



## **Recovery Assurance**

with Cristie Recovery Software

# **CBMR**

## **Cristie Bare Machine Recovery**

# **Quick Start Guide** **For Solaris**

**April 2019**

**Version 8.5**

Cristie Software Ltd.  
New Mill  
Chestnut Lane  
Stroud GL5 3EW  
United Kingdom  
Tel: +44(0)1453 847000  
Fax: +44(0)1453 847001  
support@cristie.com

Cristie Data Products GmbH  
Nordring 53-55  
  
63843 Niedernberg  
Germany  
Tel: +49 (0) 60 28/97 95-0  
Fax: +49 (0) 60 28/97 95 7-99  
cbmr@cristie.de

Cristie Nordic AB  
Knarramäsgatan 7  
164 40 Kista  
Sweden  
Tel: +46(0)8 718 43 30  
cbmr@cristie.se

**Copyright © 2013-2019 Cristie Software Ltd.  
All rights reserved.**

The software contains proprietary information of Cristie Software Ltd.; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between Cristie Software Ltd. and the client and remains the exclusive property of Cristie Software Ltd. If you find any problems in the documentation, please report them to us in writing. Cristie Software Ltd. does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of Cristie Software Ltd.

IBM Tivoli Storage Manager (TSM), AIX and TIVOLI are trademarks of the IBM Corporation.

IBM Spectrum Protect is a trademark of the IBM Corporation.

IBM Virtual I/O Server (VIOS) is a trademark of the IBM Corporation.

NetWorker and Avamar are trademarks of the Dell EMC Corporation.

vSphere, vCenter and vCloud are trademarks of VMware Inc.

Hyper-V is a trademark of Microsoft Corporation.

Azure is a trademark of Microsoft Corporation.

Amazon Web Services (AWS) and Amazon Elastic Compute Cloud (EC2) are trademarks of Amazon.com, Inc.

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), Recovery Simulator (RS) 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](mailto:support@cristie.com)**

# Contents

<b>1</b>	<b>Document conventions</b>	<b>5</b>
<b>2</b>	<b>About CBMR for Solaris</b>	<b>6</b>
<b>3</b>	<b>System Requirements</b>	<b>7</b>
<b>4</b>	<b>Installation</b>	<b>8</b>
	4.1 Checking Prerequisites .....	8
	4.2 Installing Files .....	8
	4.3 License .....	9
	4.4 Uninstall .....	9
	4.5 Zones .....	9
<b>5</b>	<b>Product Licensing</b>	<b>10</b>
	5.1 Trial License .....	10
	5.2 Full License .....	11
	5.2.1 Setting up a Cristie Licensing Portal account .....	11
	5.2.2 Manual Activation .....	13
	5.2.3 Online Activation .....	14
<b>6</b>	<b>Creating a Recovery Image</b>	<b>16</b>
	6.1 Creating a Recovery CD ISO .....	17
	6.2 Creating a Recovery Miniroot .....	18
	6.3 Adding Additional Drivers .....	18
	6.4 Create CD from Miniroot .....	19
<b>7</b>	<b>Performing a DR backup</b>	<b>20</b>
	7.1 Recording System Information .....	20
	7.2 Configure the Backup Location .....	22
	7.2.1 Configuring a Backup Location using the GUBAX User Interface .....	22
	7.3 Selecting the Directories to be backed up .....	29
	7.3.1 Viewing the current backup selection .....	29
	7.3.2 Editing the current backup selection .....	30
	7.3.3 Saving the current backup selection .....	31
	7.4 Performing the Backup .....	31
<b>8</b>	<b>Performing a Recovery</b>	<b>33</b>
	8.1 Starting the Recovery Environment .....	33
	8.2 Automatic Recovery Wizard .....	35
	8.2.1 Drive Mapping .....	39
	8.2.2 Set IBM Spectrum Protect SSL Certificate .....	40
	8.2.3 Start Recovery .....	42

8.2.4 Copy Logs .....	43
<b>8.3 Manual Recovery .....</b>	<b>43</b>
<b>8.4 Post Recovery Steps .....</b>	<b>47</b>
<b>8.5 Copying Log Files .....</b>	<b>48</b>
<b>8.6 Troubleshooting .....</b>	<b>50</b>
<b>9 Cristie Technical Support .....</b>	<b>51</b>

# 1 Document conventions

The following typographical conventions are used throughout this guide:

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

## 2 About CBMR for Solaris

CBMR for Solaris provides a file-based backup and disaster recovery (DR) system for Solaris 9, 10 and 11 on Sparc and Solaris 10 and 11 (excluding 11.4) on Intel (64-bit only).

The process of backing up and recovering a Solaris machine comprises three steps:

1. Create a bootable recovery environment from the running machine
2. Perform the Disaster Recovery (DR) backup
3. Perform the recovery

Steps 1 and 2 of the above actions may be performed using the Graphical User Interface run from the command `cbmr`. Step 3 is performed using the DR environment created from step1. Documentation describing command line tools with the same functionality is also included, allowing you to easily create scheduled and 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

CBMR for Solaris supports Solaris 9, 10 and 11 on Sparc hardware and Solaris 10 and 11 on Intel hardware.

**Note: Solaris 11.4 Intel is not supported by CBMR.**

CBMR requires the following minimum hardware requirements:

<b>Disk Space</b>	16MB
<b>Memory</b>	256MB

CBMR for Solaris supports the following:

Platform	Sparc			Intel (64-bit)	
Solaris Version	9	10	11	10	11 (excluding 11.4)
IBM Spectrum Protect Client Version	5.5 only	6.3.x to 7.1.8		6.3.x to 8.1.6.1	
IBM Spectrum Protect Server Version	6.3.x to 8.1.6.0				
Veritas Storage Foundation	5.0 - 6.1				

#### Prerequisites

Name	Version	Sun Package	Open Source Package
Libxml2	2.4.23	SUNWlxml	SMClxml2
Mkisofs	2.01	SUNWmkcd	SMCcdrt
Programming Tools	Any	SUNWtoo	-

These tools are included in modern Solaris distributions and, for the open source packages, on the installation media. In this case, package installations are independent so both may be installed simultaneously.

## 4 Installation

On default installations of Solaris 9, 10 and 11, all of the necessary prerequisites should be available.

However, if a minimal installation was performed or if an earlier operating system is in use, then the prerequisites must be checked.

### 4.1 Checking Prerequisites

The `pkginfo` tool may be used to determine whether a package is installed and the `pkgchk` tool can verify the files for the given package are correct. For example:

```
> pkginfo SUNWmkcd
> pkgchk SUNWmkcd
```

Additionally, the CBMR installation media contains a '[checkpackages.sh](#)' script, which will attempt to determine whether the necessary files are installed:

```
> cd ./cbmr-8.5.2020/
> ./checkpackages.sh
```

Finally, it is recommended that the core system files are also checked, as these are required to build the recovery environment. This can be performed by checking the core Solaris package:

```
> pkgchk -n SUNWcsr
```

### 4.2 Installing Files

CBMR can be installed using the Solaris packaging system. After unpacking the archive or mounting the CD to a directory, change to this directory using '`cd`' then the following command will install CBMR 8.5 for Solaris:

```
> pkgadd -G -d ./CSTEcblr-8.5.2020-i86pc.pkg
for Intel machines
```

and

```
> pkgadd -G -d ./CSTEcblr-8.5.2020-sparc.pkg
in the case of Sparc hardware
```

**Note:** If you wish to create backups to IBM Spectrum Protect, it is recommended that the IBM Spectrum Protect backup client is installed prior to installing CBMR. This way CBMR will be installed with the appropriate IBM Spectrum Protect support.

This release of CBMR is not able to **upgrade** an existing installation (say version 7.5.1). You must first uninstall the existing version and then install this latest version. If you wish to preserve your current settings during this process (e.g. Backup Location definitions), you should first save these settings and then re-instate after the new installation is complete.



## 4.3 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 licence, you will have been sent an activation code, these can be used to activate the product with the `licmgr` tool as follows:

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

More information about the `licmgr` tool can be found by typing '`man licmgr`'.

## 4.4 Uninstall

The package may be uninstalled by running the following command:

```
>pkgrm CSTEcbmr
```

## 4.5 Zones

As Solaris **Zones** are not bootable from installation media, CBMR is not applicable to Zone backup *inside* a zone. However, all Zones may be fully backed up and restored with the host operating system.

## 5 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.

### 5.1 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 achieved by opening up a terminal and entering:

```
#  
# licmgr -p cbmr
```

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

```
=====
                        Cristie License Manager Version
                          X.X
                Copyright (C) 2012-2019 Cristie Software Limited
=====
Machine attributes : {virtual, server}
  Contract ID : 0
    Signature : EKSEWPSC-L3AF7EWW-DFY9GH69-5Z48W7PJ
      Product : Bare Machine Recovery for XXXXXXXX (XBMR)
      Version : X.X
    Trial ends on : 2019-03-24

                Status : Trial licence
```

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

## 5.2 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 either via the Cristie Licensing Portal website or via the product Cristie License Manager. In either case 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.

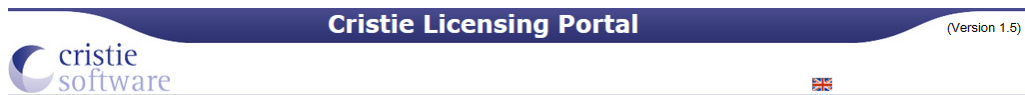
*Note this discussion assumes that CBMR is already installed on a Customer production machine.*

### 5.2.1 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 (e.g. Microsoft Internet Explorer on Windows or say Firefox on UNIX) and navigate to the Cristie Licensing Portal web page at <https://portal.cristie.com/login>. If accessing the internet on a Solaris machine use the the available installed browser.



**Log in**

User E-mail:

Password:

[Log in](#) [Register](#)

[Forgot Password?](#)



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

**Cristie Licensing Portal** (Version 1.5)

**Register a new user**

E-mail ID:  \*

User Name:  \*

Password:  \*

Confirm password:  \*

Password reset question:  \*

Password reset answer:  \*

Contract/Agreement No.:  \*

Contract Password:  \*

Address:  \*

City:  \*

Zip or Postal Code:  \*

State or County:  \*

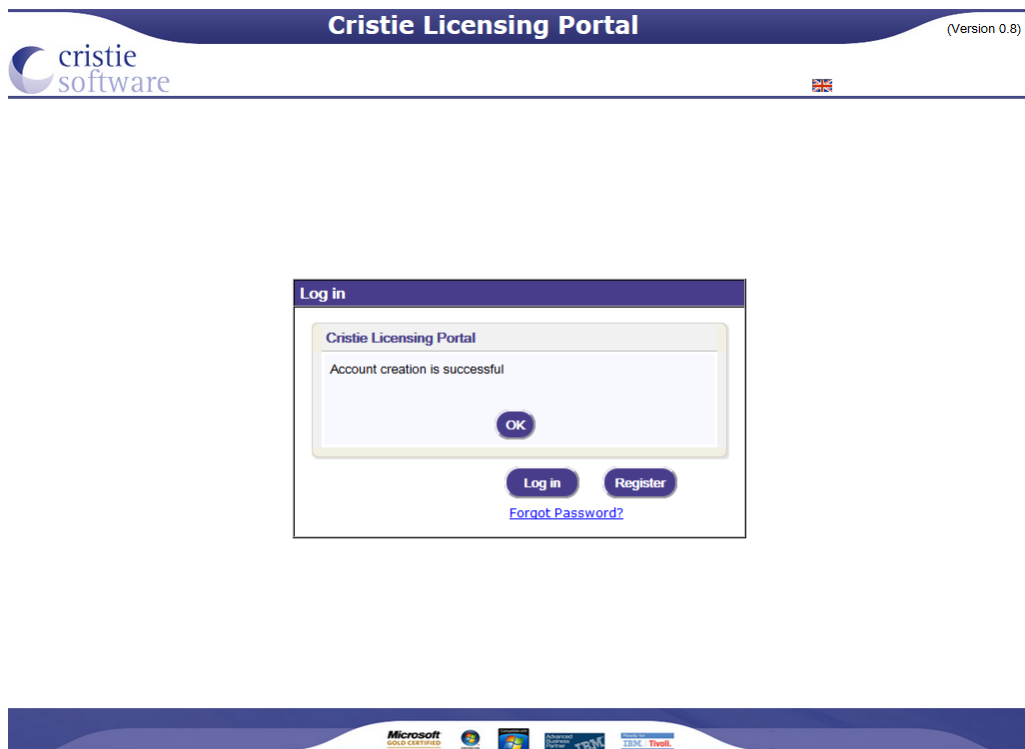
Country:  \*

Fields with a \* are mandatory

[Create](#) [Cancel](#)

Footer: Microsoft Gold Certified Partner, IBM, Godaddy Verified & Secured.

3. Then click **Create**. If successful the following is shown.



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.

### 5.2.2 Manual Activation

The steps involved in manual activation using the Cristie Licensing Portal are as follows. This discussion assumes your contract is already setup on the Cristie Licensing Portal.

1. Licence CBMR by entering the command:

```
#
# licmgr -p cbmr --act xxxxxxxx-xxxxxxx-xxxxxxx-xxxxxxx
```

(where xxxxxxxx-xxxxxxx-xxxxxxx-xxxxxxx is your Activation code, which can be obtained by signing into the Cristie Licensing Portal) and activating a license for this server. You will require the machine IP address, hostname and machine signature to do this. Use the command `licmgr -p cbmr` to get the signature.

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

```
=====
Cristie License Manager Version
X.X
Copyright (C) 2012-2019 Cristie Software Limited
=====
Successfully applied the activation code.
Machine attributes : {virtual, server}
Contract ID : 1
Signature : EKSEWPSC-L3AF7EWW-DFY9GH69-5Z48W7PJ
Product : Bare Machine Recovery for XXXXXXXX (XBMR)
Version : X.X
Maintenance ends on : 2019-12-31

Activation code : XXXXXXXX-Z94ABKH9-UFWKN2BD-R3CCJB53
Activation type : Product activation
Maintenance ends on : 2019-12-31
Attributes : {virtual, server}

Status : Full licence
```

### 5.2.3 Online Activation

The steps involved in activating the product automatically using the Cristie License Manager are summarised below. This discussion assumes your contract is already setup on the Cristie Licensing Portal and you have access to both Contract and Activation codes.

1. Assign your Contract code on the CBMR host machine, by opening up a terminal and entering:

```
# licmgr -p cbmr --cid xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
```

(where xxxxxxxx-xxxxxxx-xxxxxxx-xxxxxxx is your Contract code)

```
=====
Cristie License Manager Version
X.X
Copyright (C) 2012-2019 Cristie Software Limited
=====
Successfully set the contract ID.
Machine attributes : {virtual, server}
Contract ID : 1
Signature : EKSEWPSC-L3AF7EWW-DFY9GH69-5Z48W7PJ
Product : Bare Machine Recovery for XXXXXXXX (XBMR)
Version : X.X
Trial ends on : 2019-03-24

Status : Trial licence
```

2. Then activate the license online CBMR by entering the command:

```
# licmgr -p cbmr --cred user@example,password
```

(The required email and password are the ones you use to sign into the Cristie Licensing Portal)

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

```
=====
                        Cristie License Manager Version
                          X.X
                Copyright (C) 2012-2019 Cristie Software Limited
=====
Connecting with: 'xxxxxxxxxxxxxxxxxxxx@xxxxxxxx.com' and 'xxxxxxxxxxxxx'
Licensing machine: 'EKSEWPSC-L3AF7EWW-DFY9GH69-5Z48W7PJ'
Details: 'jn-source' on '10.1.4.197' (Virtual)
Activating using code: XXXXXXXX-XXXXXXX-UFWKN2BD-R3CCJB53
Success

Machine attributes : {virtual, server}
Contract ID : 1
Signature : EKSEWPSC-L3AF7EWW-DFY9GH69-5Z48W7PJ
Product : Bare Machine Recovery for XXXXXXXX (XBMR)
Version : X.X
Maintenance ends on : 2019-12-31

Activation code : XXXXXXXX-XXXXXXX-UFWKN2BD-R3CCJB53
Activation type : Product activation
Maintenance ends on : 2019-12-31
Attributes : {virtual, server}

Status : Full licence
```

*Note: Internet access on the host machine is required to run the online activation process from the Cristie License Manager directly.*

If you see the error "Failed to initialise SSL" with the reason "unable to get local issuer certificate" then this means that a bundle of Certificate Authority root certificates is missing. This is a frequent problem with Solaris installations and is easily solved.

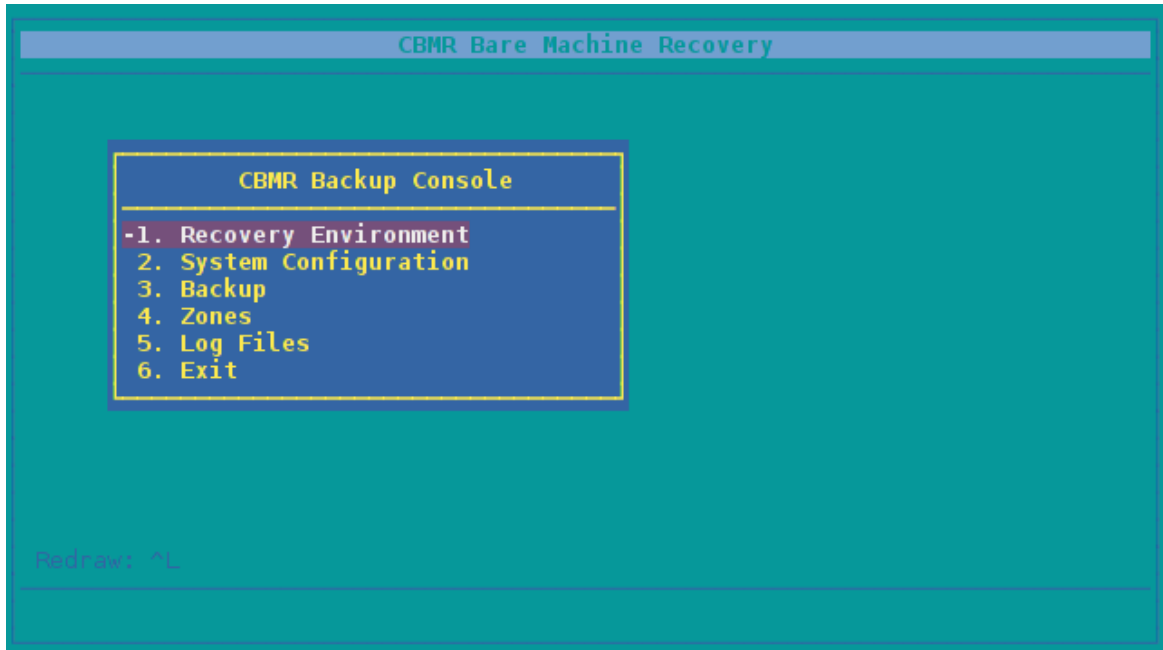
Linux machines contain a copy of the Mozilla CA root certificate bundle. It is therefore possible to copy `"/etc/pki/tls/cert.pem"` from any Linux machine into `/etc/cristie/cacert.pem` on the Solaris machine. Alternatively, this file is made available for download as part of the "CURL" project here: <http://curl.haxx.se/ca/cacert.pem>.

