. 2008-2022
```

It is also possible to select the last backup performed before a given point in time.



```
                  CBMR Bare Machine Recovery Environment

   Select Backup Version
  Version:        2:Point in time

  Point in time: Tue Dec 13 14:39:10 UTC 2022

                   OK     Cancel

        4. Mount NFS Volume
        5. Continue..
        6. Back

 Redraw: ^L
               Copyright (C) Cristie Software Ltd. 2008-2022
```

When you have selected the required version click OK to continue. Then on the Automatic Recovery menu select Continue..

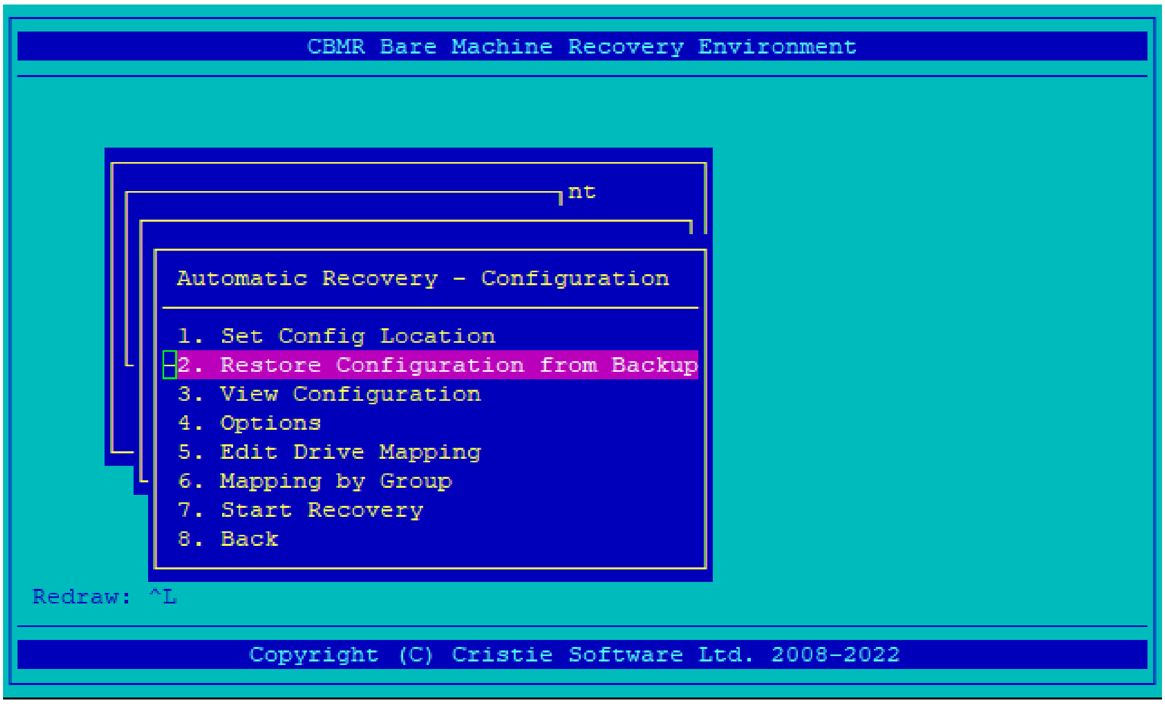


```
CBMR Bare Machine Recovery Environment

                     nt
  Automatic Recovery - Backup Location

  1. Create Backup Location
  2. Select Backup Version
  3. Setup Encryption
  4. Mount NFS Volume
  5. Continue..
  6. Back

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

Once the backup has been successfully setup, you can move to the next stage to setup the configuration.

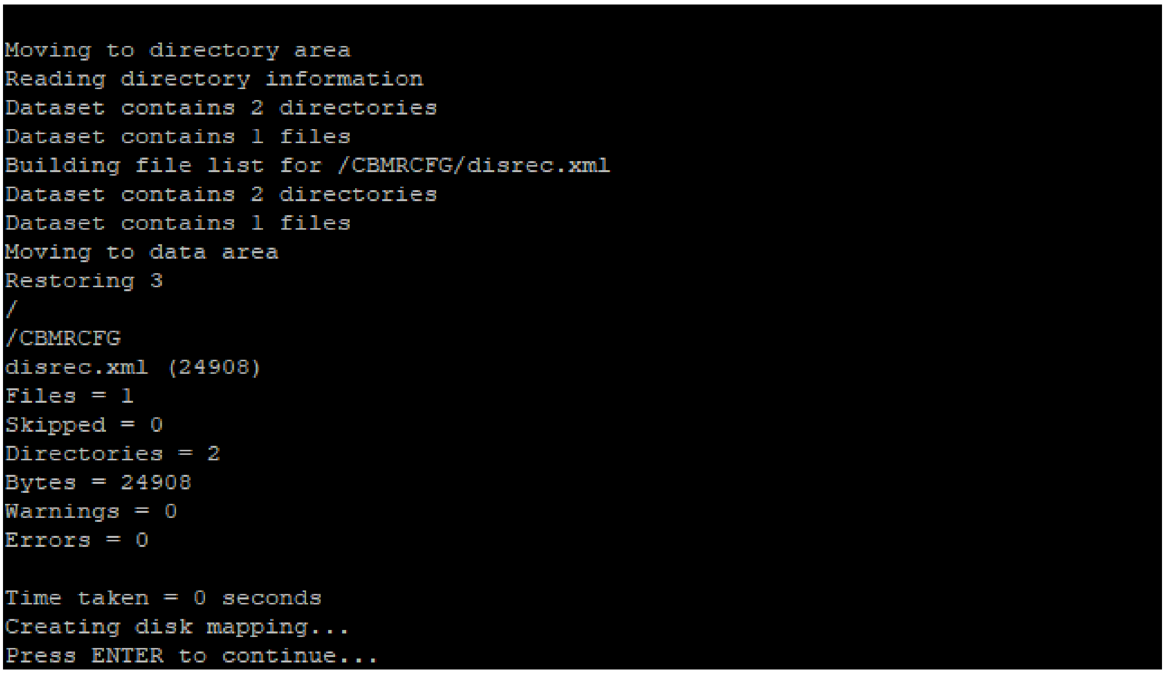
Configuration

Before recovery can begin, the machine configuration information created earlier must be loaded into the recovery environment from the backup. This is performed by selecting the **Restore Configuration From Backup** option:



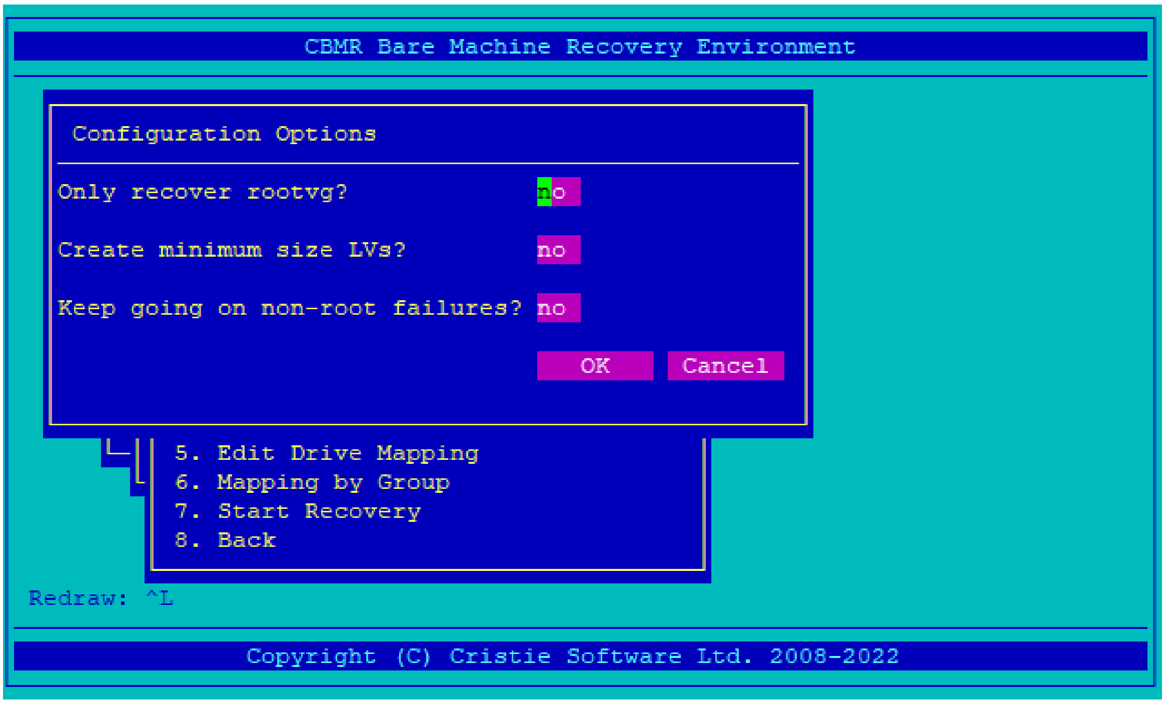
```
CBMR Bare Machine Recovery Environment

                     nt
  Automatic Recovery - Configuration

  1. Set Config Location
  2. Restore Configuration from Backup
  3. View Configuration
  4. Options
  5. Edit Drive Mapping
  6. Mapping by Group
  7. Start Recovery
  8. Back

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

If the location of the configuration information was changed during Recording System Information, you need to enter the location chosen here. A typical restore configuration looks like this:



```
Moving to directory area
Reading directory information
Dataset contains 2 directories
Dataset contains 1 files
Building file list for /CBMRCFG/disrec.xml
Dataset contains 2 directories
Dataset contains 1 files
Moving to data area
Restoring 3
/
/CBMRCFG
disrec.xml (24908)
Files = 1
Skipped = 0
Directories = 2
Bytes = 24908
Warnings = 0
Errors = 0