More information can be found about the Certificate Authorities trusted in this file on the Mozilla website here:

<https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/included/>

## 6 Creating a Recovery Image

All functionality can be accessed through the **CBMR Graphical User Interface**. After entering the command 'cbmr', select Recovery Environment from the **CBMR Backup Console** main menu:



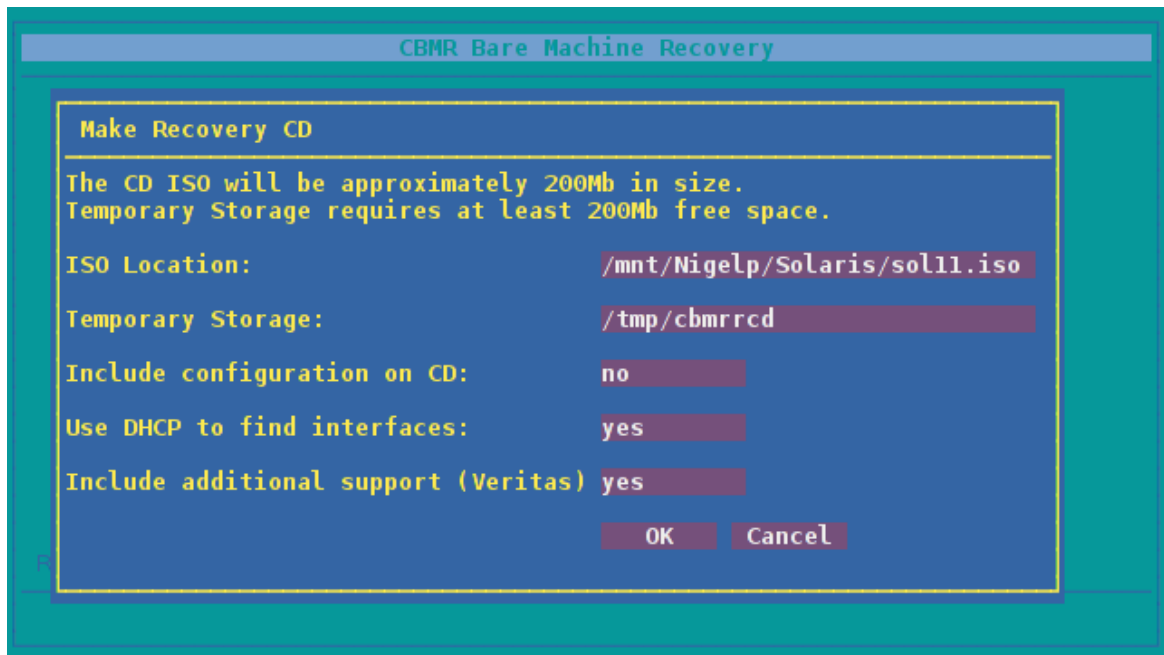
Then select **Make Recovery CD**:



The first step is to create a recovery CD or PXE/Jumpstart bootable image. This is an image that can either be burned to CD to boot the recovery environment, or extracted to create a network boot environment.

The creation of recovery media is performed by opening the **Make Recovery CD** menu.





This menu presents various options for creating the recovery environment:

- **Make Recovery CD** - create an ISO image that can be burned to a CD
- **Make Recovery Miniroot** - create a miniroot file for PXE or Jumpstart booting
- **Add driver to image** - add an extra driver to support hardware not on the CD
- **Create CD from Miniroot** - create a bootable ISO from a miniroot file

*Note: the recovery image uses only files from the running system and only uses files required for recovering that system. Therefore, a new ISO should be created for each processor architecture and Solaris version*

Additionally, this means that if the hardware to be restored to contains a storage controller or network card requiring additional drivers not present on the previous machine, these drivers will have to be added to the image.

## 6.1 Creating a Recovery CD ISO

The '**Make Recovery CD**' option creates an ISO image that can be burned to a CD using a tool such as `cdrecord`:

```
> cdrw -i /tmp/dr.iso
```

This also provides the option to include the configuration information on the CD. This will allow the recovery process for this machine to begin immediately once the backup has been located

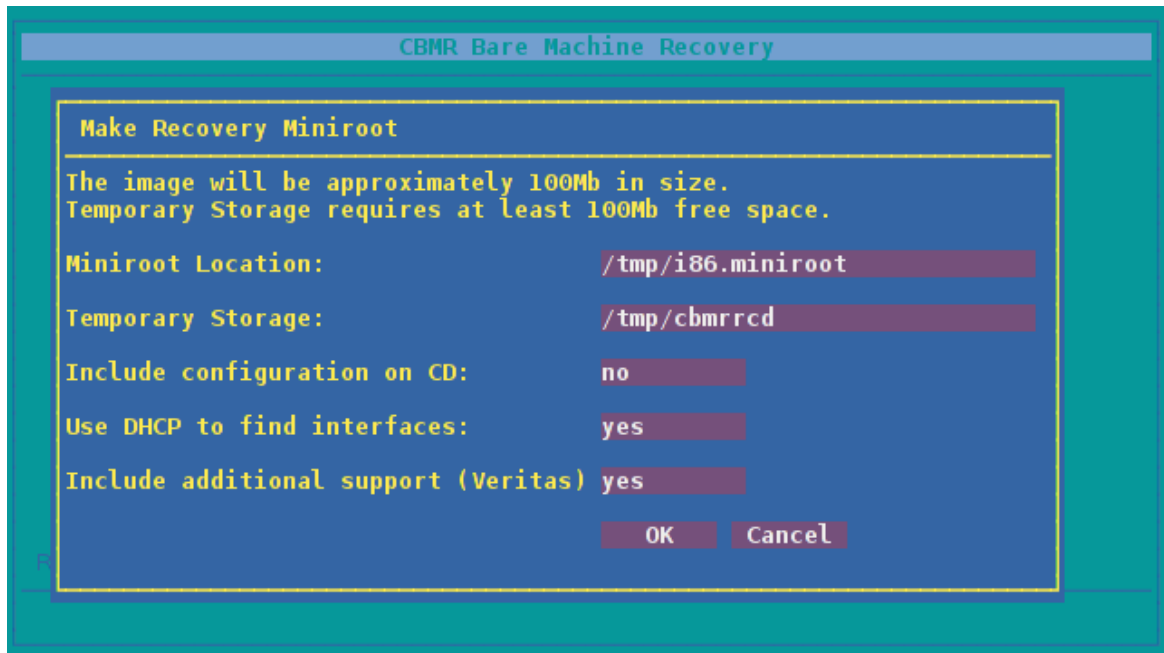
*Note: the output log for CD creation is saved in '/var/log/cristie/mkdracd.log'*

## 6.2 Creating a Recovery Miniroot

The '**Make Recovery Miniroot**' option performs the same function as 'Make Recovery CD', except it creates a `x86.miniroot` or `sparc.miniroot` file, depending on the machine architecture.

This file can be used to network boot the machine over jumpstart or PXE.

Detailed instructions on how to setup PXE and jumpstart booting are available in additional documentation.

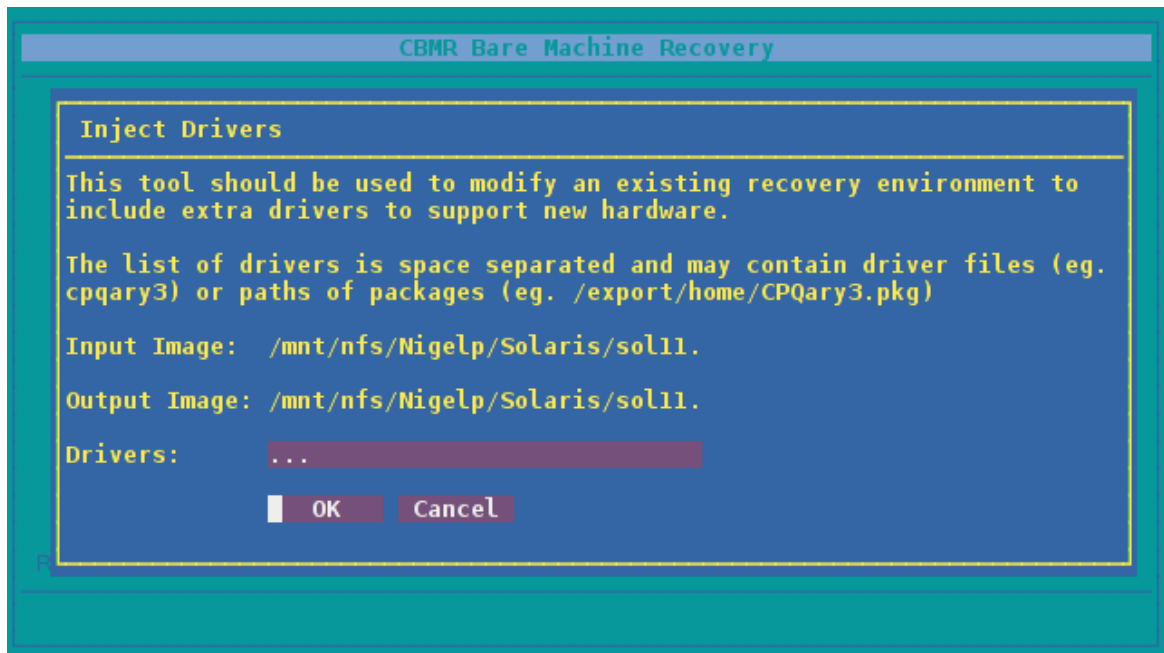


The miniroot dialogue presents the same options as the CD dialogue.

## 6.3 Adding Additional Drivers

The recovery environment created provides only those drivers present on the machine upon which it was created.

Therefore, if the machine is being restored to different hardware with storage controllers or network cards requiring drivers not present on the original machine, then additional drivers must be installed.

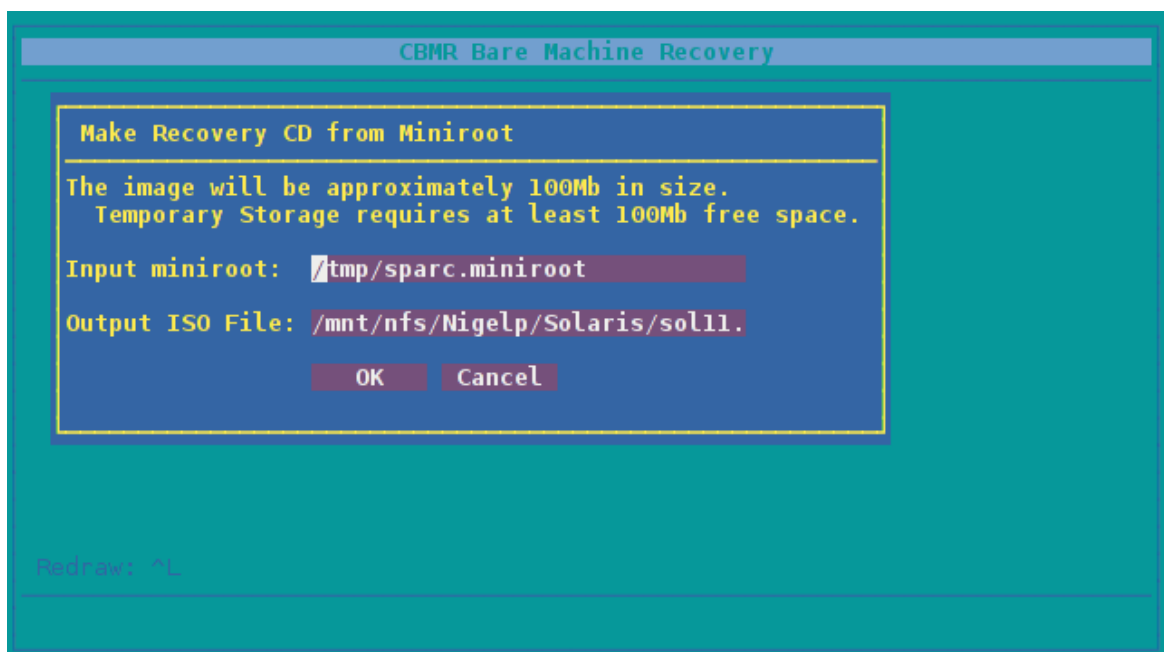


The drivers can be injected either from the running system (eg. 'cpqary3') or may be a path to a package file (eg. '/export/home/CPQary3.pkg'). It is recommended that the latter form is used wherever possible, as packages may install additional files or modify system files that cannot be picked up by examining the system driver database.

*Note: the machine used to inject the driver does not have to match the machine the CD was built on. It is only required that the driver will function on the intended hardware*

## 6.4 Create CD from Miniroot

This option provides a method to create a CD ISO file from a miniroot file



## 7 Performing a DR backup

Performing a DR backup is split into two stages:

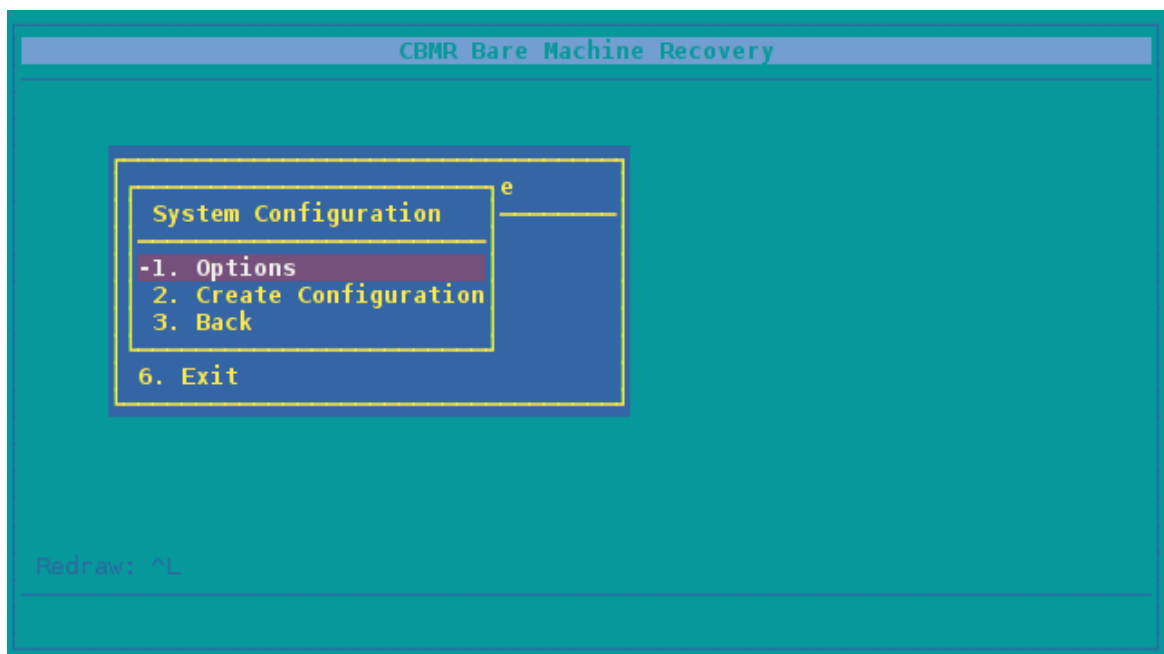
1. Record system configuration
2. Perform the backup using GUBax or Ubax

The system information is recorded to allow the recovery environment to recreate the original system environment. This will include drive and file-system information, as well as information about essential packages for rebuilding the system.

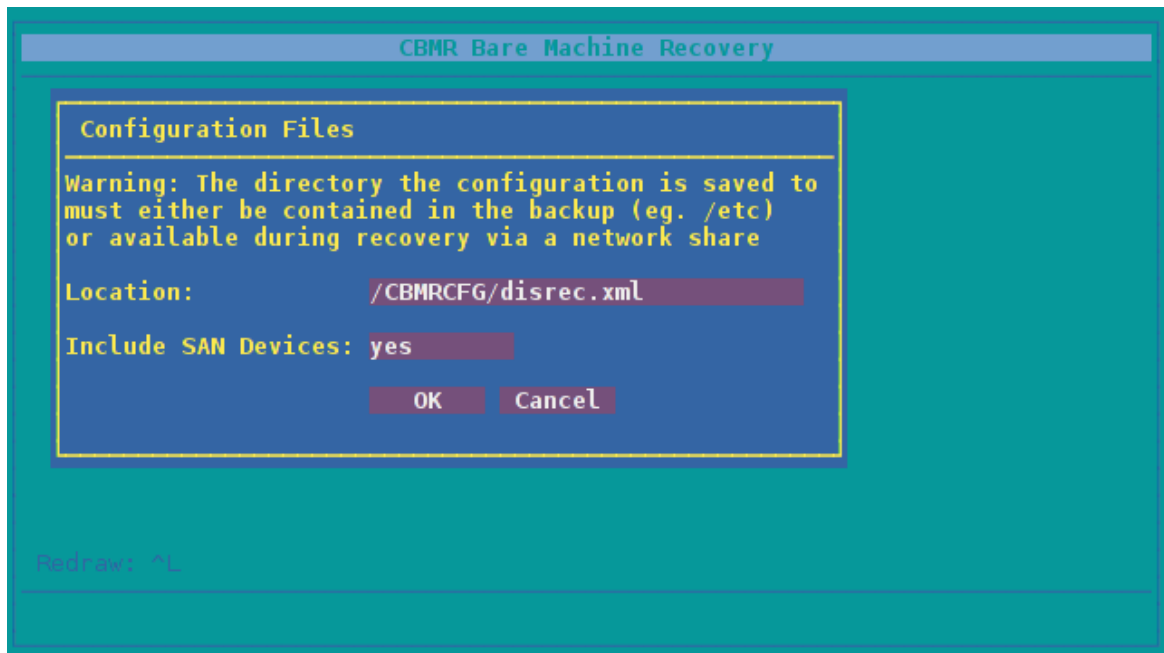
### 7.1 Recording System Information

The system information must be recorded and stored so that the system can be rebuilt at recovery time. This is performed using the `cbmr cfg` tool, available through the **System Configuration** option of the **cbmr Backup Console**.