Time taken = 0 seconds
Creating disk mapping...
Press ENTER to continue...
```

Selecting the **Options** item displays any additional options that can be applied at this point.



CBMR Bare Machine Recovery Environment

Configuration Options

Only recover rootvg? no

Create minimum size LVs? no

Keep going on non-root failures? no

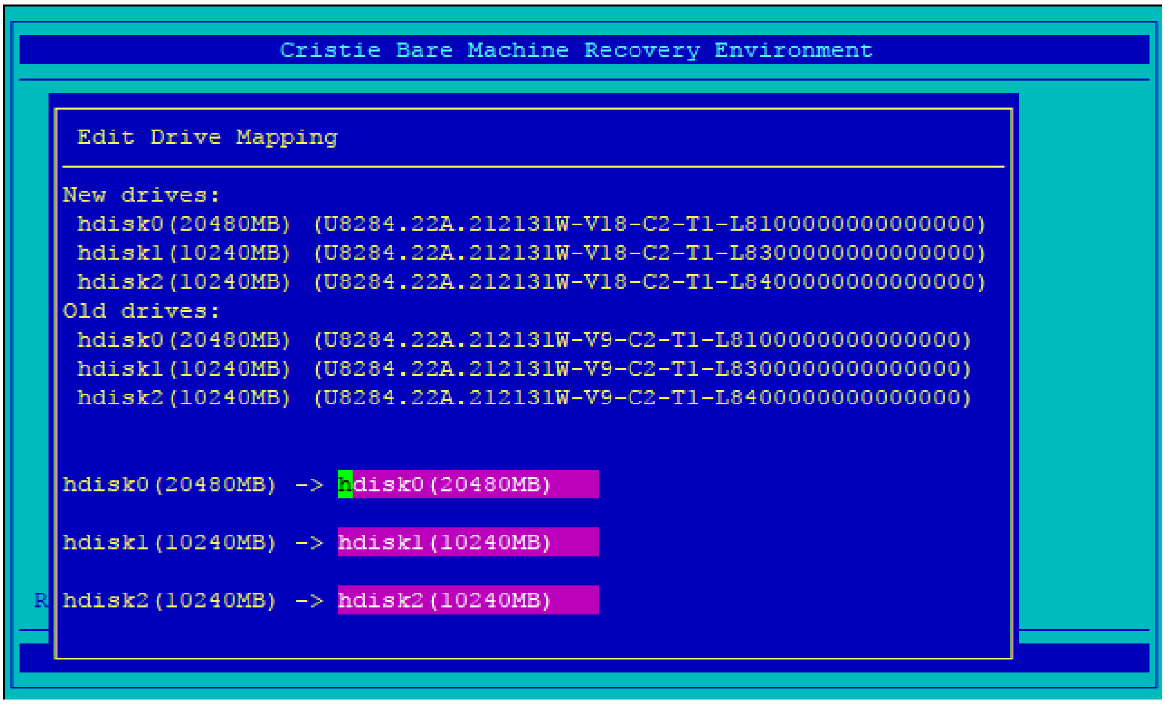
Copyright (C) Cristie Software Ltd. 2008-2022

Only Recover Root VG: By default, all volume groups are recovered. This option is useful in situations where data is stored on a second data-only volume group which is not included in the backup.

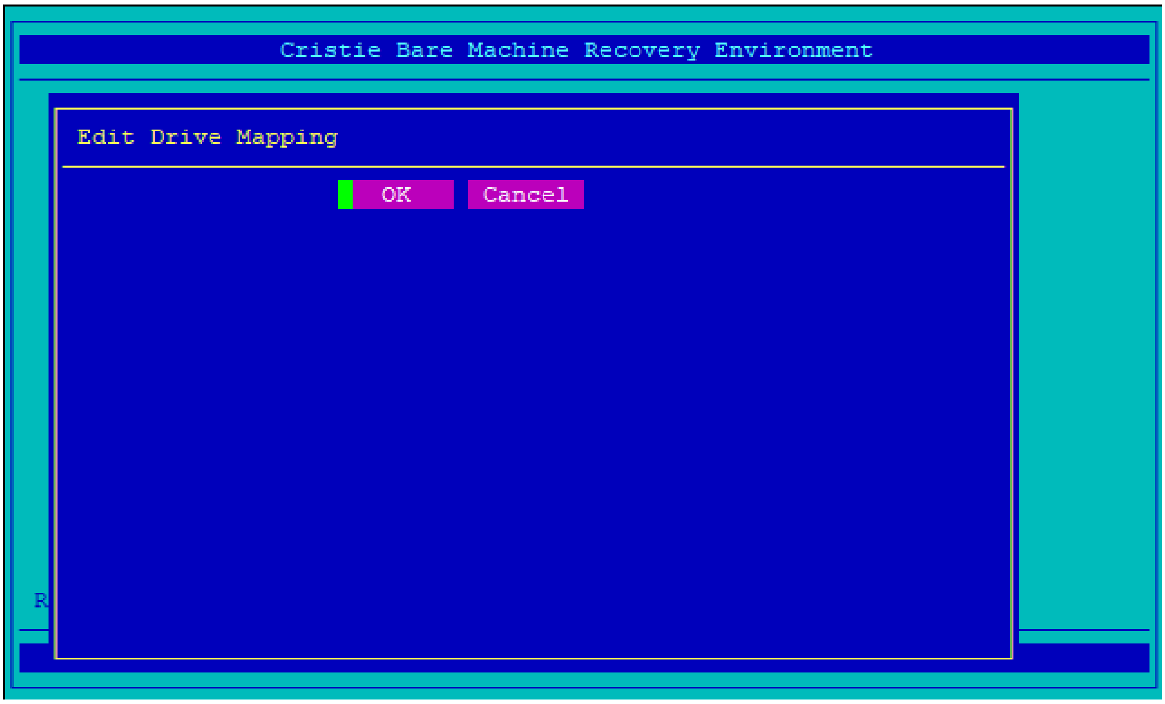
Create Minimum Size LVs: This option ensures that the logical volumes created are of the smallest size such that the data to restore fits. This option is useful if you are recovering to a machine with smaller disks.

Keep going on non-root failures: By default all failures are considered fatal and immediately halt a recovery. If this option is selected only failures that prevent the restoration of volumes and file-systems directly associated with the root volume group halt a recovery.

> *Note: the minimum size calculation is performed when the configuration information is recorded but it is re-calculated when the backup is accessed.*



```
Cristie Bare Machine Recovery Environment

 Edit Drive Mapping

New drives:
 hdisk0(20480MB) (U8284.22A.212131W-V18-C2-T1-L8100000000000000)
 hdisk1(10240MB) (U8284.22A.212131W-V18-C2-T1-L8300000000000000)
 hdisk2(10240MB) (U8284.22A.212131W-V18-C2-T1-L8400000000000000)
Old drives:
 hdisk0(20480MB) (U8284.22A.212131W-V9-C2-T1-L8100000000000000)
 hdisk1(10240MB) (U8284.22A.212131W-V9-C2-T1-L8300000000000000)
 hdisk2(10240MB) (U8284.22A.212131W-V9-C2-T1-L8400000000000000)


hdisk0(20480MB) -> hdisk0(20480MB)

hdisk1(10240MB) -> hdisk1(10240MB)