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

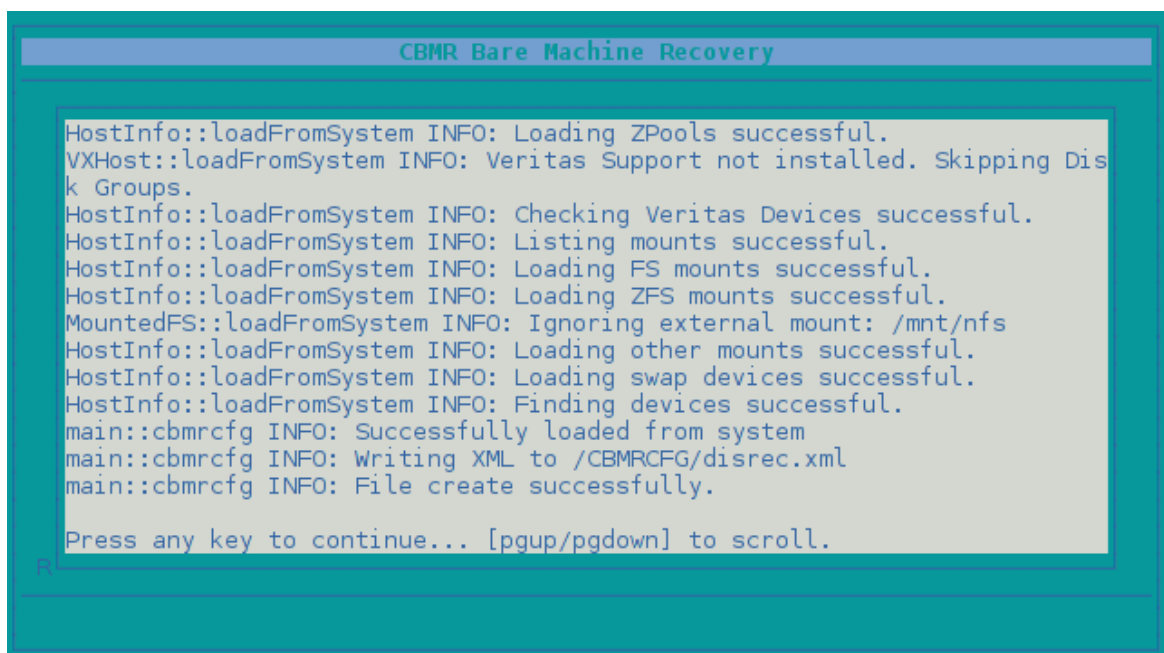


The default location of the configuration information is `/CBMRCFG/disrec.xml`. However, the **Set Location** option will allow you to select a different location if desired.



*Note: the location chosen MUST be included in the file paths specified to be included in the backup. If you change the location of the configuration information, ensure this is included in the backup.*

When running the configuration tool information, the current operations will be displayed:



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

## 7.2 Configure the Backup Location

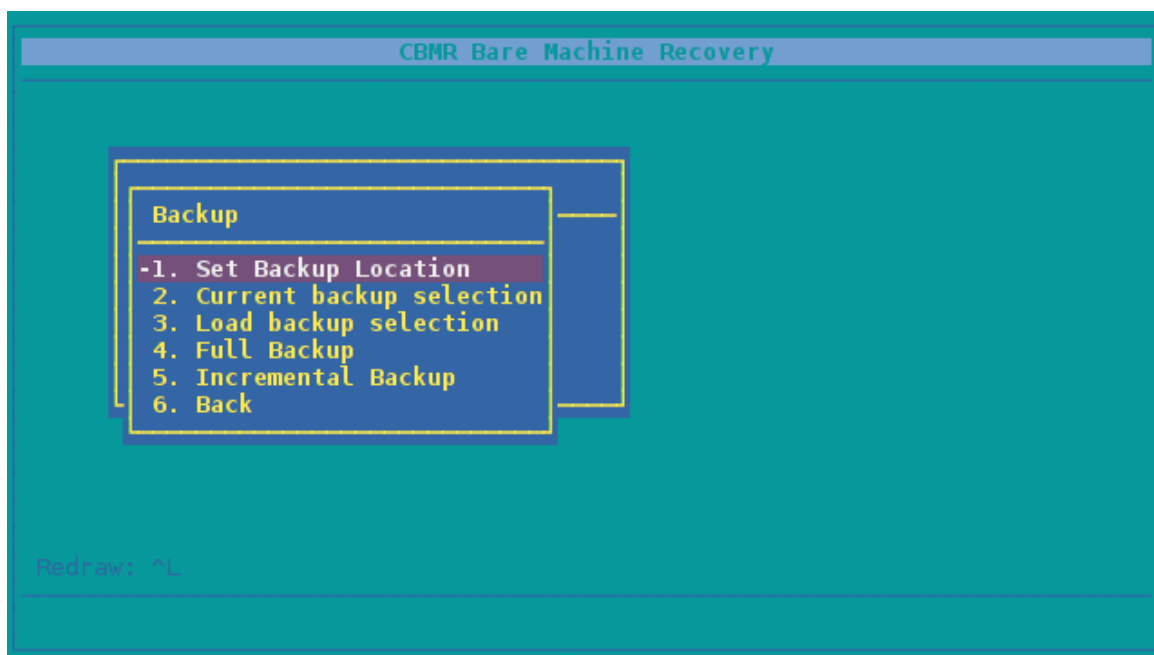
A **Backup Location** is a definition of the entity to which you will backup data. CBMR can backup to tape drives, tape libraries, files, IBM Spectrum Protect nodes and cascaded locations.

All backup functionality may be accessed via the Backup option from the gubax main menu. This provides functionality to change the location of the backup (ie. file, 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.

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

### 7.2.1 Configuring a Backup Location using the GUBAX User Interface

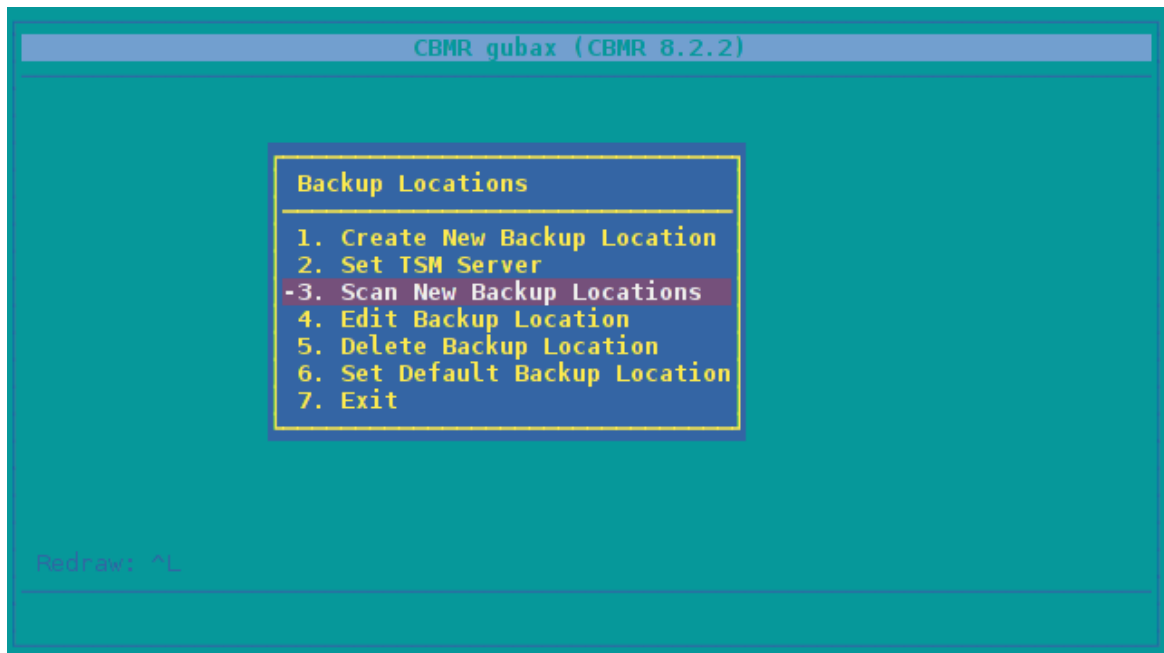
The **Graphical User Interface**, GUBAX, can be accessed either by selecting **Set Backup Location** from the CBMR tool or by running gubax at the command prompt. This example shows the cbmr being used which, in turn, calls gubax..



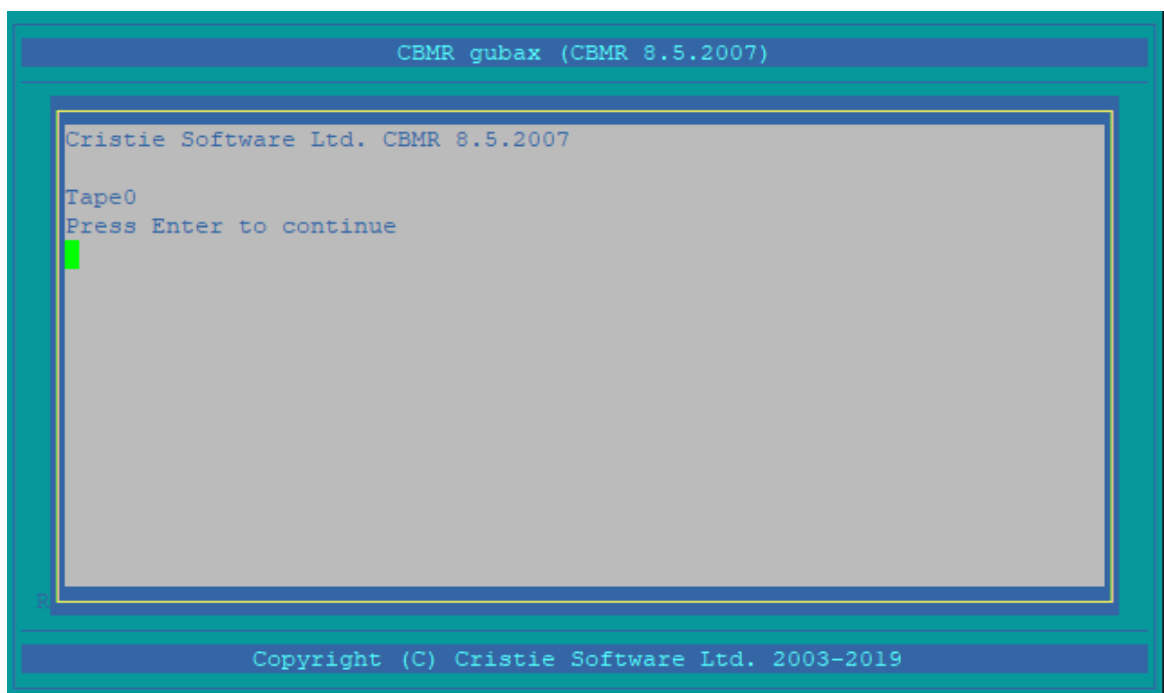
The GUBAX menu provides the ability to create, modify and delete file, tape and IBM Spectrum Protect backup locations.

#### Tape Drives

If you are using a tape drive, this can be automatically detected by selecting the **Scan New Backup Location** option from the device menu.



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

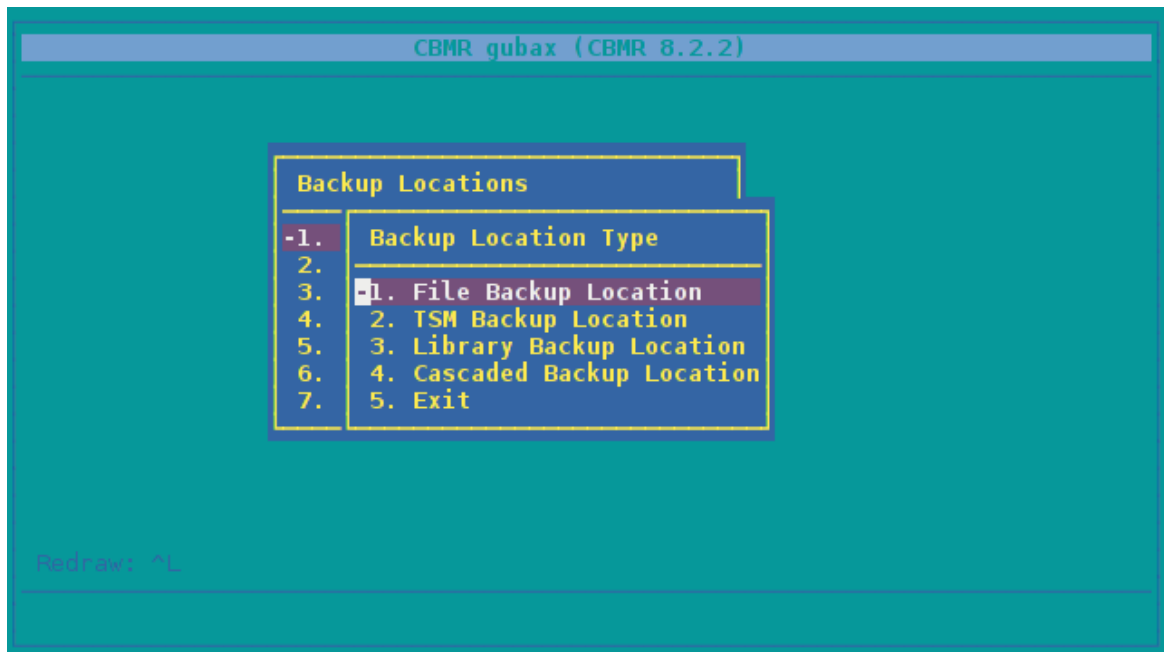


Other types of device should be configured manually by selecting **Create New Backup Location** from the device menu.

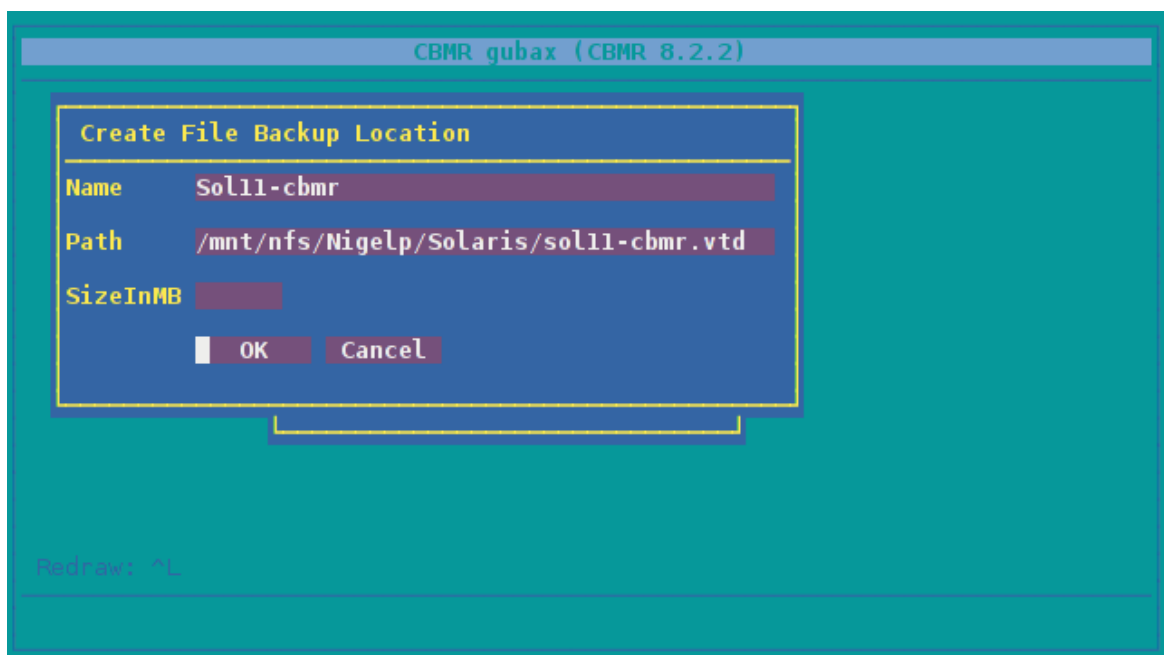
The menu presented allows creation of File, IBM Spectrum Protect, Tape Library and cascaded devices.

### File Backup Locations

A File 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 **file**.

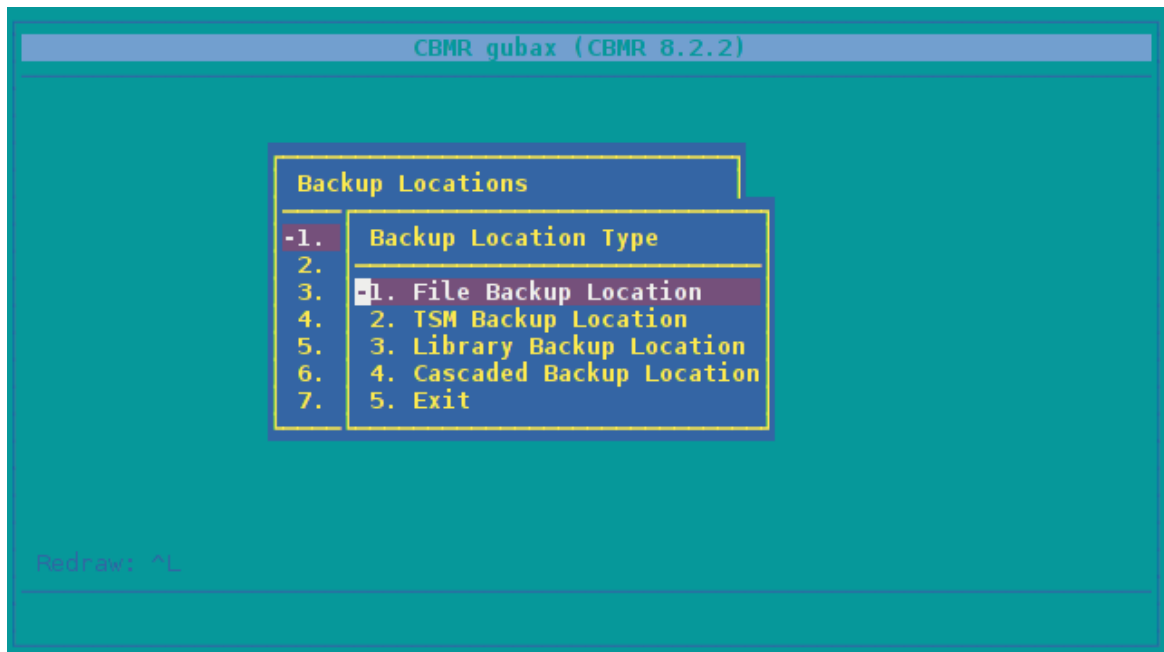


It is recommended that you leave both **SizeInMB** and **Remote** fields blank or set to zero. SizeInMB sets a maximum size for the file - by leaving this blank it will allow it to expand until the backup is complete or there is no more space on the disk. The Remote field is used to indicate that **Cristie Storage Manager** is being used.

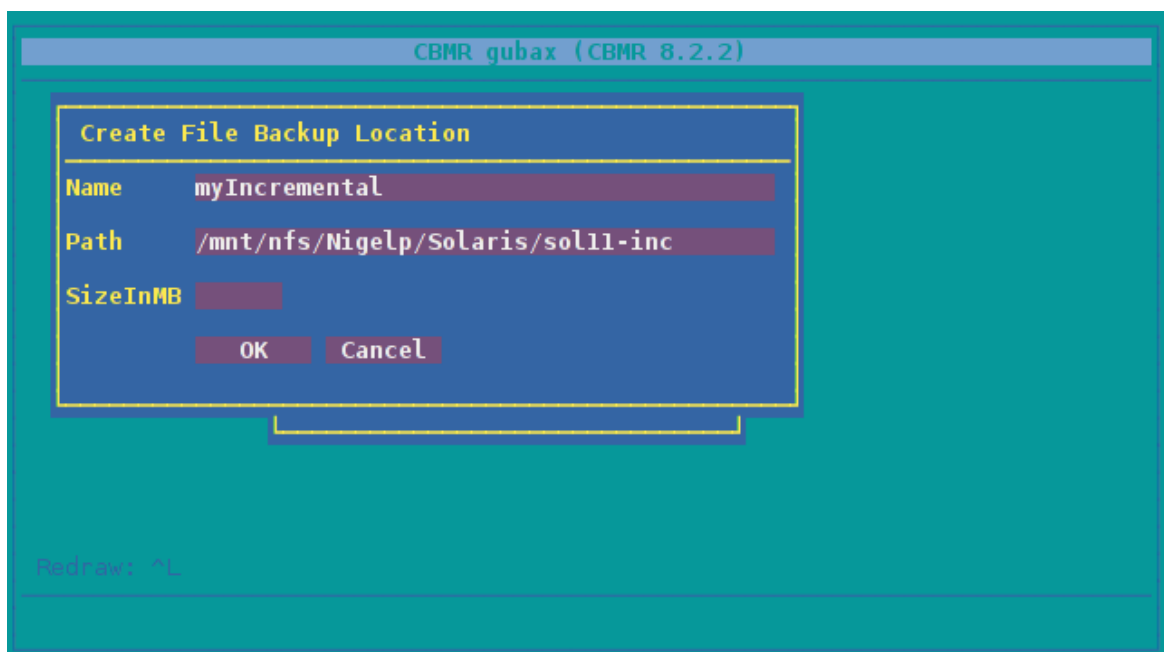
### Incremental File Backup Locations

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:





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

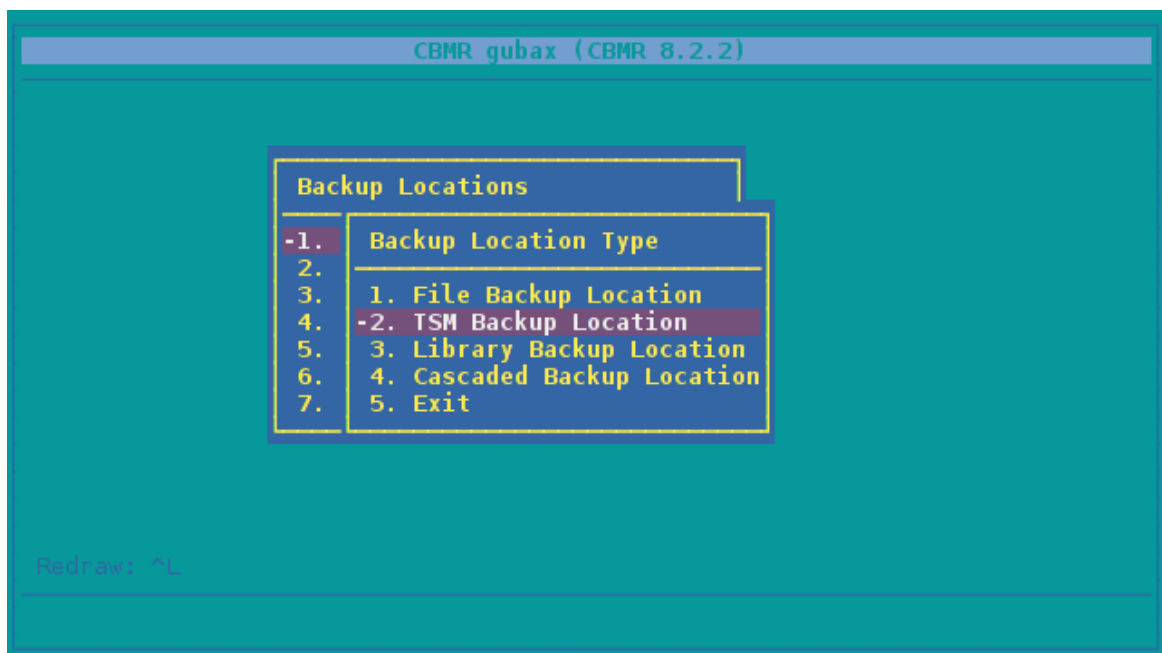
A IBM Spectrum Protect (formerly TSM) node is a port to a network storage system. Currently, CBMR treats a node as though it were a tape. This means that there are some restrictions to the way in which CBMR can be configured and used with IBM Spectrum Protect.

The node must be reserved for **sole** use by CBMR and may not be shared with any other

process - particularly the IBM Spectrum Protect 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 **TSM 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:

The screenshot shows the CBMR gubax (CBMR 8.2.2) interface. A form titled "Create TSM Backup Location" is displayed with the following fields and values:

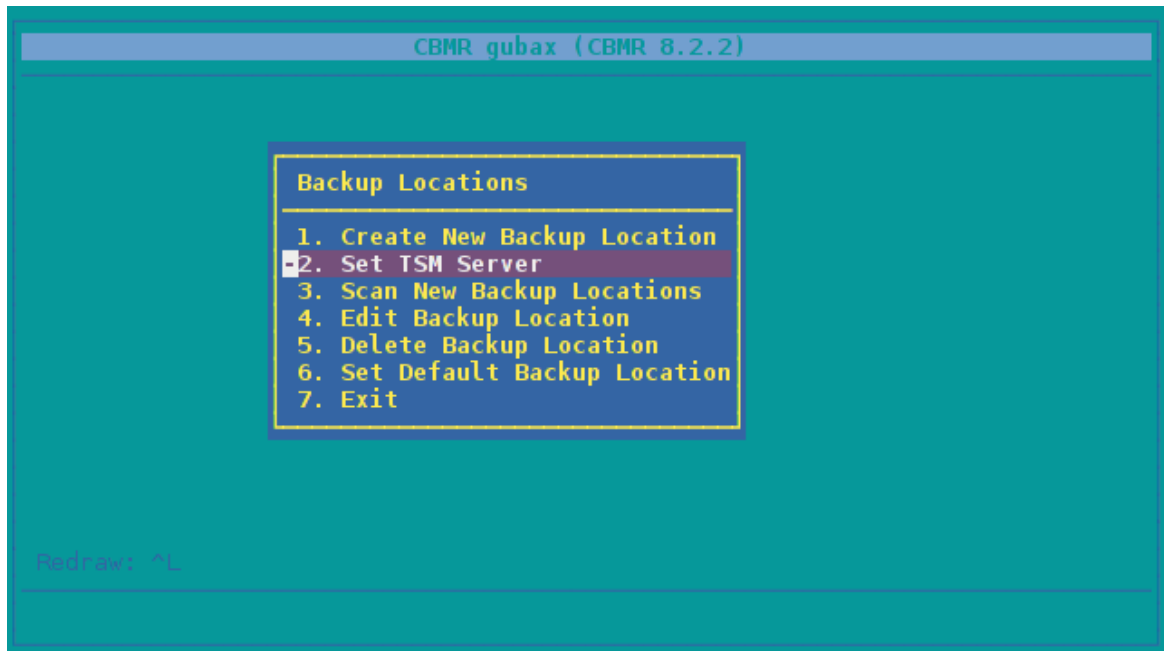
Name	TSM812
ServerName	10.10.2.82
NodeName	NIGELPTBMR
Password	*****
FSName	TBMR

At the bottom of the form, there are "OK" and "Cancel" buttons. At the bottom of the screen, the text "Redraw: ^L" is visible.

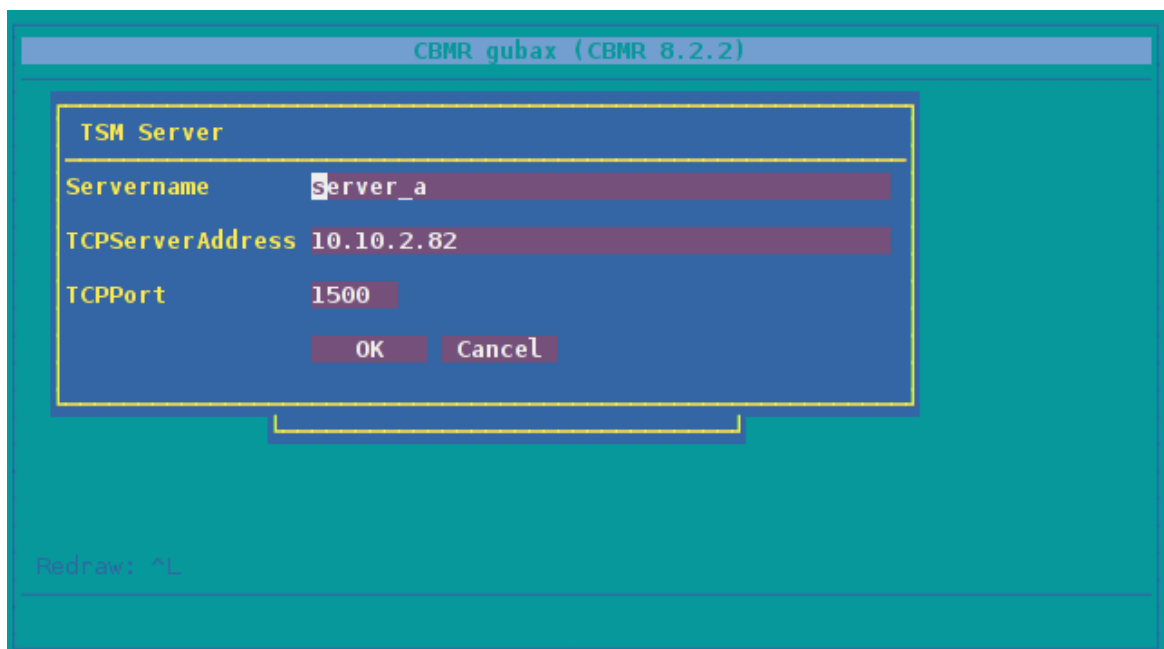
There is no validity check of the parameters at this time - they will be validated when you

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



Add the IBM Spectrum Protect Servername, IP address and access port number.



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 will overwrite 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 TSM Backup Location form.

*Backup operations with server versions 8.1.2.x or later IBM Spectrum Protect require the use of a Transport Layer Security (TLS) certificate. This is mandatory for this server version. Register your certificate using the dsmcert program.*

### 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.

### 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.

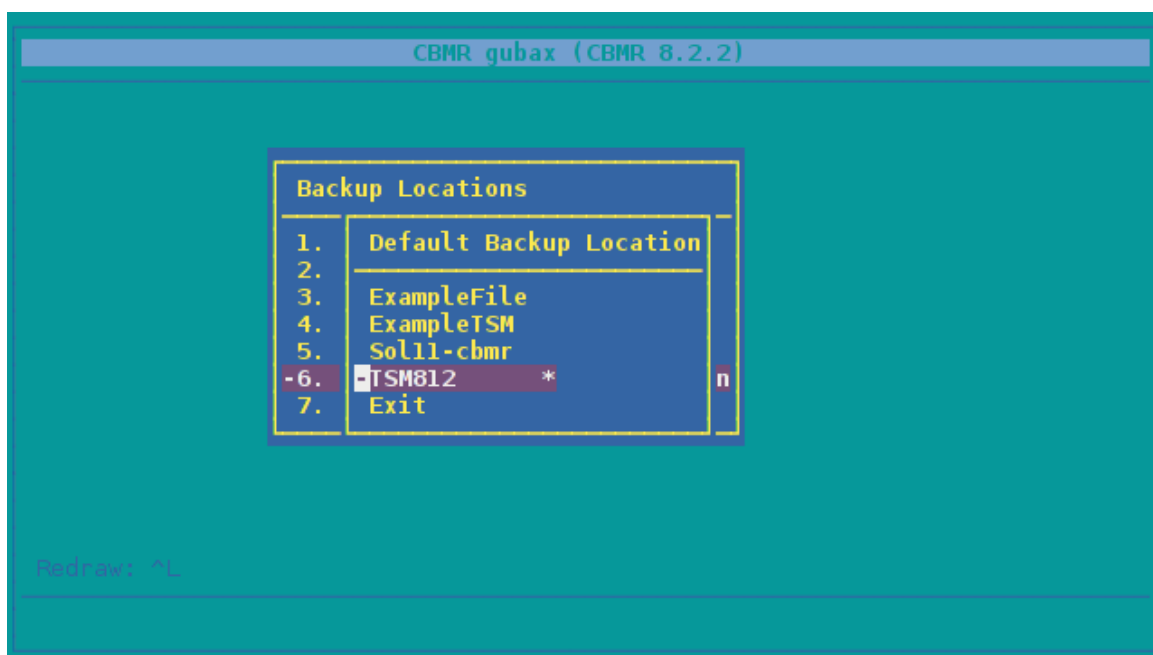
Typically, you could use this on tape drives or virtual tape drives. In order to create a Cascaded Backup Location, you need first to create individual backup locations that you can then cascade.

*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.

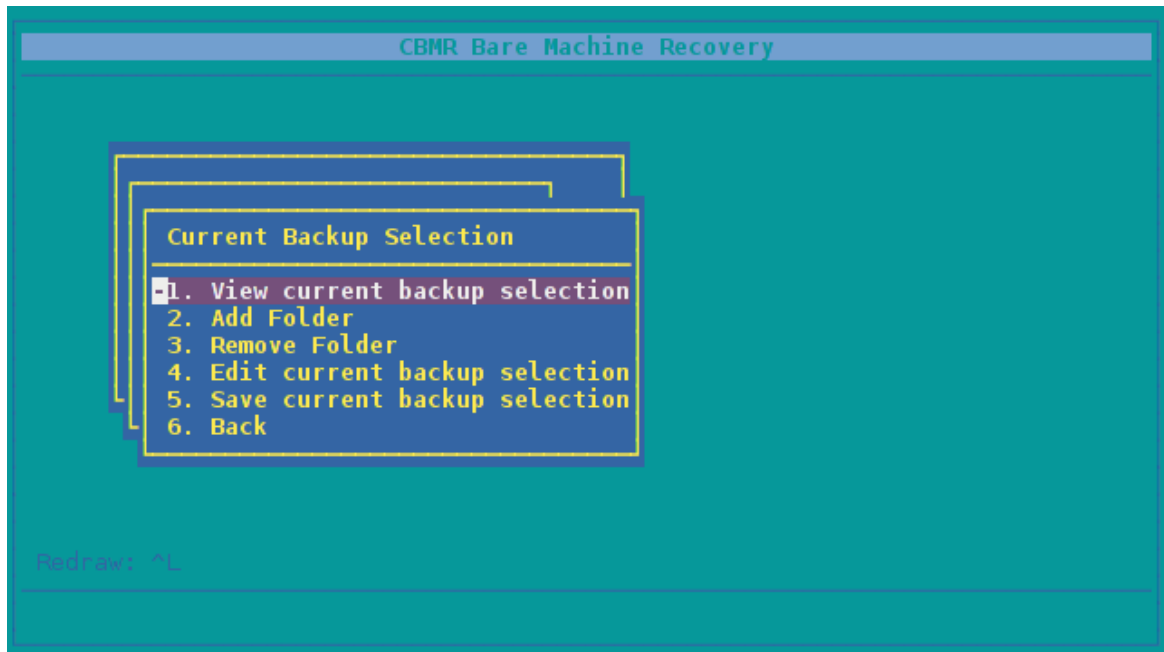


## 7.3 Selecting the Directories to be backed up

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 Solaris, all **mounted** volumes will be selected for backup.