hdisk2(10240MB) -> hdisk2(10240MB)
```

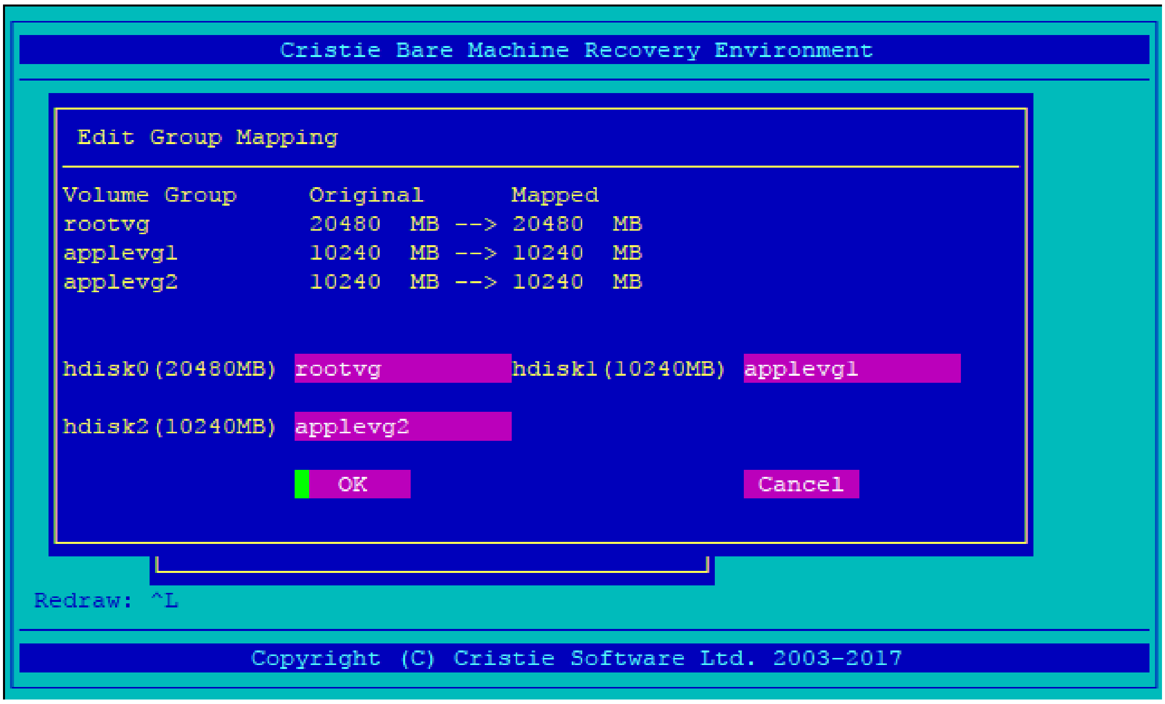


```
Cristie Bare Machine Recovery Environment

 Edit Drive Mapping

                   OK    Cancel
```

The **Edit Drive Mapping** item is used to modify the disks that the backup is restored to. In the example given, a system using two disks is mapped to a use only one disk during recovery.

> *Note: Should the drive display spread over more than one screen you can navigate forwards Ctrl +N or the previous page Ctrl +P.*

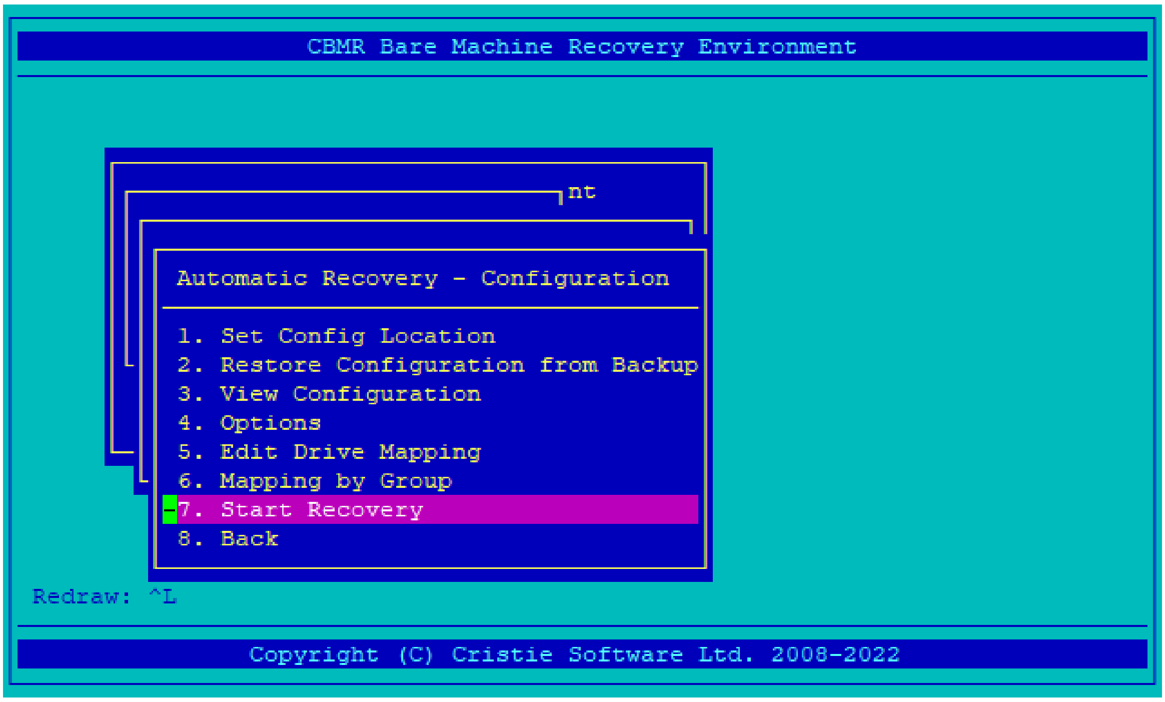
When recovering to fewer disks, any volume groups other than rootvg which cannot be re-created are dropped. However, a volume group spanning more than one physical volume can be restored to a single volume provided that volume has enough capacity. In the case of mirrored volume groups the mirroring is split if the mapping indicates this.



```
                 Cristie Bare Machine Recovery Environment

 Edit Group Mapping

Volume Group      Original      Mapped
rootvg            20480  MB --> 20480  MB
applevg1          10240  MB --> 10240  MB
applevg2          10240  MB --> 10240  MB


hdisk0(20480MB) rootvg         hdisk1(10240MB) applevg1

hdisk2(10240MB) applevg2

                  OK                              Cancel

Redraw: ^L

            Copyright (C) Cristie Software Ltd. 2003-2017
```

The **Edit Group Mapping** item is used to modify the disks that the backup is restored to by selecting which disks belong to which volume group. In the example given both disks are given to the rootvg volume group and the testvg volume group is given one, so is not restored. The same rules for recovering to fewer disks as were used for Edit Drive Mapping are used here.

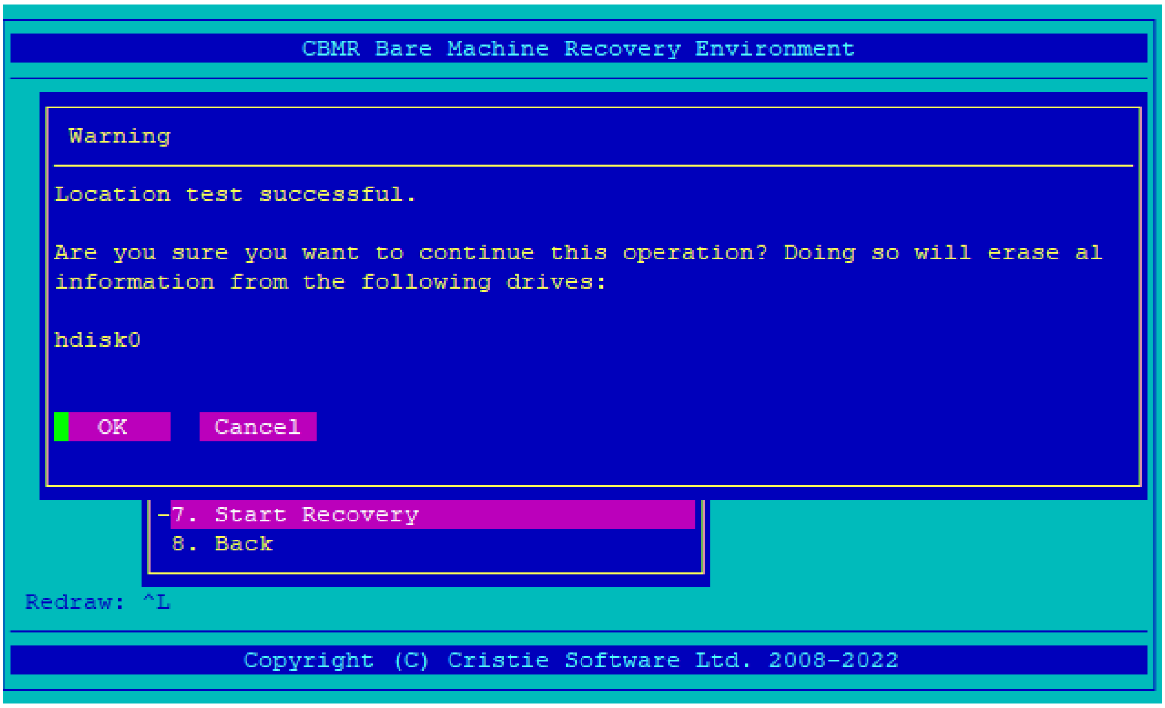
Now select **Start Recovery**.



```
CBMR Bare Machine Recovery Environment

                                                  nt

      Automatic Recovery - Configuration

      1. Set Config Location
      2. Restore Configuration from Backup
      3. View Configuration
      4. Options
      5. Edit Drive Mapping
      6. Mapping by Group
      7. Start Recovery
      8. Back