### 7.3.1 Viewing the current backup selection

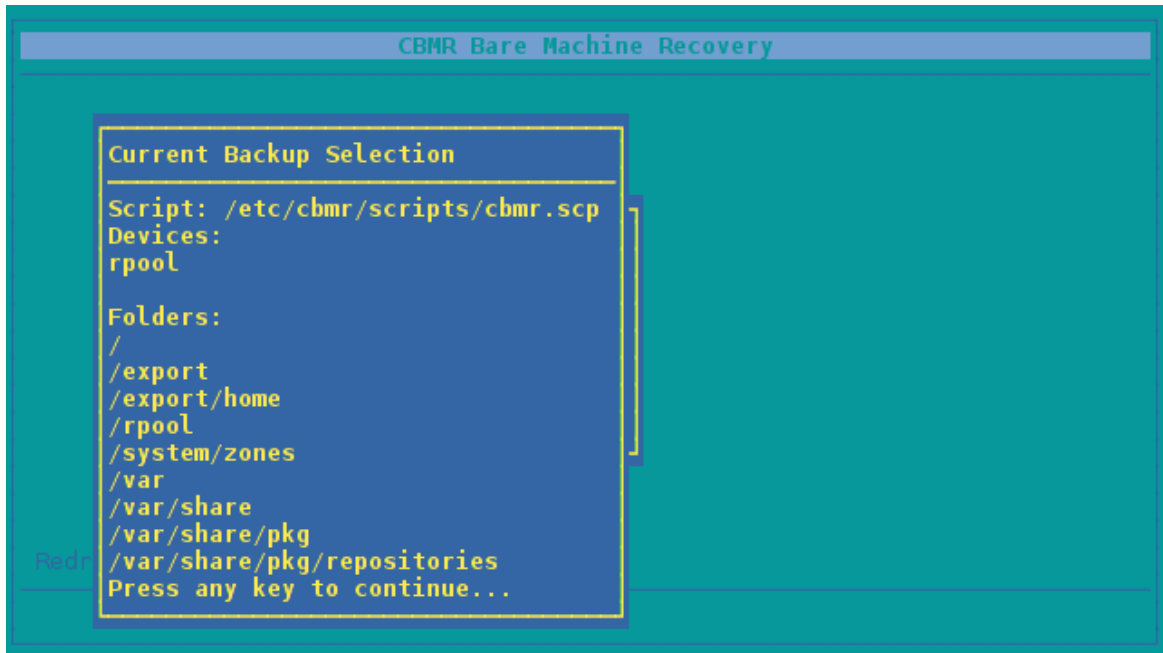
The current backup selection can be viewed and modified via the **Current Backup Selection** menu, accessed via the Backup menu:



The current backup selection can be viewed using the **View Current Backup Selection** option. This will display the following information:

- **Script** - the location of the script file.
- **Directories** - the directories that will be backed up
- **Directories not included in the selection**

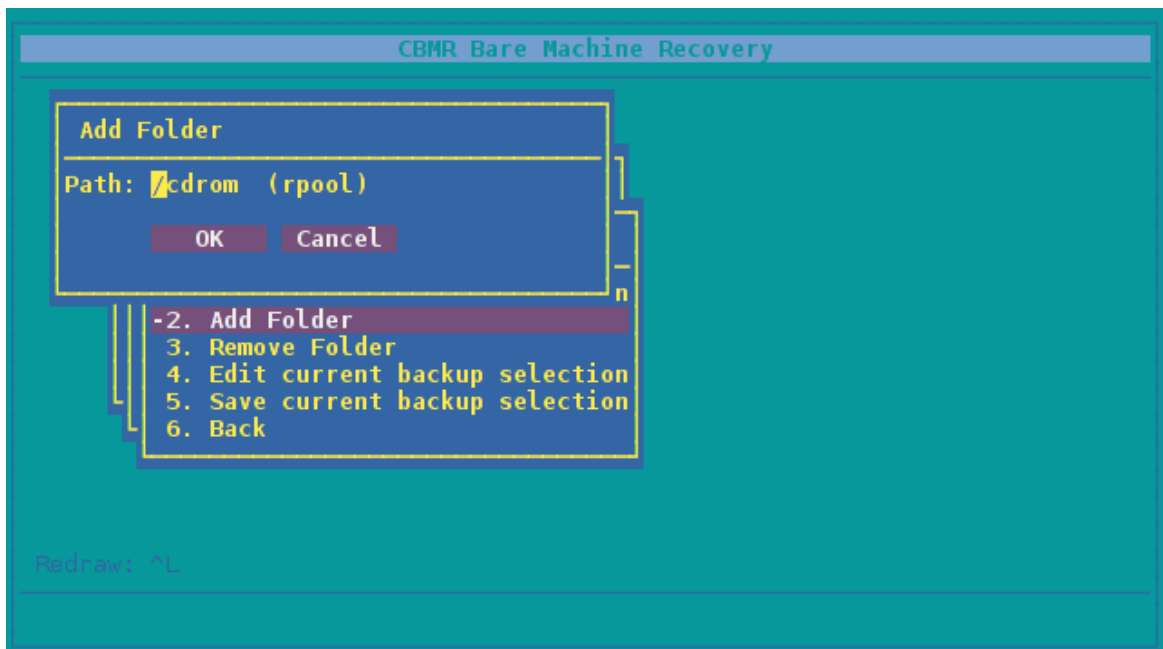
The following is an example of a backup selection for a typical system:



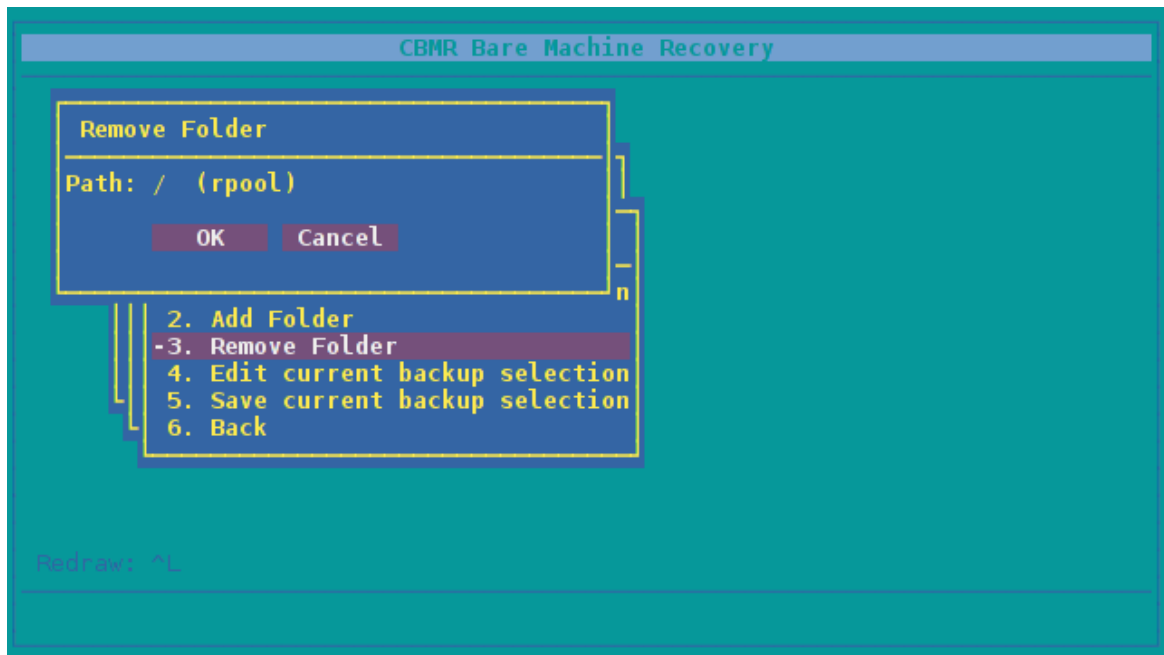
### 7.3.2 Editing the current backup selection

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.

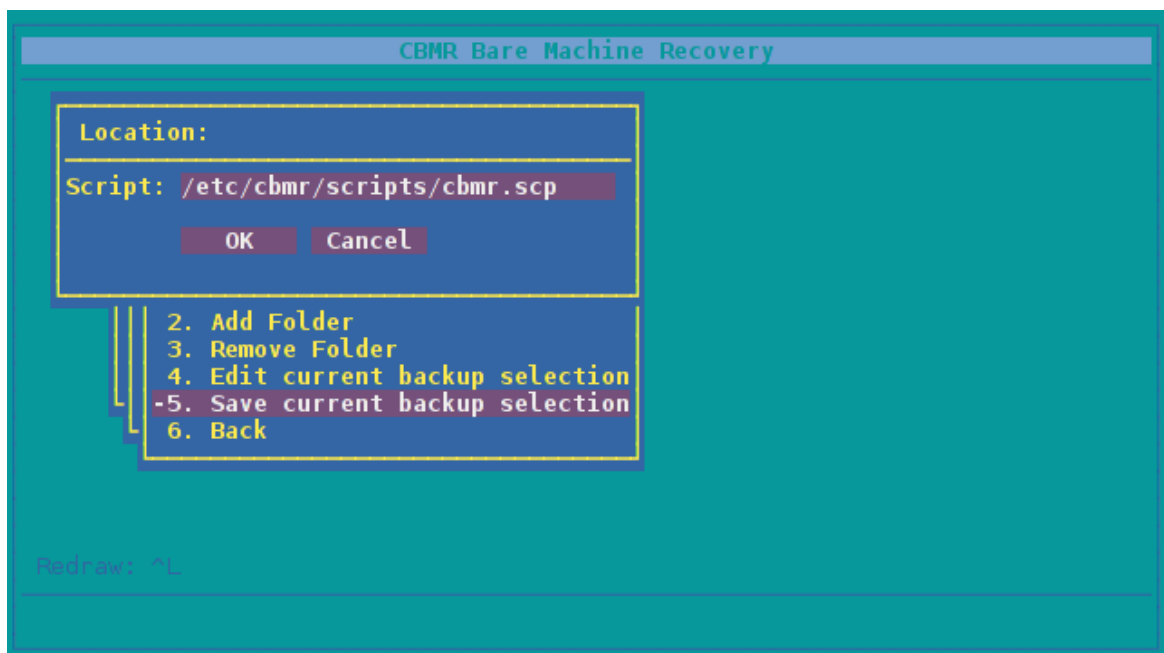


Each directory to be added or removed will have the device it resides on in brackets. If all directories for a given device are removed using Remove Folder, then it will not be necessary (but still possible) to recreate this device at recovery time.



### 7.3.3 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.

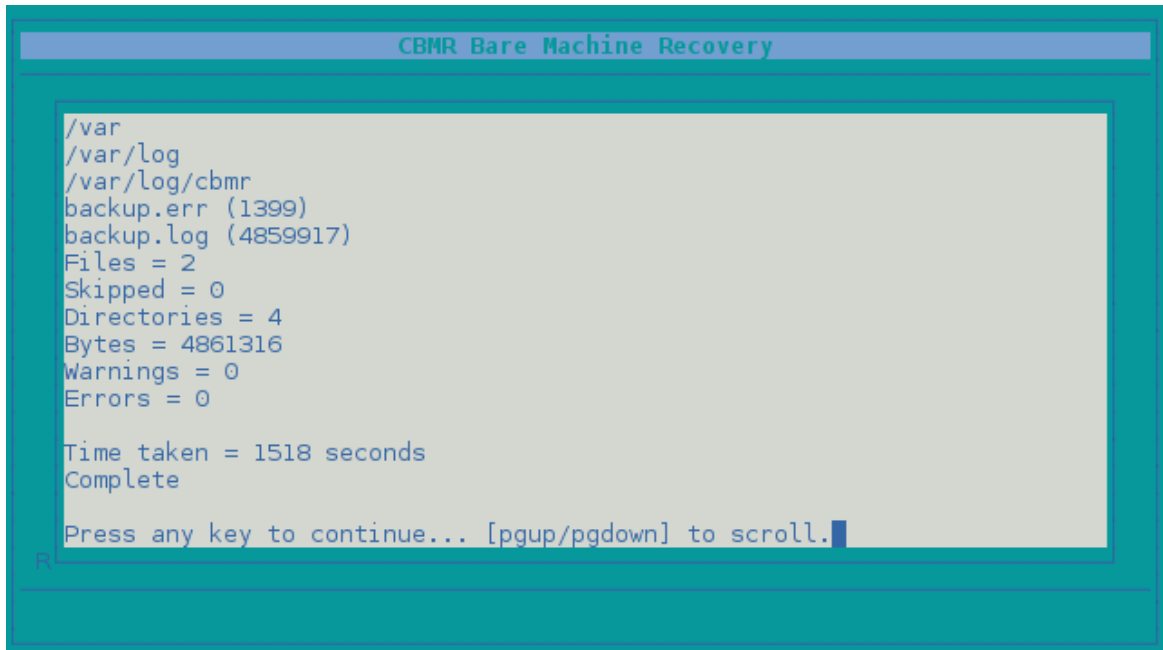


## 7.4 Performing the Backup

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

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.

A screenshot of a terminal window titled "CBMR Bare Machine Recovery". The window has a teal border. Inside, a light gray rectangular area contains the following text in a monospaced font: 

```
/var
/var/log
/var/log/cbmr
backup.err (1399)
backup.log (4859917)
Files = 2
Skipped = 0
Directories = 4
Bytes = 4861316
Warnings = 0
Errors = 0

Time taken = 1518 seconds
Complete

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

 A cursor is visible at the end of the last line.

A backup can also be performed using the gubax utility or the ubax command line utility direct but Cristie recommends using `cbmr`. See the man pages of each utility for a description of their functionality.



## 8 Performing a Recovery

The final stage will test the backup location supplied, then perform the recovery. Recovery is divided into a number of stages dependent upon the system configuration:

1. **FDisk** - make the disks recognisable to Solaris
2. **Partition** - partition disks to match configuration

*Veritas Volume Manager* installed:

3. **VXDisks** - set disks to be managed by VxM
4. **VXGroups** - create Veritas disk groups
5. **VXVolumes** - create Veritas volumes

*Solaris Volume Manager* installed:

6. **MetaVolumes** - create SVM meta-devices

*ZFS support* installed:

7. **ZPools** - create FS Zpools
8. **FileSystems** - create file-systems on the volumes created in steps 5, 6 and 7
9. **Mounting** - mount the file-systems
10. **Recovery** - recover files from the backup
11. **PostRecover** - perform modifications to recovered files to match new configuration
12. **Make bootable** - make the system bootable

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

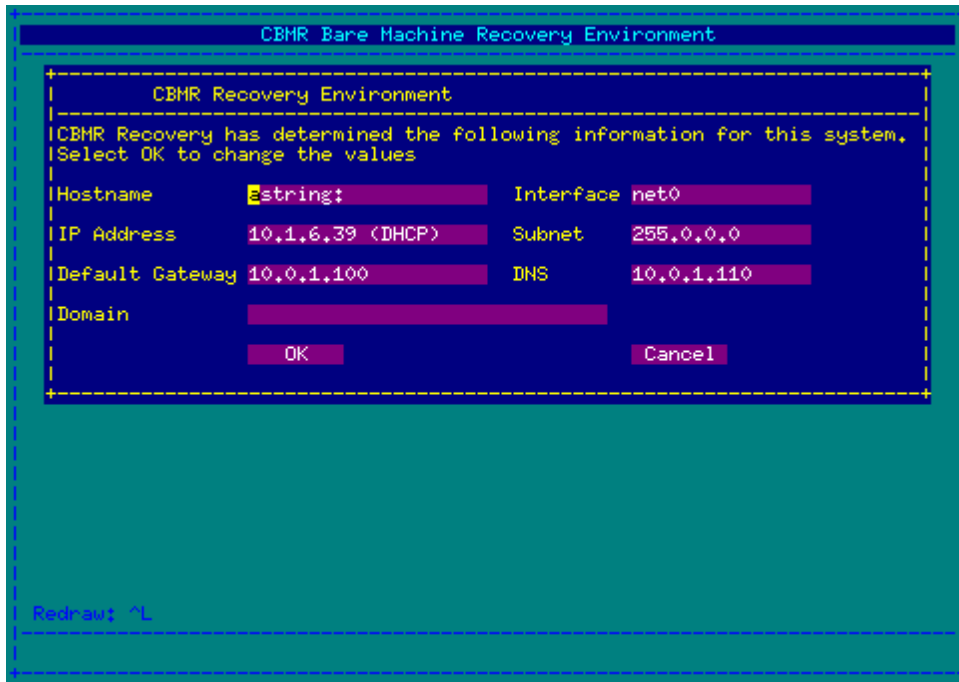
Before reboot, it is recommended that a copy of the log files generated during the recovery is made, as shown in Copying Log Files.

### 8.1 Starting the Recovery Environment

A recovery may be performed by booting into the recovery console from the recovery CD created earlier. The environment will initialise by attempting to acquire a network address via DHCP or RARP and starting an SSH server if available.

*Note: the password for the SSH server will be identical to the password of the machine on which it was created*

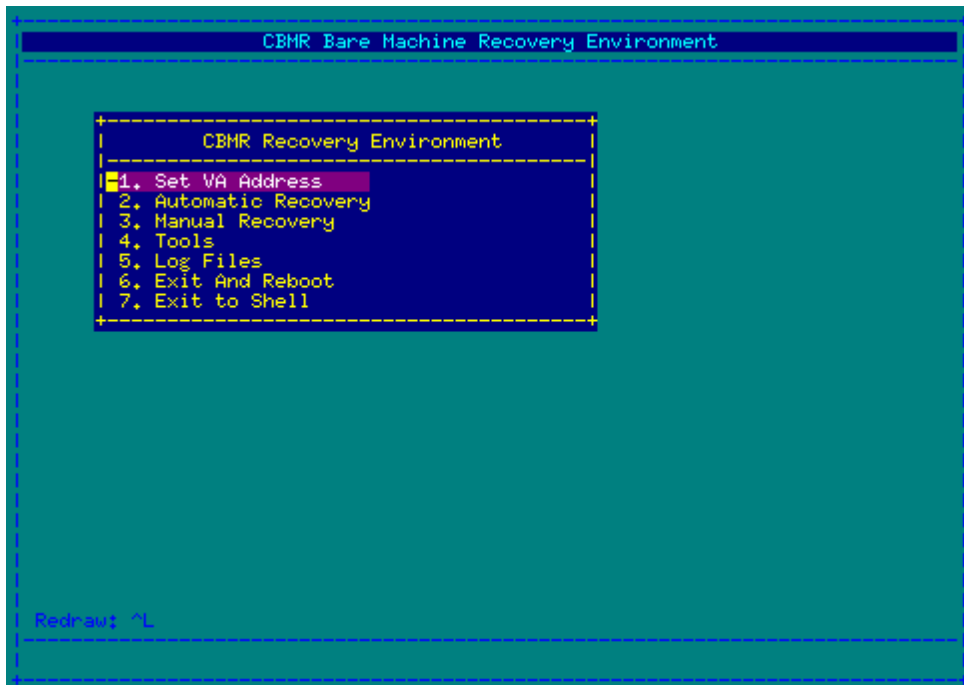
Once boot-up is complete, a dialogue will be presented to change the hostname or network setup.



Selecting **Cancel** at this stage will leave these values as they are.

*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** will be presented:



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.

Two recovery modes are available - **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
- The manual recovery provides the ability to run through 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. This can be performed by exiting to the shell and restarting the GUI using: > TERM=vt102 dr*

## 8.2 Automatic Recovery Wizard

The **Automatic Recovery Wizard** takes you through the following steps in order:

1. **Setup Network** - if initial setup was unsatisfactory
2. **Backup Location** - specify the attributes of the TSM Server, incremental backup directory or VTD file holding 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

### Setup Network

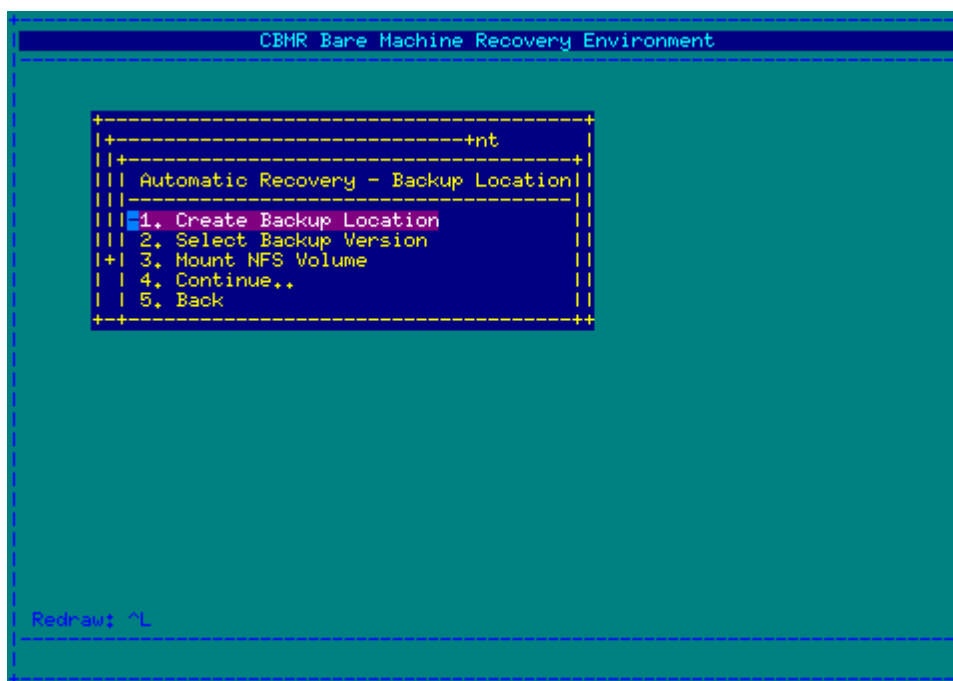
The network can be setup for any interfaces found using either DHCP (Dynamic Host Configuration Protocol) or manual configuration.

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

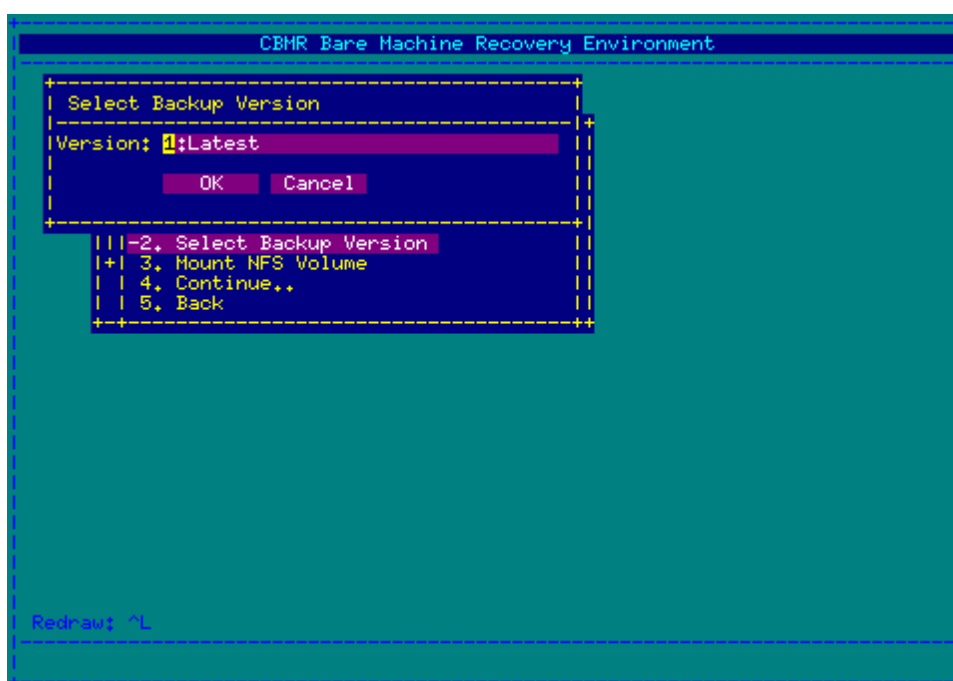
*Note: it is common to see warning messages during DHCP setup as interfaces may be polled whilst they are in uncertain states. The DHCP setup will fail if an IP address is not received in ten seconds. Therefore, if DHCP fails initially, it may succeed on subsequent attempts.*

### Backup Location

The backup location menu allows the user to set up the backup location in the same manner as described in [Configuring a Backup Location using the Graphical User Interface](#). By default the Backup Locations available on the host used to create the ISO image will be available in the recovery environment.



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

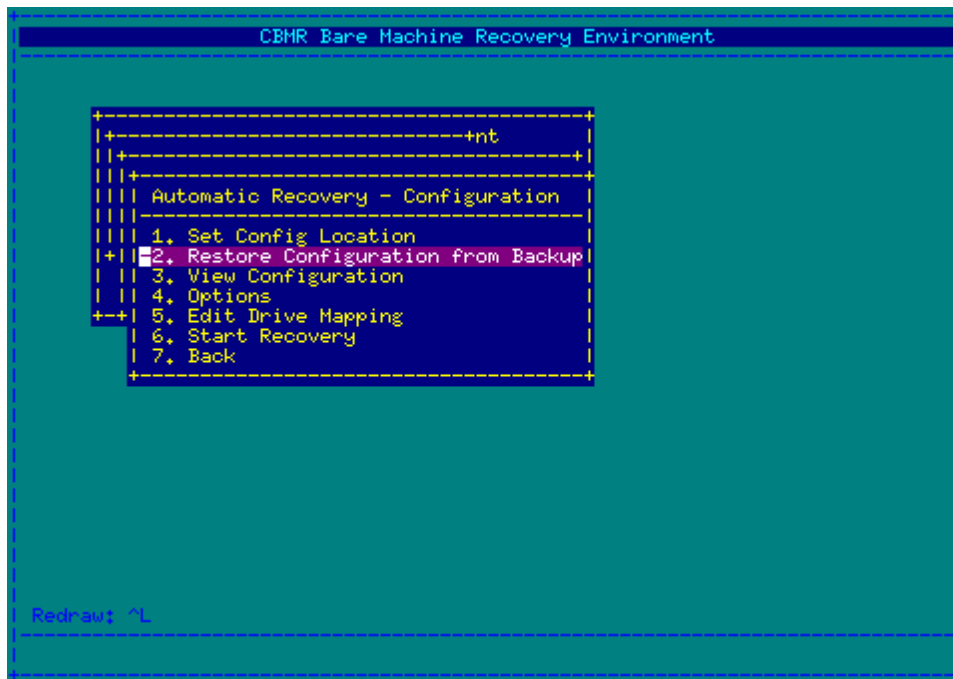


**Note:** a backup version only applies to file based incremental backups

Once the backup version has been successfully selected, you can move to the next stage to set up 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.



A typical configuration is shown:

```

Comments =
Time Created = Tue Dec 19 11:12:48 2017
Volume Number = 0

Dataset number = 0

AREA HEADER:
Name =
Comments =
Compression Method = 0
Time Created = Tue Dec 19 11:12:48 2017
Volume Number = 0
Backup Version = CBMR 8.2.2
Buffer Size = 16384

Moving to directory area
Reading directory information
Building file list for /CBMRCFG/disrec.xml
Moving to data area
Restoring 3
/CBMRCFG/
/CBMRCFG/CBMRCFG
disrec.xml (102521)
Files = 1
Skipped = 0
Directories = 2
Bytes = 102521
Warnings = 0
Errors = 0