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

Perform Recovery

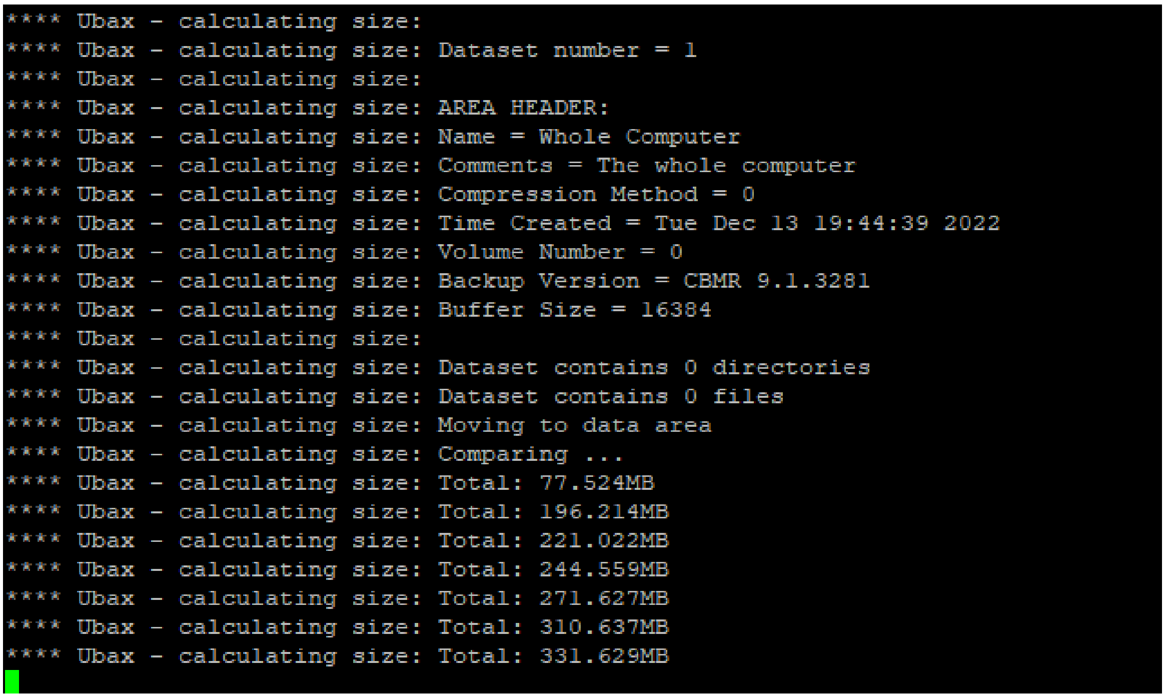
Once the configuration has been restored, it is possible to start the recovery. When this option is selected, the backup location is tested and a confirmation dialogue presented:



```
CBMR Bare Machine Recovery Environment

 Warning

Location test successful.

Are you sure you want to continue this operation? Doing so will erase al
information from the following drives:

hdisk0


  OK     Cancel

        -7. Start Recovery
         8. Back

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

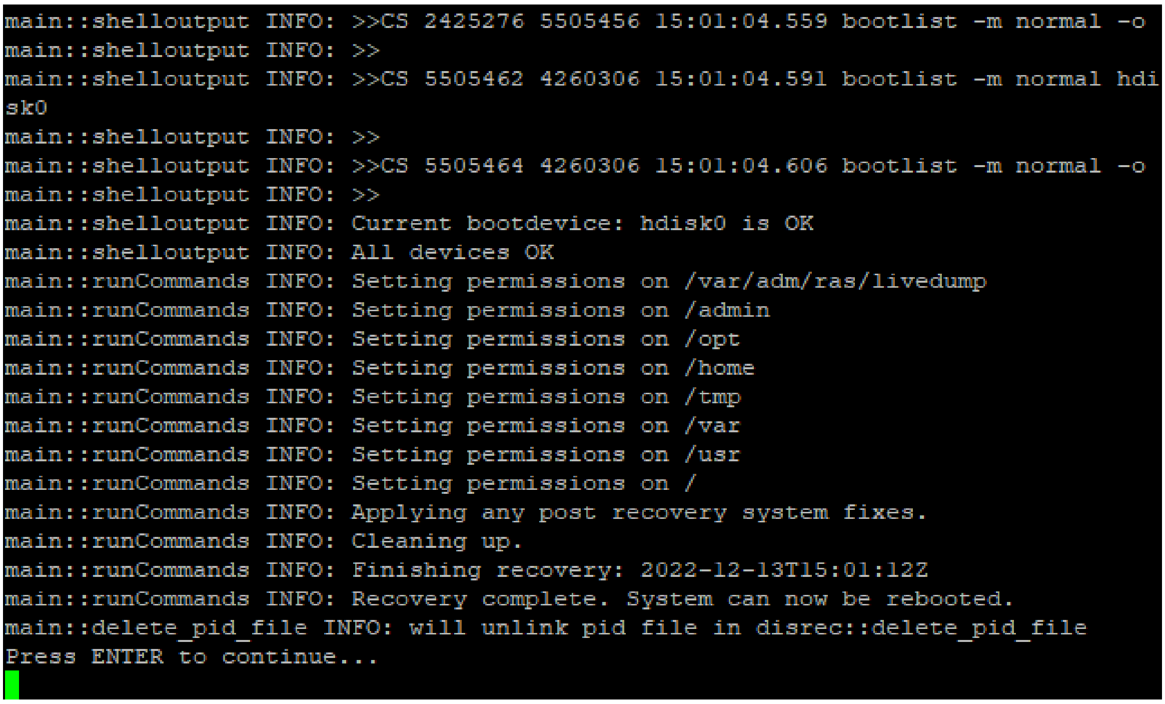
Note: as soon as the automatic recovery is started, ALL data is destroyed on the disks being recovered to

The recovery then proceeds.



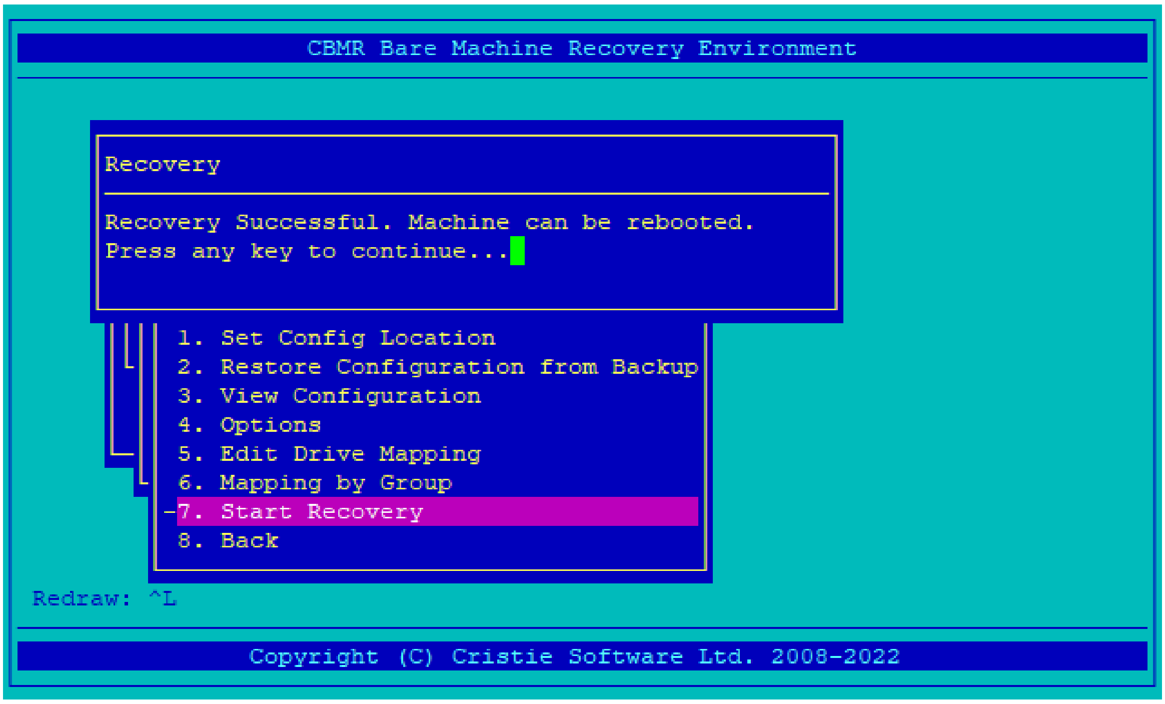
```
**** Ubax - calculating size:
**** Ubax - calculating size: Dataset number = 1
**** Ubax - calculating size:
**** Ubax - calculating size: AREA HEADER:
**** Ubax - calculating size: Name = Whole Computer
**** Ubax - calculating size: Comments = The whole computer
**** Ubax - calculating size: Compression Method = 0
**** Ubax - calculating size: Time Created = Tue Dec 13 19:44:39 2022
**** Ubax - calculating size: Volume Number = 0
**** Ubax - calculating size: Backup Version = CBMR 9.1.3281
**** Ubax - calculating size: Buffer Size = 16384
**** Ubax - calculating size:
**** Ubax - calculating size: Dataset contains 0 directories
**** Ubax - calculating size: Dataset contains 0 files
**** Ubax - calculating size: Moving to data area
**** Ubax - calculating size: Comparing ...
**** Ubax - calculating size: Total: 77.524MB
**** Ubax - calculating size: Total: 196.214MB
**** Ubax - calculating size: Total: 221.022MB
**** Ubax - calculating size: Total: 244.559MB
**** Ubax - calculating size: Total: 271.627MB
**** Ubax - calculating size: Total: 310.637MB
**** Ubax - calculating size: Total: 331.629MB
```

You will see this when the recovery is complete:



```
main::shelloutput INFO: >>CS 2425276 5505456 15:01:04.559 bootlist -m normal -o
main::shelloutput INFO: >>
main::shelloutput INFO: >>CS 5505462 4260306 15:01:04.591 bootlist -m normal hdi
sk0
main::shelloutput INFO: >>
main::shelloutput INFO: >>CS 5505464 4260306 15:01:04.606 bootlist -m normal -o
main::shelloutput INFO: >>
main::shelloutput INFO: Current bootdevice: hdisk0 is OK
main::shelloutput INFO: All devices OK
main::runCommands INFO: Setting permissions on /var/adm/ras/livedump
main::runCommands INFO: Setting permissions on /admin
main::runCommands INFO: Setting permissions on /opt
main::runCommands INFO: Setting permissions on /home
main::runCommands INFO: Setting permissions on /tmp
main::runCommands INFO: Setting permissions on /var
main::runCommands INFO: Setting permissions on /usr
main::runCommands INFO: Setting permissions on /
main::runCommands INFO: Applying any post recovery system fixes.
main::runCommands INFO: Cleaning up.
main::runCommands INFO: Finishing recovery: 2022-12-13T15:01:12Z
main::runCommands INFO: Recovery complete. System can now be rebooted.
main::delete_pid_file INFO: will unlink pid file in disrec::delete_pid_file
Press ENTER to continue...
```

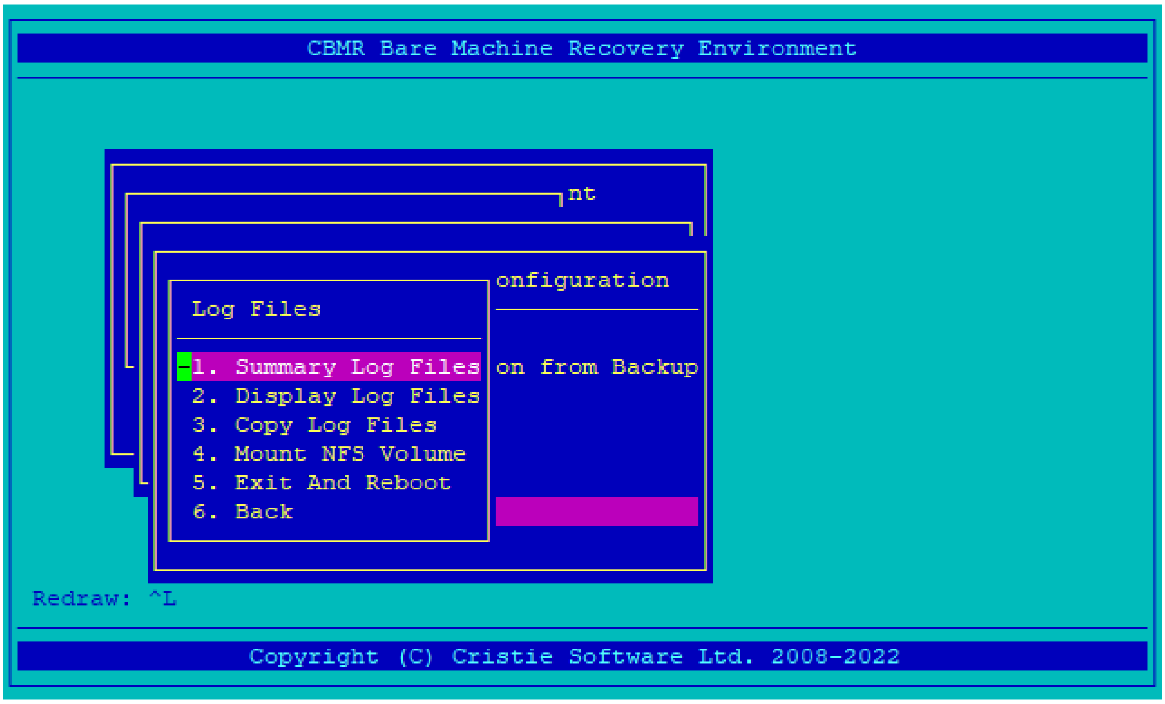
Press ENTER and you will be presented with a dialogue indicating that the machine can be rebooted:



```
                CBMR Bare Machine Recovery Environment

     Recovery

     Recovery Successful. Machine can be rebooted.
     Press any key to continue...

          1. Set Config Location
          2. Restore Configuration from Backup
          3. View Configuration
          4. Options
          5. Edit Drive Mapping
          6. Mapping by Group
          7. Start Recovery
          8. Back
 Redraw: ^L

            Copyright (C) Cristie Software Ltd. 2008-2022
```

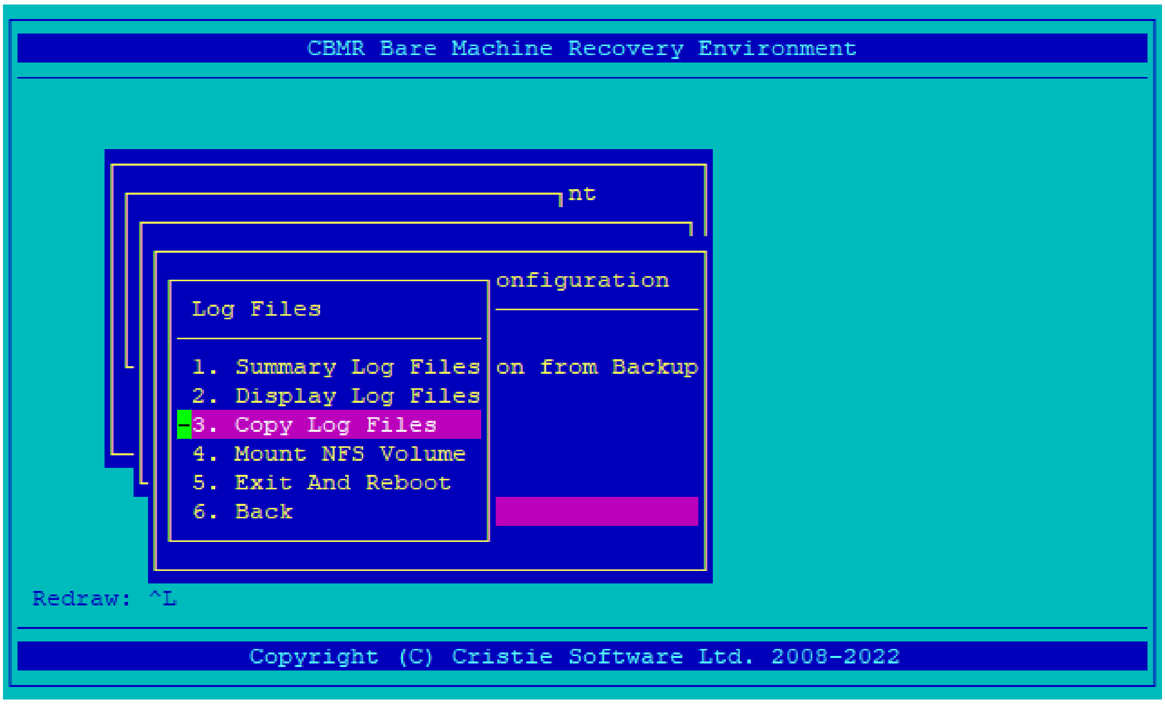
Copy Logs

Once the recovery is complete, a menu is opened containing options for viewing and copying the log files.



```
                CBMR Bare Machine Recovery Environment

                                     nt

                                   onfiguration
           Log Files

           1. Summary Log Files    on from Backup
           2. Display Log Files
           3. Copy Log Files
           4. Mount NFS Volume
           5. Exit And Reboot
           6. Back
 Redraw: ^L

            Copyright (C) Cristie Software Ltd. 2008-2022
```

It is recommended that Log Files are copied to a network share as a precaution in case the booted system does not boot correctly or the target configuration is created incorrectly. Use **Copy Log Files** to do this but you may need to mount a network share first. Use **Mount NFS Volume** to do this. **Display Log Files** does exactly that but only a screen's worth at a time.

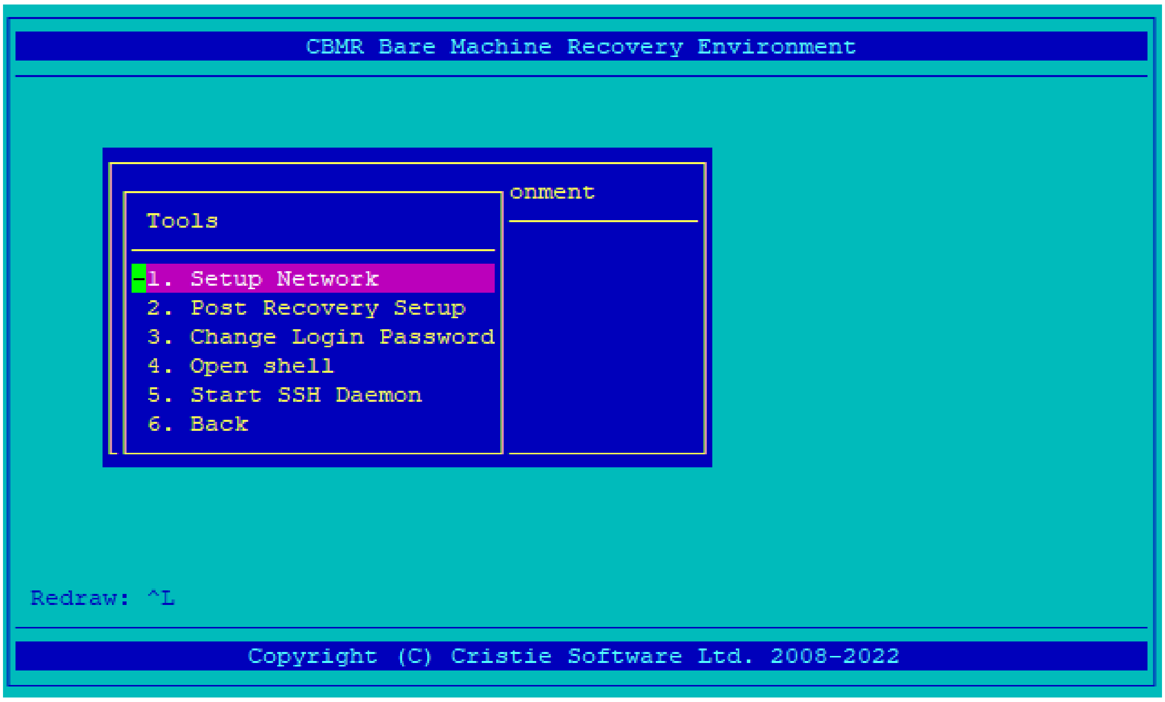


```
CBMR Bare Machine Recovery Environment

Log Files

1. Summary Log Files
2. Display Log Files
3. Copy Log Files
4. Mount NFS Volume
5. Exit And Reboot
6. Back

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

The **Summary Log Files** item is used to present a summary of the warnings, errors and informational items that occurred during the recovery for immediate inspection.