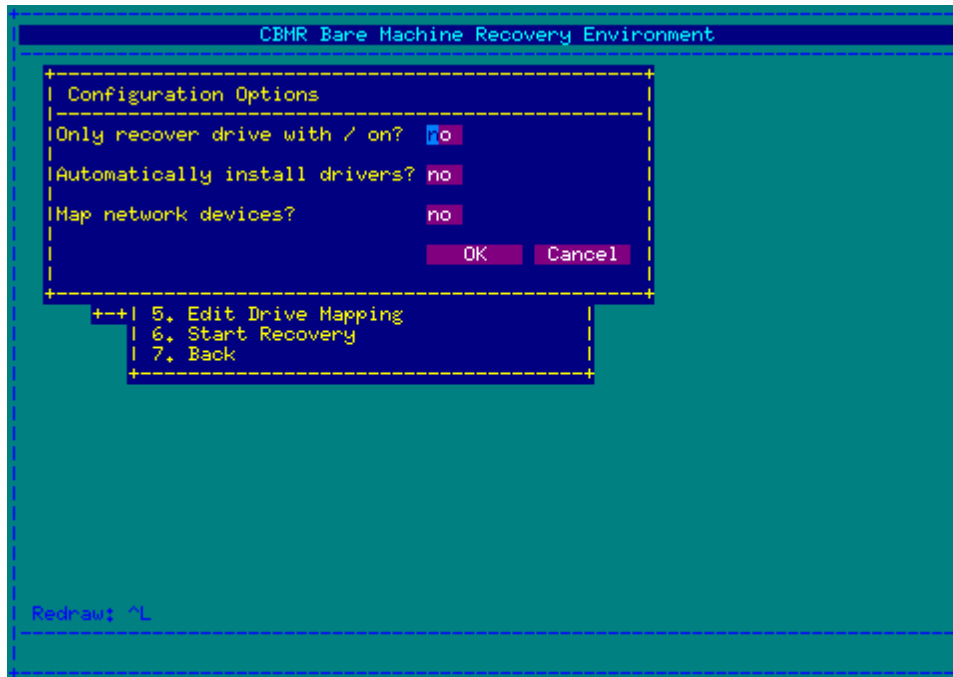
Time taken = 0 seconds
Creating disk mapping...
Press ENTER to continue...

```

**Note:** if the location was saved with the recovery CD, as outlined in [Creating a Recovery Image](#), then this step may be skipped

**Note2:** if the location of the configuration was changed in [Recording System Information](#), you will need to enter the location chosen here

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



The **Configuration Options** control what is to be recovered and which steps are to be performed upon completion.

Your first option defines whether you intend to recover only the drive that the root filesystem (/) is mounted on. This will work in addition to drive mapping by removing all drives from the mapping that are not required. This option is useful if the system has a number of drives, many of which are data drives that do not need to be recovered.

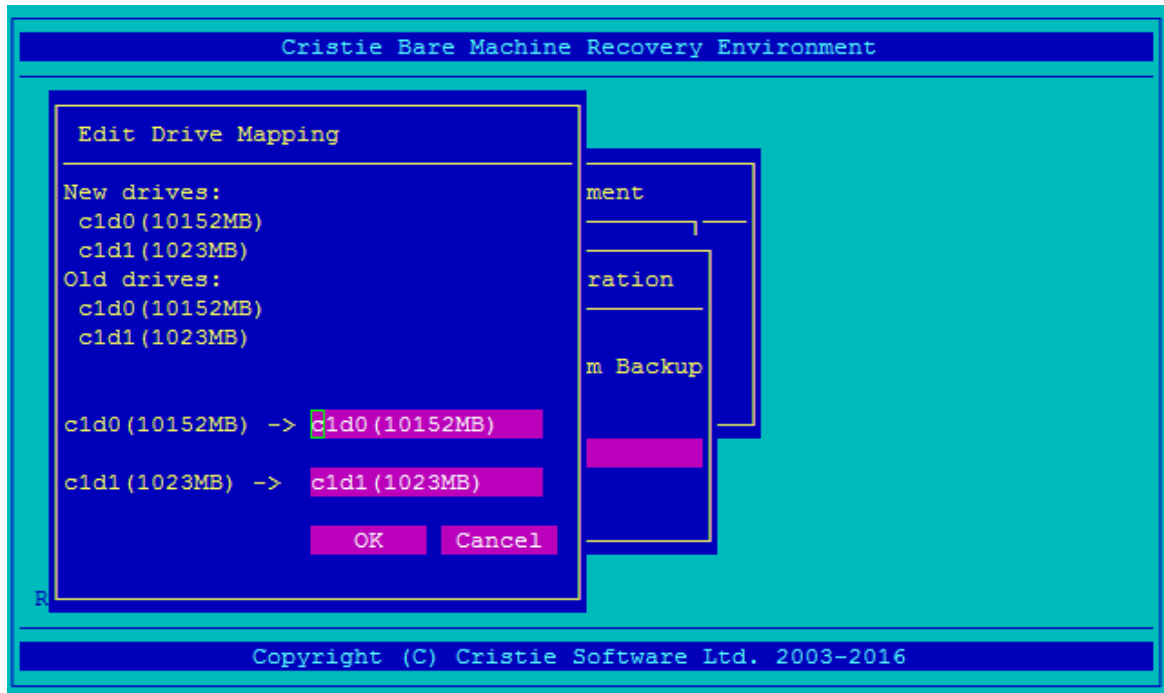
*Note: this can also be achieved by setting all but the root drives to 'Unmapped' in the drive mapping*

The second option enables you to instruct the recovery environment to automatically install drivers. It is rare that this is required, as Solaris systems usually install with drivers necessary for all supported hardware. However, if additional drivers were added to the CD to support the disk controller or network cards, then this option will automatically add them to the recovered environment.

The third option will instruct the recovery environment to map network devices from the backup to those present on the current machine. This will ensure that any interfaces previously in use are available on the restored machine.

*Note: if fewer interfaces are present on the new machine, then mapping can only work on a best effort basis*

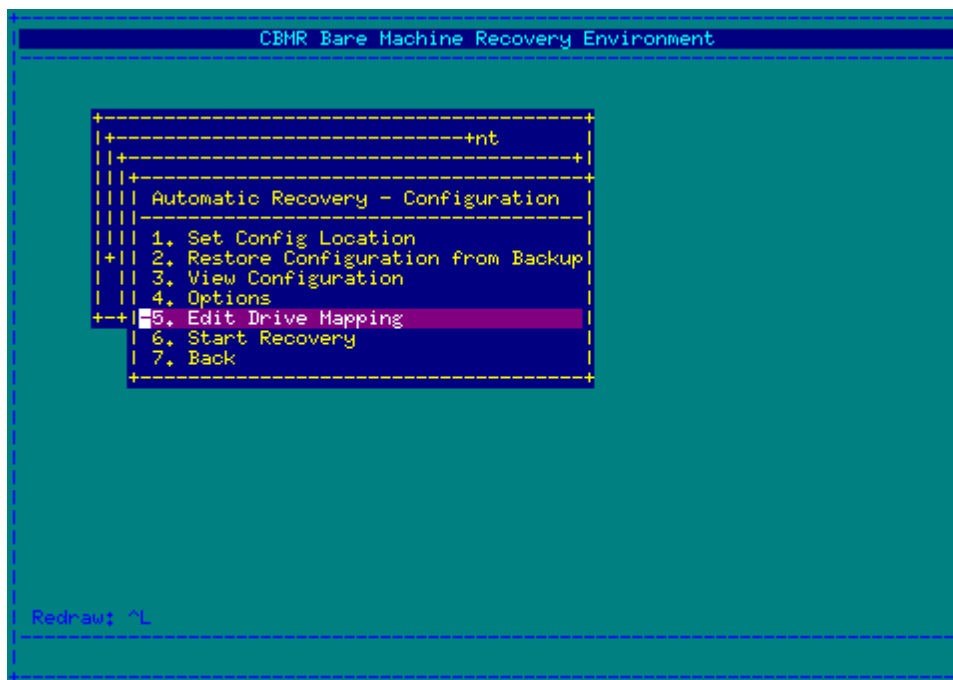
The **Edit Drive Mapping** item is used to modify the disks that the backup is restored to. In the example given, a system using two disks is mapped to a use only one disk during recovery.



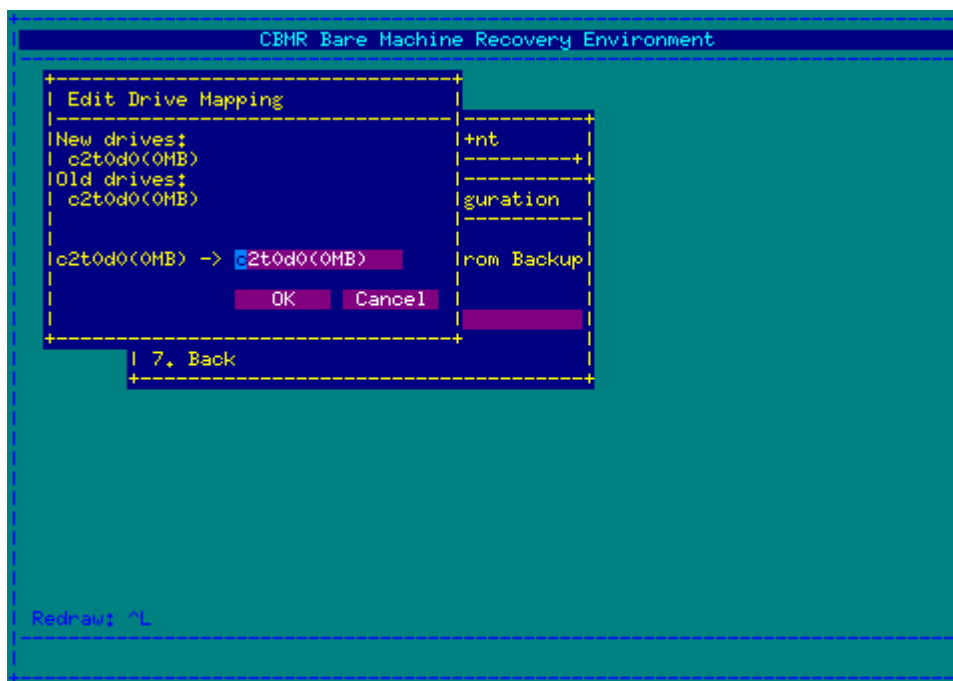
When recovering to fewer disks, any volume groups other than **rootvg** which cannot be re-created will be dropped. However, a volume group spanning more than one physical volume can be restored to a single volume provided that volume has enough capacity. In the case of mirrored volume groups the mirroring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

## 8.2.1 Drive Mapping

Selecting the **Drive Mapping** option will display a form matching drives in the configuration to drives on the system.



It is also possible to remove drives from being recovered here. If you do not wish the data on a particular drive to be recovered, then select '**Unmapped**':



*Note 1: if a disk is set to 'Unmapped', then the restore procedure will remove ALL devices that rely on that disk. In particular, if the disk is part of a mirror, then the mirror will not be recovered*

*Note 2: in some circumstances where there are a large number of disks, the 'OK' and 'Cancel' buttons may not be visible. You can scroll the Drive Mapping window up or down by pressing the short-cut keys CTRL-N or CTRL-P to bring them into view.*

If critical devices are removed by a mapping, it will result in the error 'Mapping removes the root filesystem' and the recovery will not proceed.

## 8.2.2 Set IBM Spectrum Protect SSL Certificate

If your DR backup is held on a IBM Spectrum Protect version 8.1.2 or later server, you will need to set the correct SSL certificate **before** running the recovery.

To do this you will need to follow this sequence:

1. Boot the DR environment from the correct CBMR DR ISO.
2. Drop out to a shell from the main DR menu.
3. Mount a directory to a network share where the correct SSL certificate for your server is located and copy the certificate into /tmp (say).
4. Run the correct IBM Spectrum Protect command to register the certificate with the server. For example:

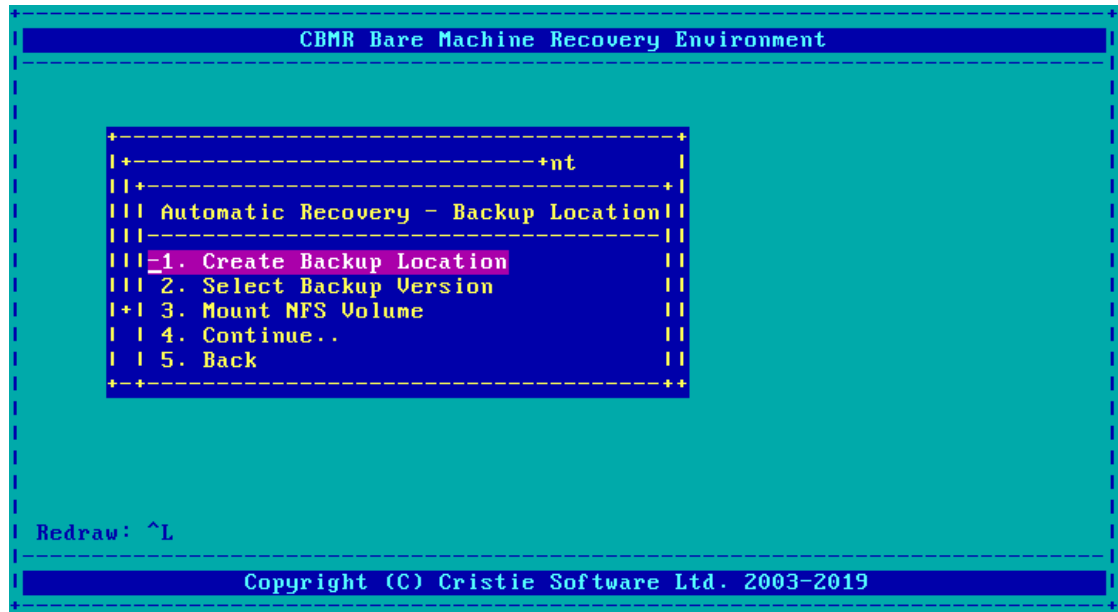
```
/op/tivoli/tsm/client/api/bin64/dsmcert -add -server 10.10.2.82 -
file /tmp/cert256.arm
```



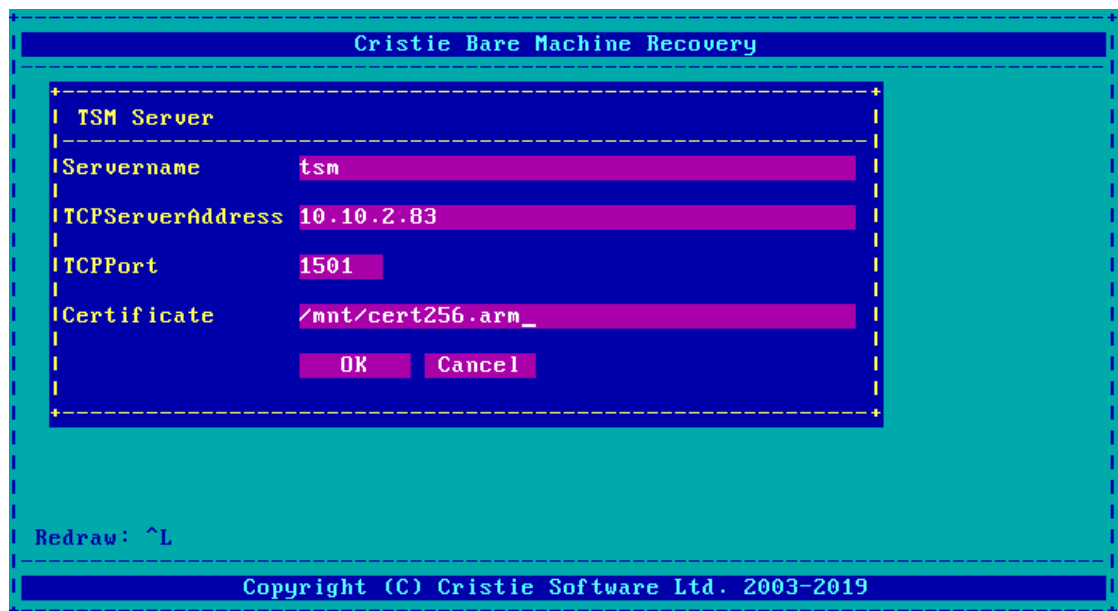
(substitute your server IP and certificate file names)

Alternatively, through the GUI you can perform the following sequence:

1. In the Automatic Recovery menu, mount the network share where the SSL certificate for your server is located by clicking [Mount NFS Volume](#).



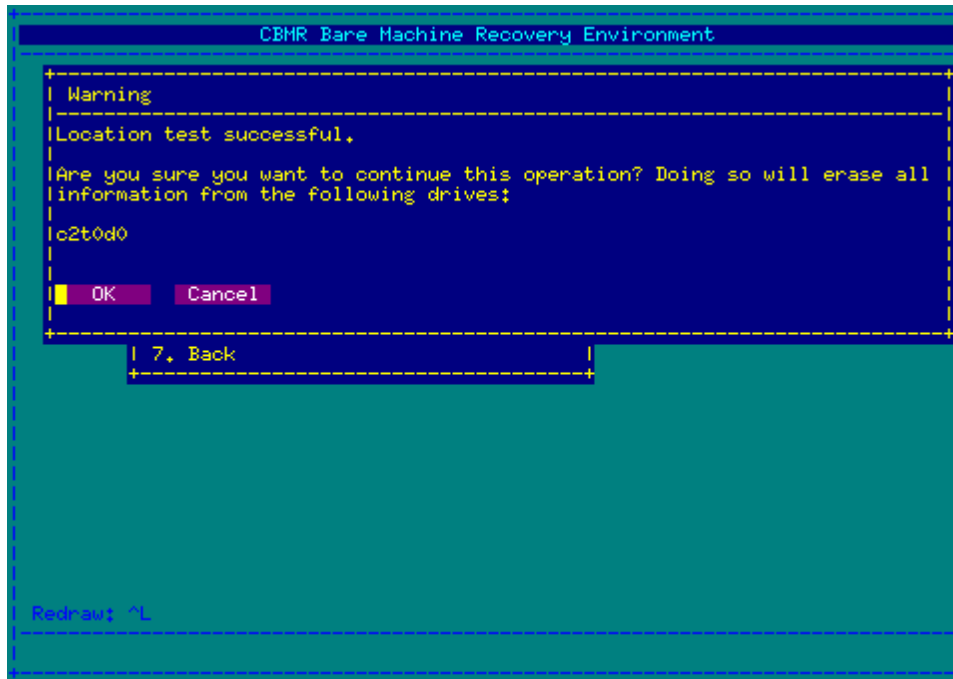
2. Once mounted click [Create Backup Location](#) and then click [Set TSM Server](#). Fill out the form with the certificate mount location and name e.g. /mnt/cert256.arm. Click [OK](#) to set the TSM details and certificate.



If you omit this certificate registration step you will see SSL protocol errors during the recovery.

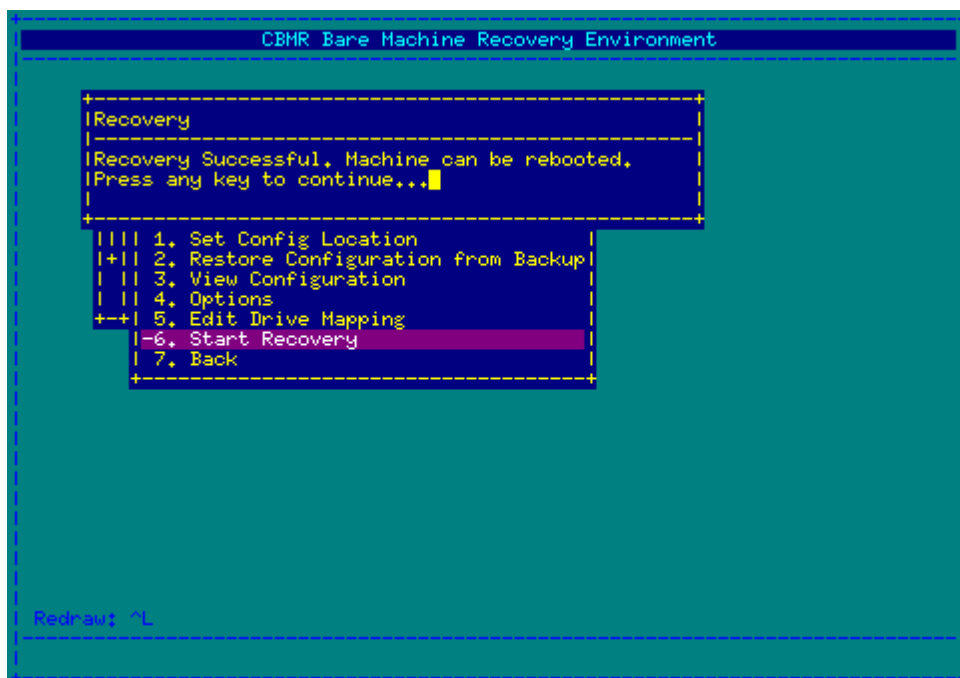
### 8.2.3 Start Recovery

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



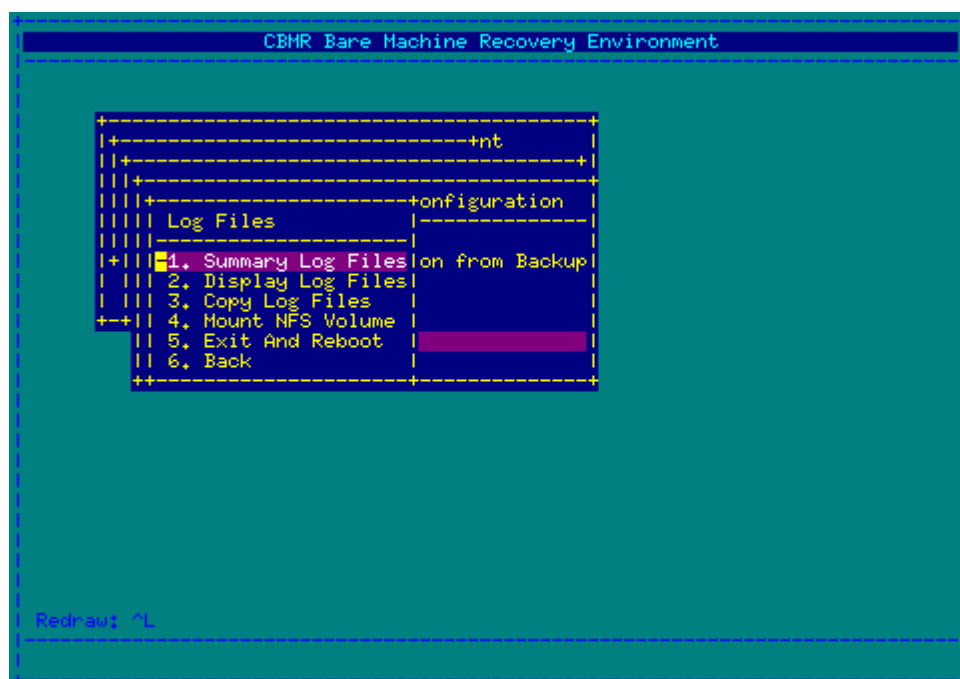