9.1.2 Tools

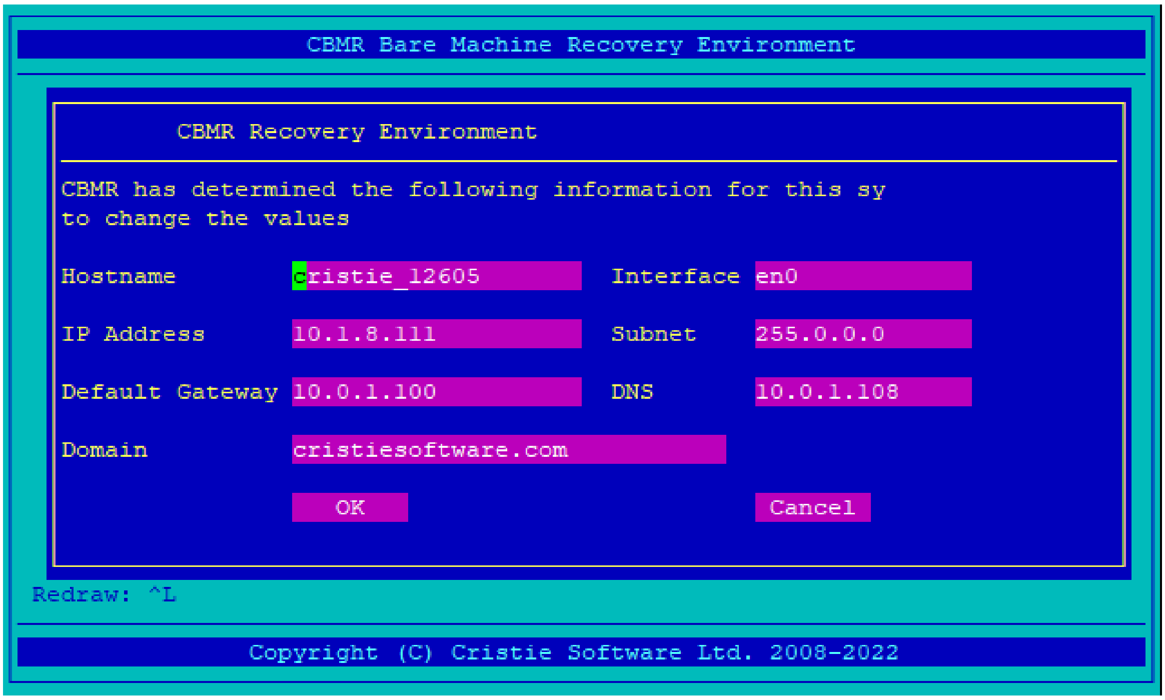
The **Tools** menu provides several miscellaneous options not frequently required



```
CBMR Bare Machine Recovery Environment

Tools

1. Setup Network
2. Post Recovery Setup
3. Change Login Password
4. Open shell
5. Start SSH Daemon
6. Back

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

9.1.2.1 Setup Network

At any point you can configure the recovery environment hostname and network details.

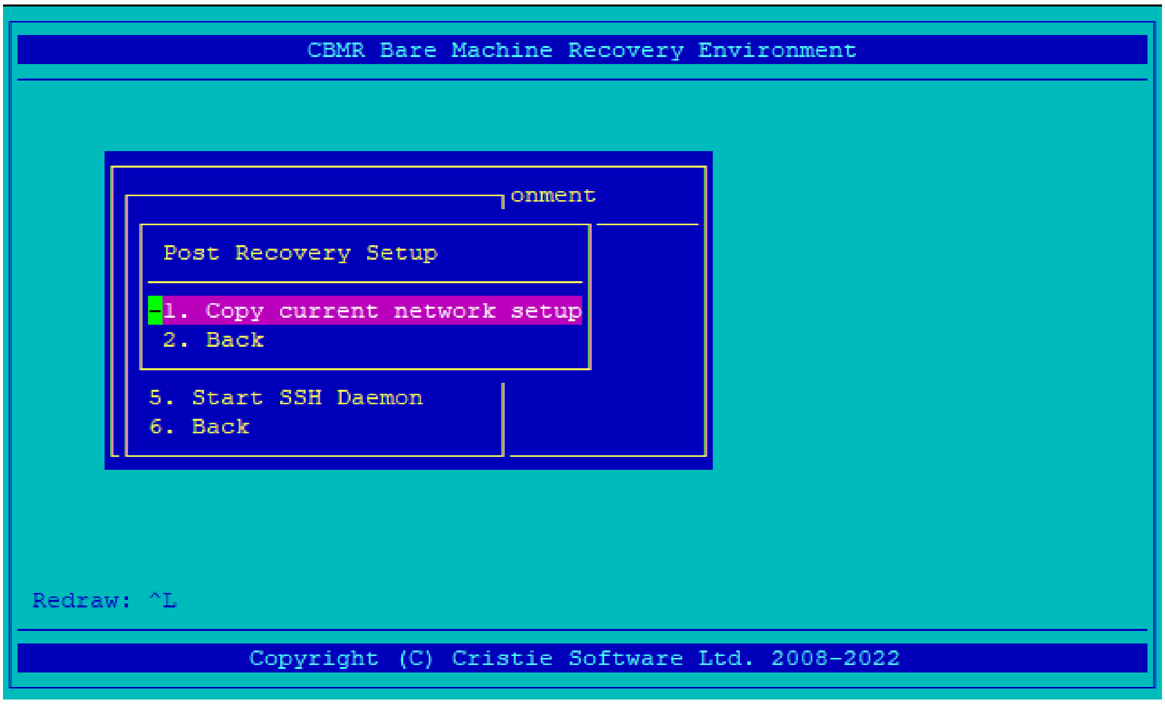


```
                CBMR Bare Machine Recovery Environment

        CBMR Recovery Environment

CBMR has determined the following information for this sy
to change the values

Hostname        cristie_12605        Interface en0

IP Address      10.1.8.111           Subnet    255.0.0.0

Default Gateway 10.0.1.100           DNS       10.0.1.108

Domain          cristiesoftware.com

                   OK                    Cancel

Redraw: ^L

            Copyright (C) Cristie Software Ltd. 2008-2022
```

Select OK to set the new configuration.

9.1.2.2 Post Recovery Setup

If you wish to change the hostname and/or network details of the recovered system use the **Setup Network** option to configure the new parameters first and then select **Copy current network setup** from the **Post Recovery Setup** menu.



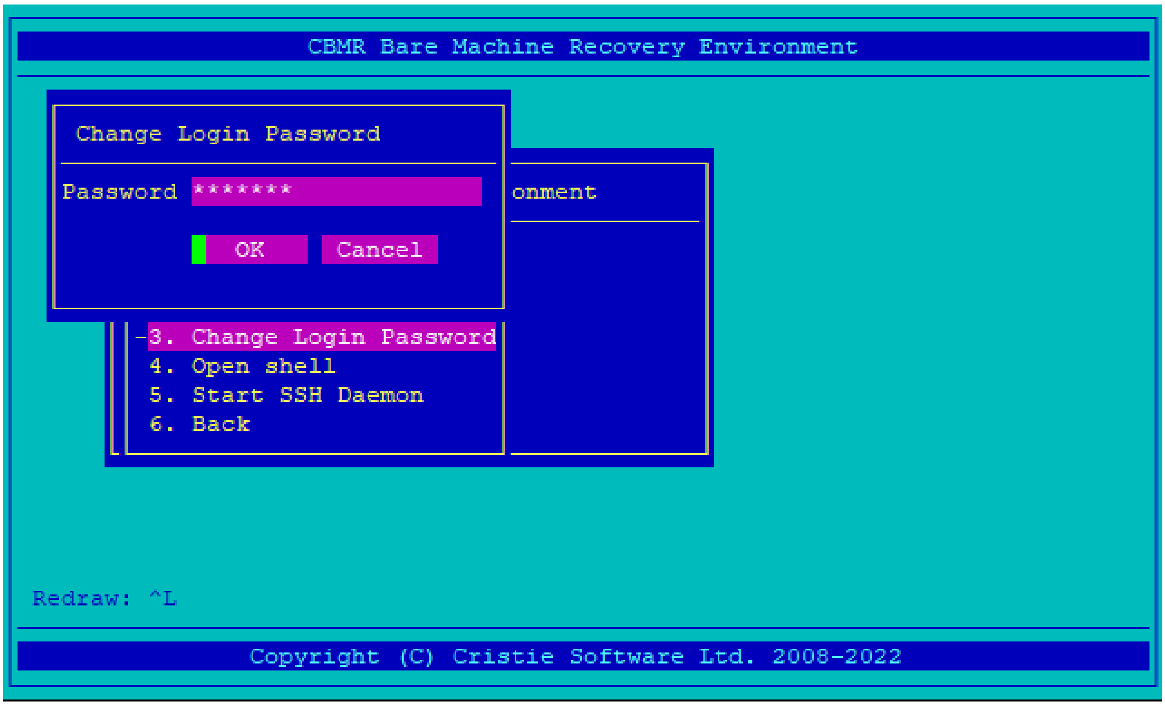
```
                CBMR Bare Machine Recovery Environment

                         onment
    Post Recovery Setup

    1. Copy current network setup
    2. Back

  5. Start SSH Daemon
  6. Back

Redraw: ^L

            Copyright (C) Cristie Software Ltd. 2008-2022
```

This is a useful option if you are cloning or moving a recovered machine.

> *Note: This must be done* ***BEFORE*** *the recovery is performed otherwise the new details will not be applied to the target.*

9.1.2.3 Change Login Password

After enabling the SSH Daemon you may reset the SSH root password using this option.

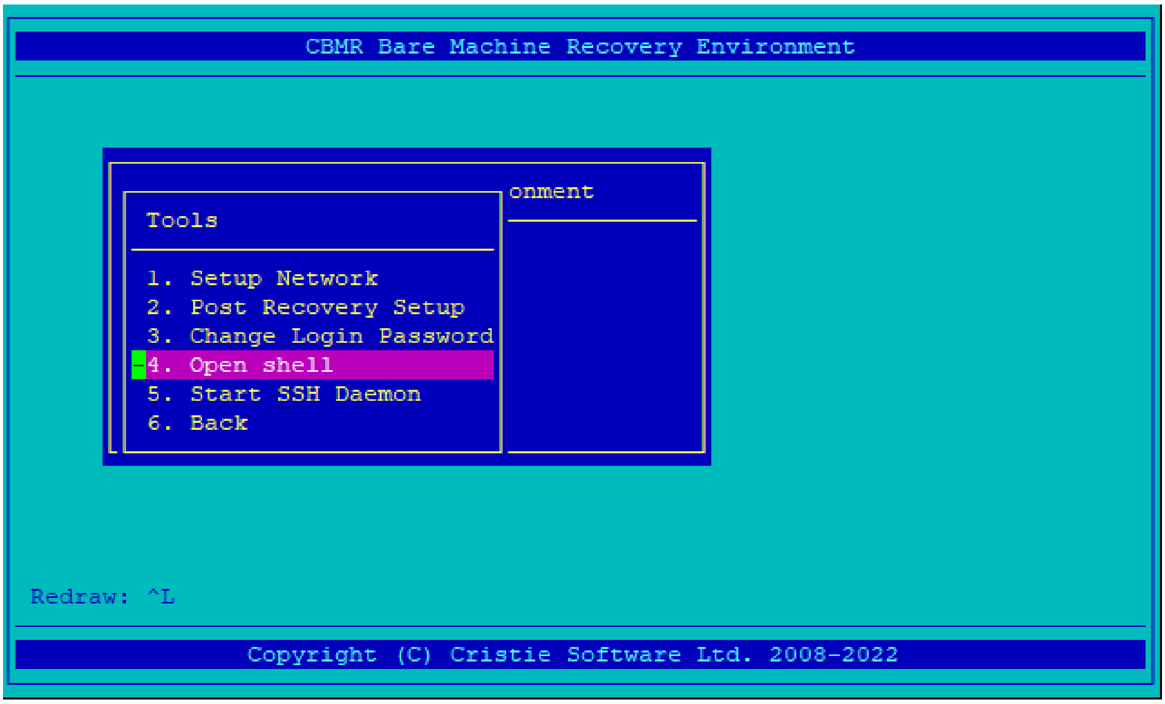


```
CBMR Bare Machine Recovery Environment

Change Login Password
Password *******
OK   Cancel

-3. Change Login Password
 4. Open shell
 5. Start SSH Daemon
 6. Back

Redraw: ^L
Copyright (C) Cristie Software Ltd. 2008-2022
```

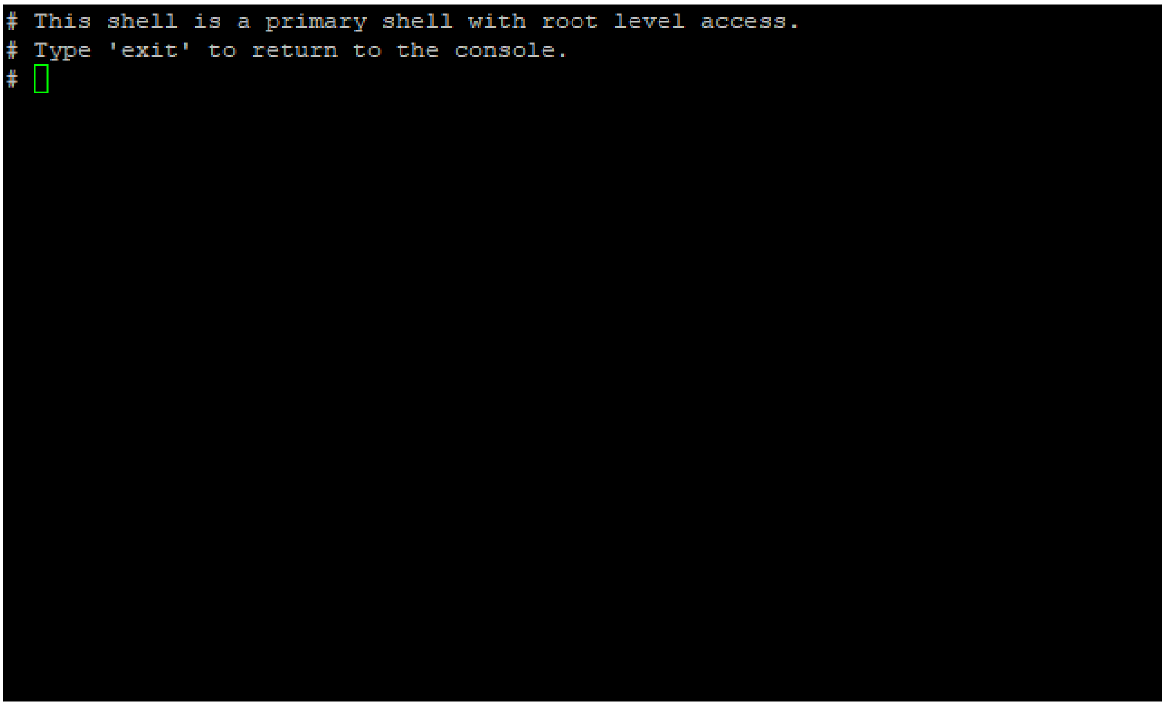
> *Note: By default the SSH password is the same as the value used on the original host. However once logged in to the DR environment it is possible to change this password to a new value with this option.*

9.1.2.4 Open shell

If you need to drop out to a shell select this option.



You will then see the shell window thus.

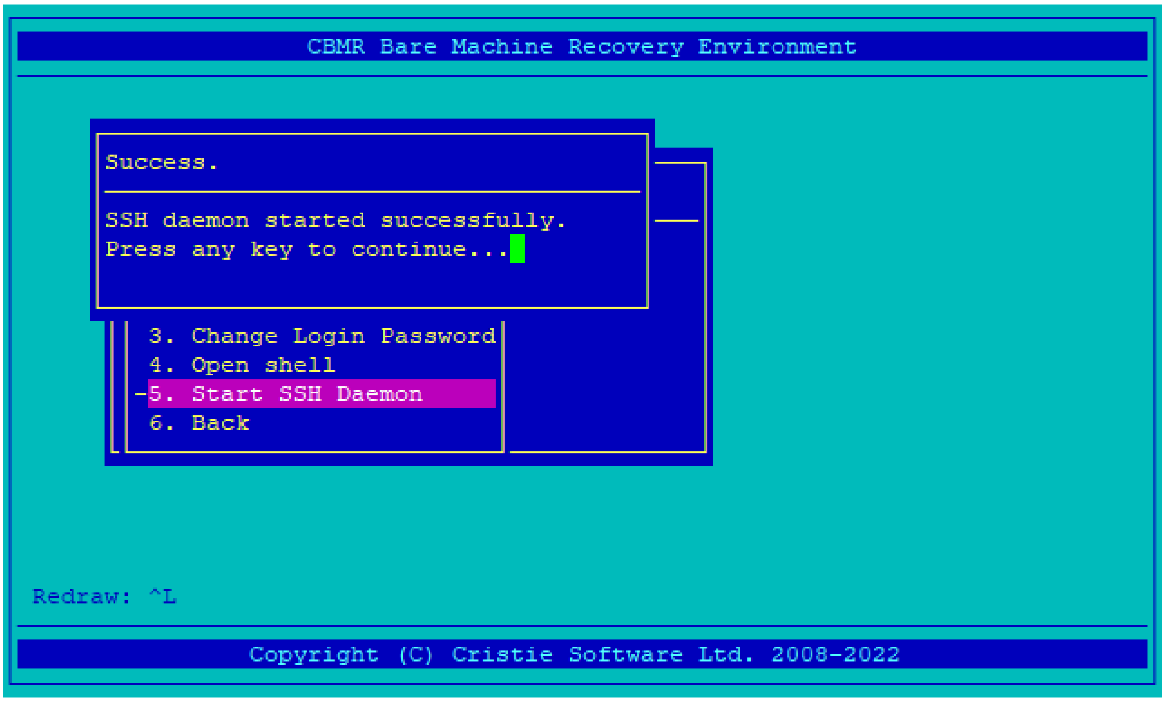


```
# This shell is a primary shell with root level access.
# Type 'exit' to return to the console.
#
```

As stated enter `exit` to return to the Recovery Environment console.

9.1.2.5 Start SSH Daemon

If you require remote SSH access to the Recovery Environment you must first start the SSH daemon. It is not run by default.



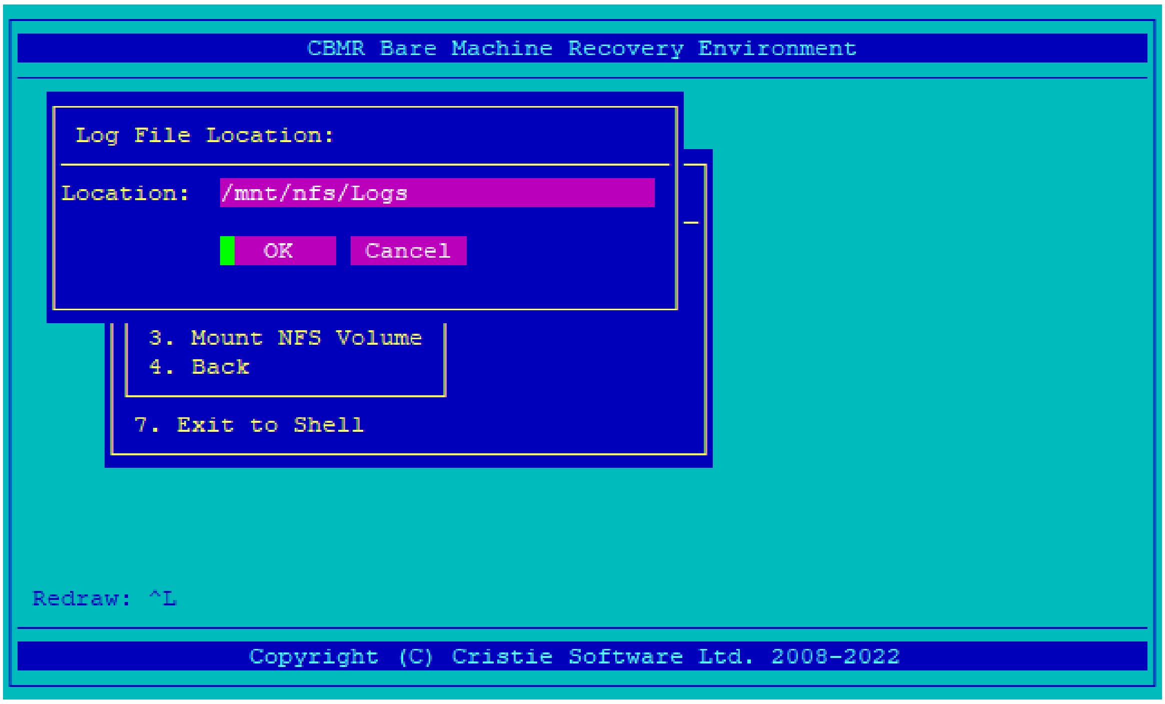
```
CBMR Bare Machine Recovery Environment

Success.

SSH daemon started successfully.
Press any key to continue...

   3. Change Login Password
   4. Open shell
  -5. Start SSH Daemon
   6. Back

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2022
```

Use in conjunction with Change Login Password to set the SSH password.

9.1.3 Copying Log Files

Once the recovery is complete, it is advised that you copy the log files to a suitable location before rebooting the system. It is recommended that you mount an NFS share and copy the log files to that location. These actions are performed using the **'Log Files'** option from the main menu:

The **Copy Log Files** option asks for a location and creates a date-stamped archive of the logs in the directory given.



```
                    CBMR Bare Machine Recovery Environment

  Log File Location:

Location:  /mnt/nfs/Logs

           OK     Cancel

     3. Mount NFS Volume
     4. Back

    7. Exit to Shell



Redraw: ^L

              Copyright (C) Cristie Software Ltd. 2008-2022
```

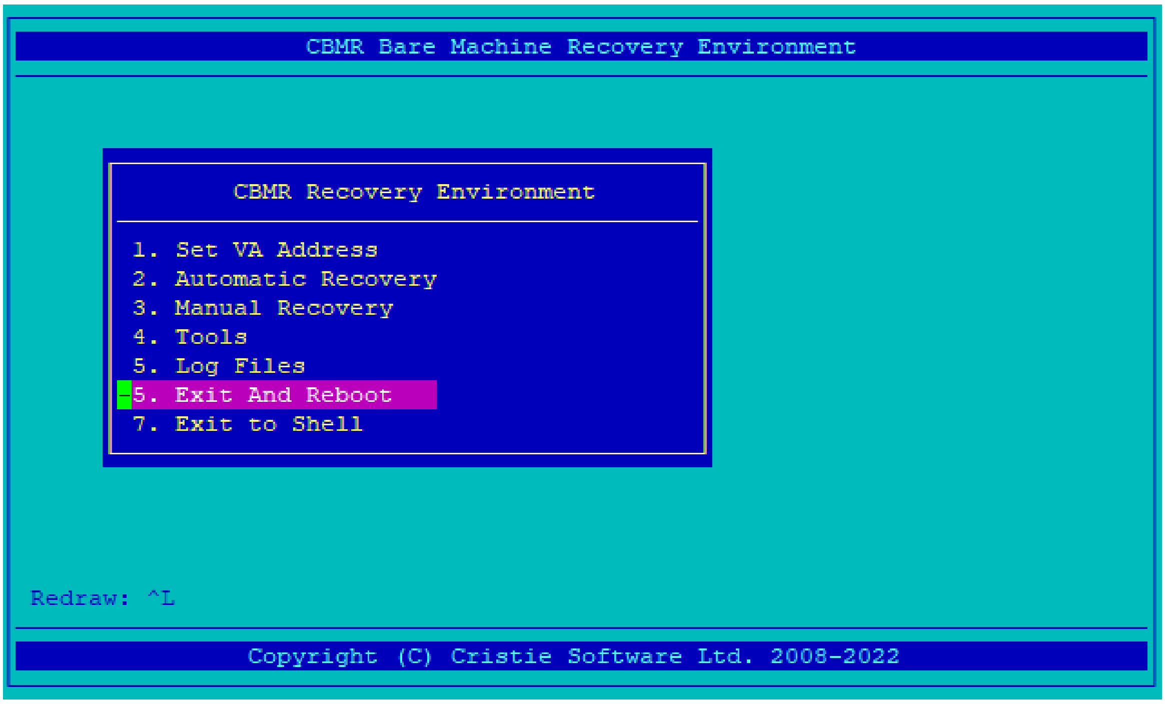
The log files are created with a filename in the form:

```
logs-1756-29112022.tar.gz
```

> *Note: it is important that the directory selected is an NFS mount, as all information in the recovery environment is lost on reboot*

9.1.4 Exit and Reboot

Exit And Reboot will set the boot device to be the disk and reboot the recovered target in one action.



```
                    CBMR Bare Machine Recovery Environment


             CBMR Recovery Environment

    1. Set VA Address
    2. Automatic Recovery
    3. Manual Recovery
    4. Tools
    5. Log Files
    5. Exit And Reboot
    7. Exit to Shell



Redraw: ^L

              Copyright (C) Cristie Software Ltd. 2008-2022
```

9.1.5 Troubleshooting

Recovery:

If the automatic recovery fails at any point, then it may be possible to continue to recover the system by continuing the recovery at the next phase.

For example, if the recovery fails with the following error:

```
Disrec::ERROR "The following commands failed in the last phase run"
...
Disrec::ERROR "Review the logs and correct any errors before proceeding
Disrec::ERROR "to the next phase  (MOUNTING)"
```

Then it *may* be possible to get a working system by running the phases from Mounting until the final phase, MakeBootable.

All phases between Mounting and MakeBootable may be run by selecting **Run Between Two Phases** and selecting the Mounting and MakeBootable phases. If preferred, the phases may be run individually by selecting **Run Single Phase.**

Once the final phase, MakeBootable, has been run then it is possible to reboot the machine. However, we recommend copying log files to an accessible location (to an NFS server for example) before performing the reboot.

Terminal:

The recovery environment uses the terminal 'aixterm' by default. However, for some displays or hardware this is not always appropriate. If the terminal is unusable, for example if the menu-options do not correctly line up, then it may be desirable to change the terminal type. This can be performed by selecting **'Exit to Shell'** and running the environment using a different terminal.

Typing 'terms' produces a list of the terminals available. However, is typically quite long, it may be useful to try one of the following common terminal types first:

- `xterm`
- `vt102`
- `vt100`
- `lft`

For example, typing `'TERM=vt100 dr'` restarts the recovery environment using the vt100 terminal type.

If using **Putty** as the terminal emulator selecting `ISO-8859-1:1998` as the remote character set can help correct character translation issues:

10 Cristie Technical Support

If you have any queries or problems concerning your 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.

11 Appendices

11.1 Snapshots

It is important (from time to time) that a user can take a backup of their Server as it was at a point in time – when they have disconnected all users, halted all required daemons, made a backup of the system that is in a consistent state; so they know they have a reliable and consistent backup they can restore from that was not mid-process. However, such a task could take a while (running into hours, potentially) to complete on a typical system.

Snapshotting enables the user to create a backup with minimal disruption – so maximising uptime without compromising the consistency of the backup. The user would still need to disconnect users and halt all required daemons (otherwise there could be areas mid-update), but running the snapshot will take much less time – typically measured in minutes – it may even be seconds (i.e. less than a minute). Then, once the snapshot is complete, daemons can be restarted, users can be reconnected and the system can go live again – meanwhile CBMR can backup that snapshot whilst the system remains live and in use – all much quicker and much less disruptive.

Provision for handling snapshots comprises 3 scripts, `backup_snapshot`, `verify_snapshot` and `restore_snapshot`.

Creation

Snapshots are created using the `backup_snapshot` script. Snapshot backups will be written to the default backup location. This location can be modified by using the program, `gubax` or within `cbmr`, prior to running the script. A recovery ISO should be created at this stage.

After setting the backup location, exit `gubax` or `cbmr` and at the command line enter `backup_snapshot`.

The user is allowed to pass 3 flags to `backup_snapshot` :

-d ... force destruction of snapshots created by this script
-k ... keep all snapshots created by this script
-s .. change snapshot location from the default `/mnt/snaps` if the directory does not exist it will be created.
-p ... percentage of original filesystem size to use for backup

If no percentage is passed to the script, then half of the free physical partitions will be used, by default.

If a parameter is passed, it will be used as the root filesystem location for the snapshot. Otherwise a default of `/mnt/snaps` is used.

A snapshot will be taken of each file system. This 'tree' of snapshots will be mounted at the snapshot root file location. ubax is then invoked using this snapshot root file location.

By default, the snapshots are removed after the backup is completed, though the snapshots may be kept if the appropriate parameter is passed to the script.

If a snapshot is kept using the `-k` parameter it will be created in the default location `/mnt/snaps`. A further attempt to create a snapshot using `backup_snapshot` will fail as the snapshot already exists.

It is highly recommended that if a snapshot is to be kept then initiate the backup using both -k and -s for example:-

```
   backup_snapshot -k -s /mnt/mysnapshot
```

Verification

Verification of the snapshot is provided by the `verify_snapshot` script. There is no user input available.

Restoration

Boot into the recovery ISO created earlier. Within the recovery environment configure the backup location then exit to a shell.

Restoration of the snapshot is provided by the `restore_snapshot` script. There is no user input available.

After a successful recovery a prompt to reboot will be displayed. This can actioned either by rebooting from the command line or exit from the shell and select reboot from the menu.

.