*Note: as soon as the recovery is started, ALL data will be destroyed on the drives listed*

Once the recovery is complete, you will be presented with a dialogue indicating that the machine can be rebooted.



## 8.2.4 Copy Logs

Once the recovery is complete, a menu will be opened containing options for copying log files:



The **Summary Log Files** entry allows you to view the most important informational, warning and error messages generated during the recovery.

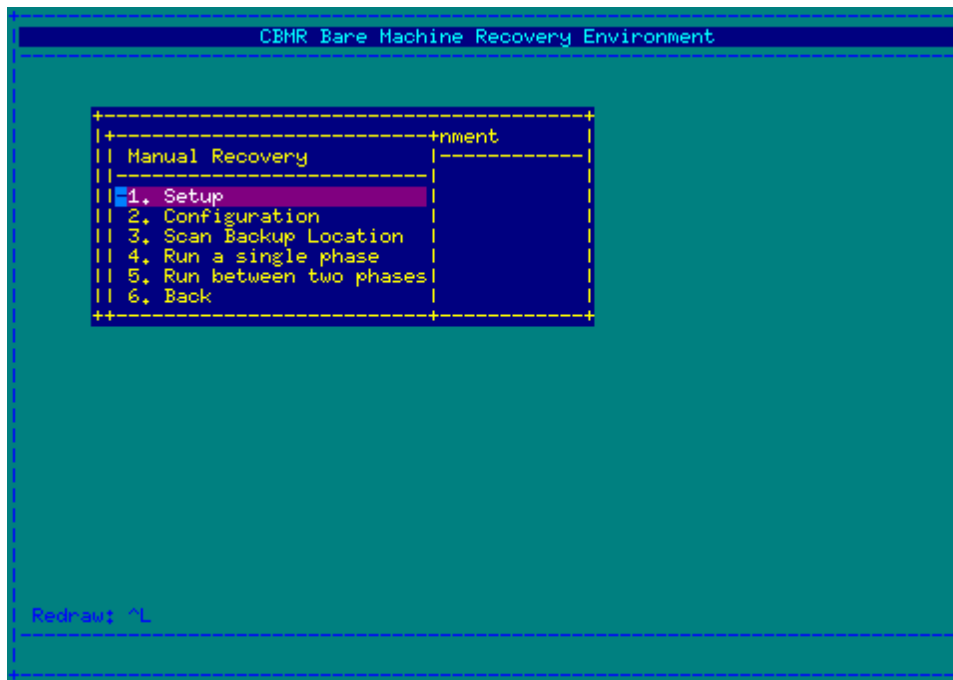
Copying the log files to an NFS share will allow any problems encountered during recovery and subsequent reboot to be diagnosed more quickly. This is highly recommended.

*Note: These log files will also be requested by Cristie Support if you contact them to assist with any recovery issues.*

## 8.3 Manual Recovery

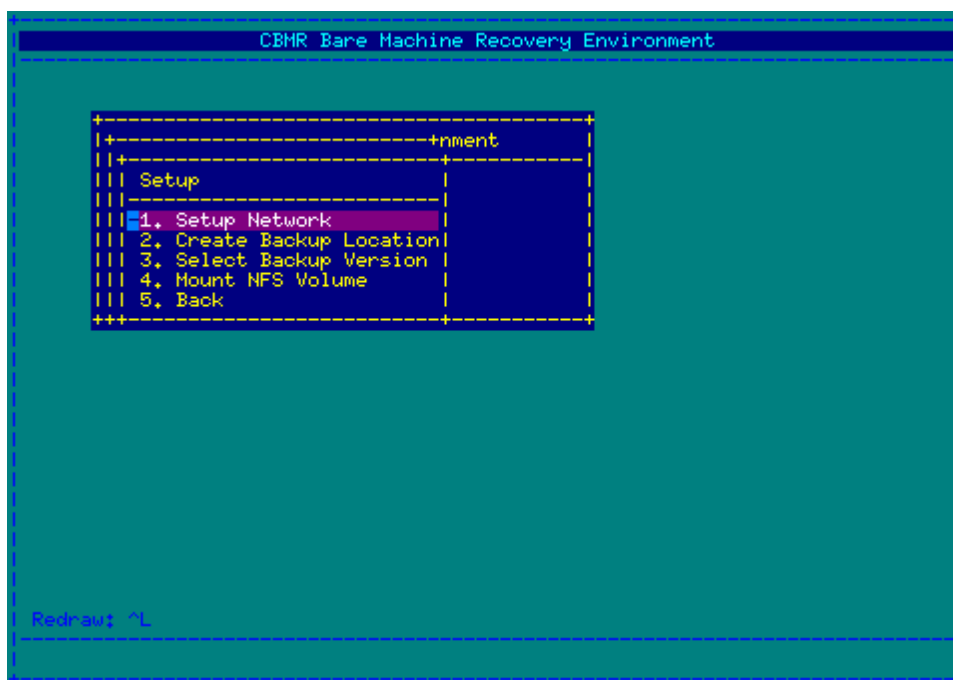
**Manual recovery** presents the stages performed during automatic recovery to be applied individually. This may be required if a particular stage fails and you wish to continue the recovery from that point onwards, rather than restart.

The options in the manual recovery menu are:



### Setup

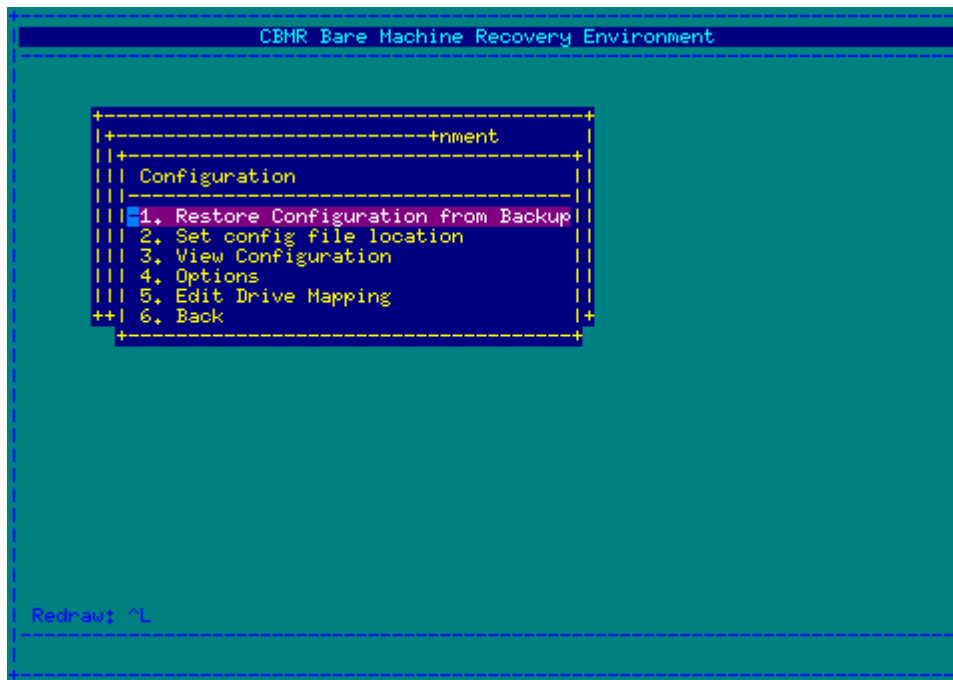
The setup menu allows you to setup networking (exactly as the first stage of the automatic recovery) and setup the IBM Spectrum Protect server if required.



This menu also allows you to directly edit the `dsm.opt` and `dsm.sys` files. This may be useful if the IBM Spectrum Protect Server requires additional parameters not set in the default setup.

### Configuration

The configuration menu allows you to restore the configuration from the backup, select which disks should be restored and modify configuration options.



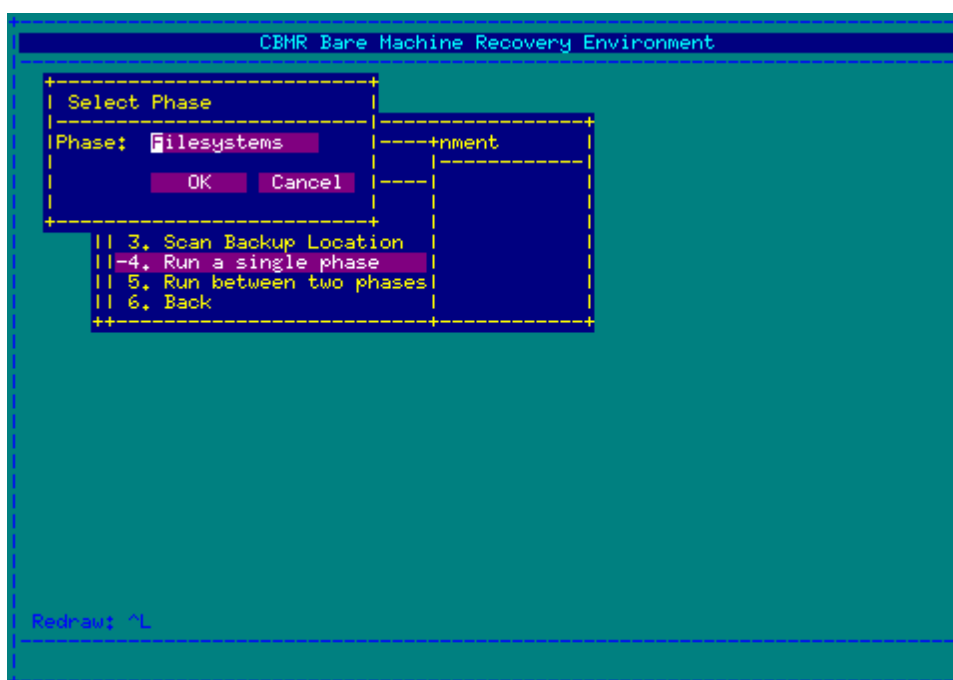
This menu presents the same options as the configuration menu for the automatic recovery.

### Test Backup Location

This option allows you to test the backup location for connectivity before performing a restore. It is recommended that this step is always performed before recovering a system.

### Running a single recovery phase

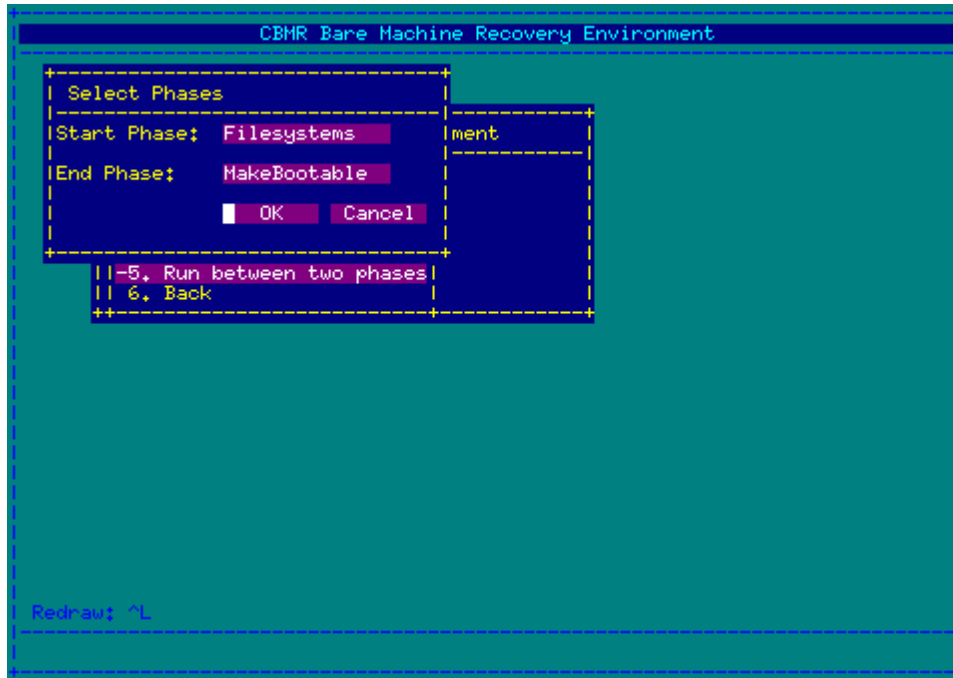
If a problem occurs during recovery, it may be desirable to attempt to run a single recovery phase. This option allows you to select a single phase and run it on its own.



*Note: running an earlier phase after a later phase, such as running Partitions after Restore, will RESET ANY WORK DONE BY A LATER PHASE. You will therefore have to run the remaining phases as well to complete the restore*

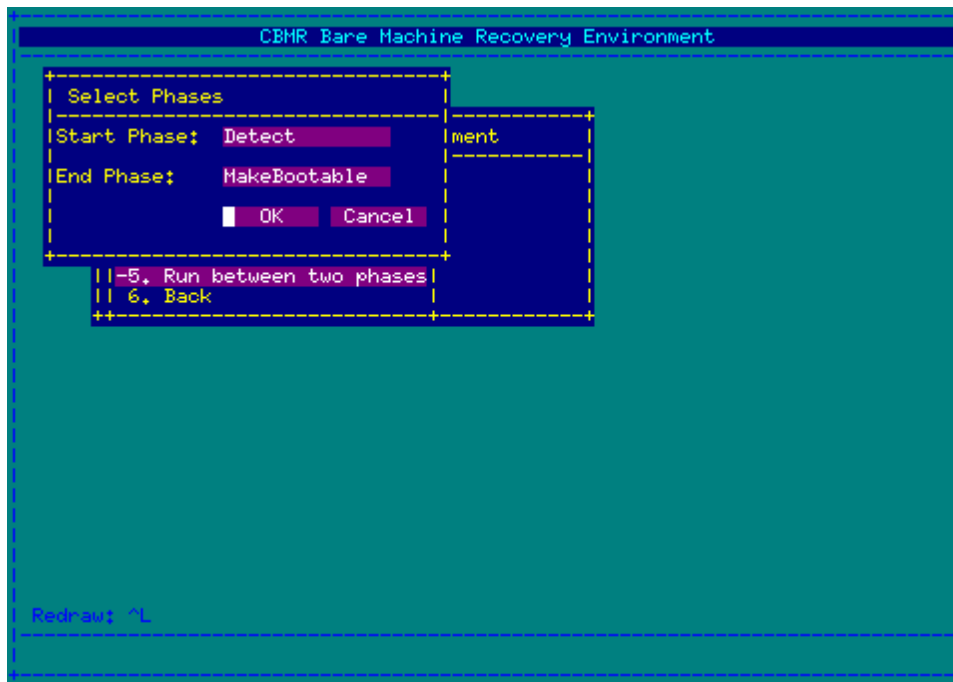
### Running between two recovery phases

The '**Run between two phases**' menu option allows you to run **all** phases, inclusively, between two sections. In the following example, the restore is being run from creation of the two pools to the mounting of file-systems:



This option may be used to restart a stalled recovery from the next phase to run until completion. For example, if the recovery stopped at the FileSystems stage, then running from Mounting to MakeBootable should result in a fully restored system.

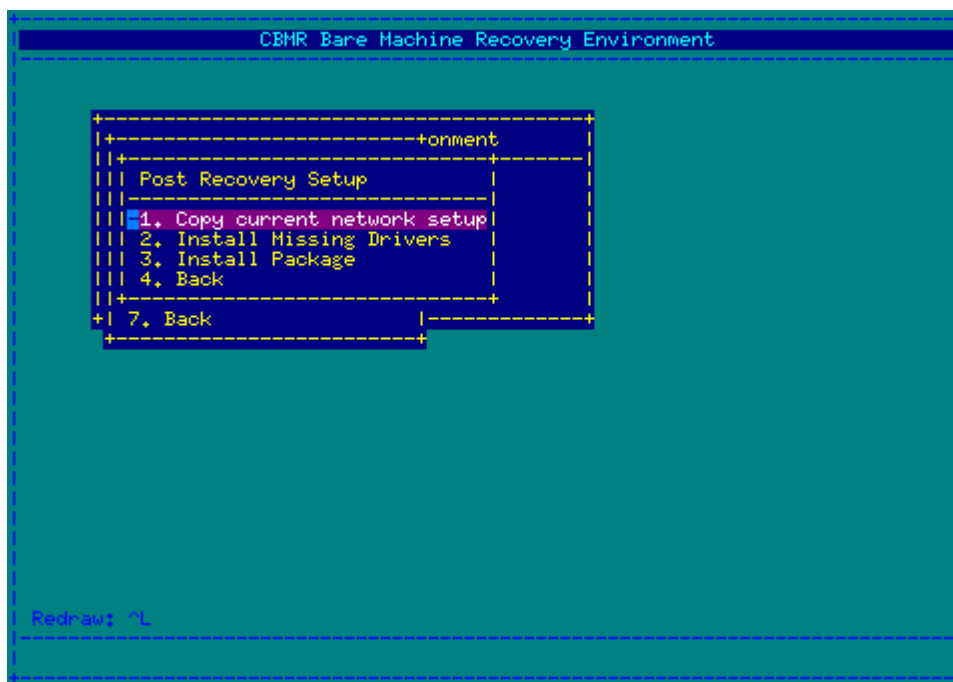
Additionally, there is a special option which will attempt to work out the last known phase:



This option is useful if it is not clear why the recovery stopped.

## 8.4 Post Recovery Steps

There are a number of steps that can be performed once the recovery is complete to help ensure that the recovered system does not need additional configuration before it is usable.



### Copy current network setup

The network settings used by the recovery environment can be copied to the recovered system so that it uses those settings on boot up. If DHCP was used to obtain an IP

address, then the recovered system will use DHCP on boot up.

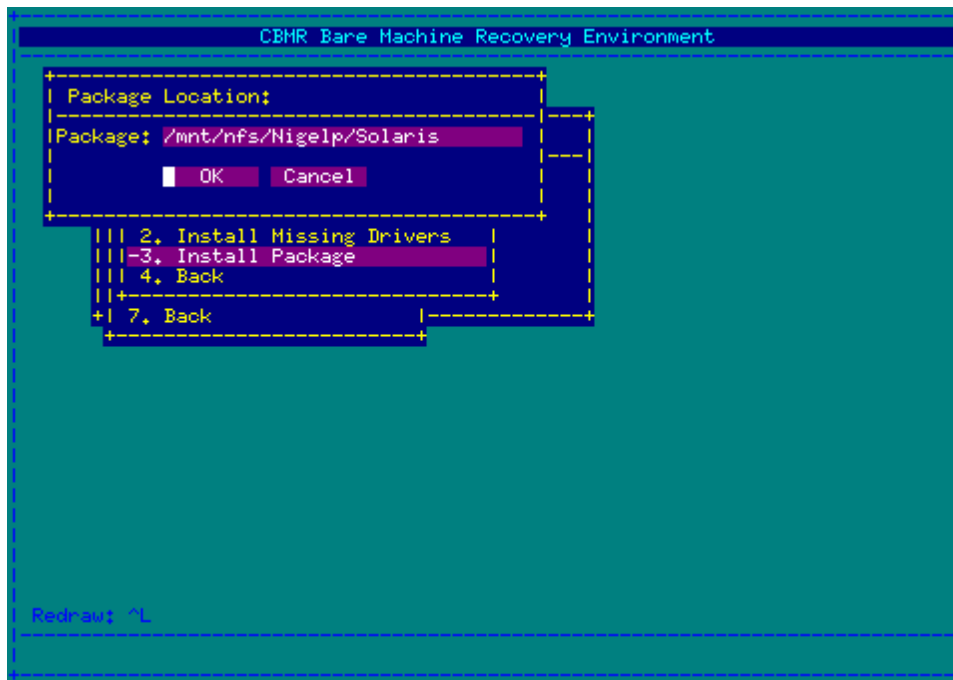
You can also use this feature to change the original hostname to something different and/or change the IP address from DHCP to static or vice versa. Note this only works when recovering to the same original system for Solaris 10. However, for Solaris 11 recoveries, both hostname and IP address may be changed regardless of the target system.

### Install Missing Drivers

This option examines the current setup to determine which drivers were used to access the disks and the network adapters. It then examines the recovered system to determine whether these drivers were installed. Once complete, it will present a list of drivers that can be pushed from the recovery CD to the recovered system.

### Install Package

Some driver packages (in particular RAID controllers, such as HP smart-array) install a set of tools alongside the driver. This often means that installing the driver by itself is not sufficient to get a working system. In these cases, it is recommended the driver package is installed instead.

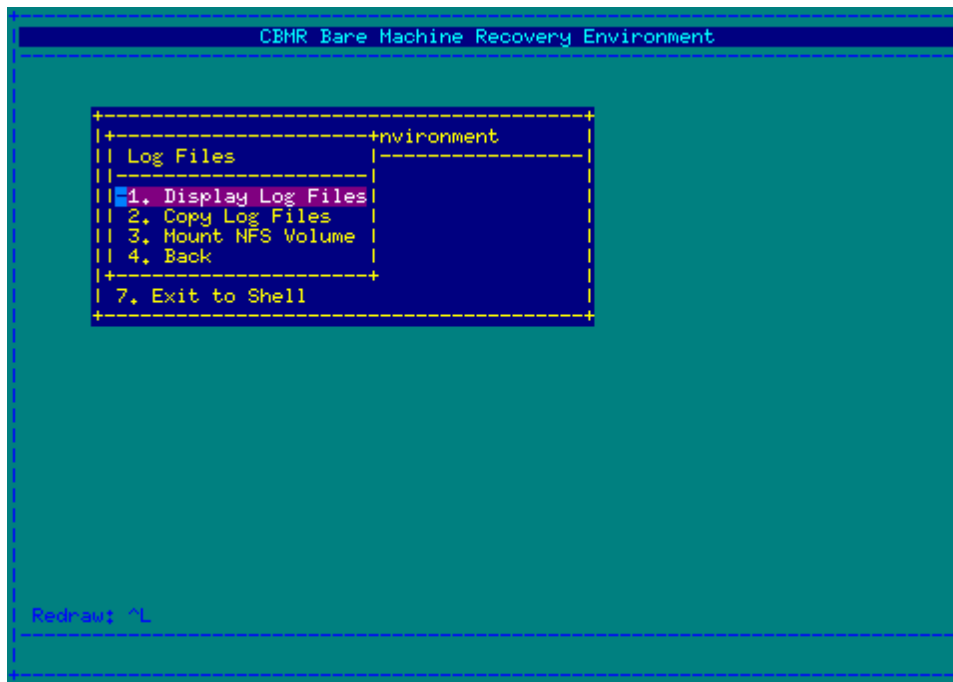


The simplest method to perform this operation is to mount an NFS drive that contains packages and install from there.

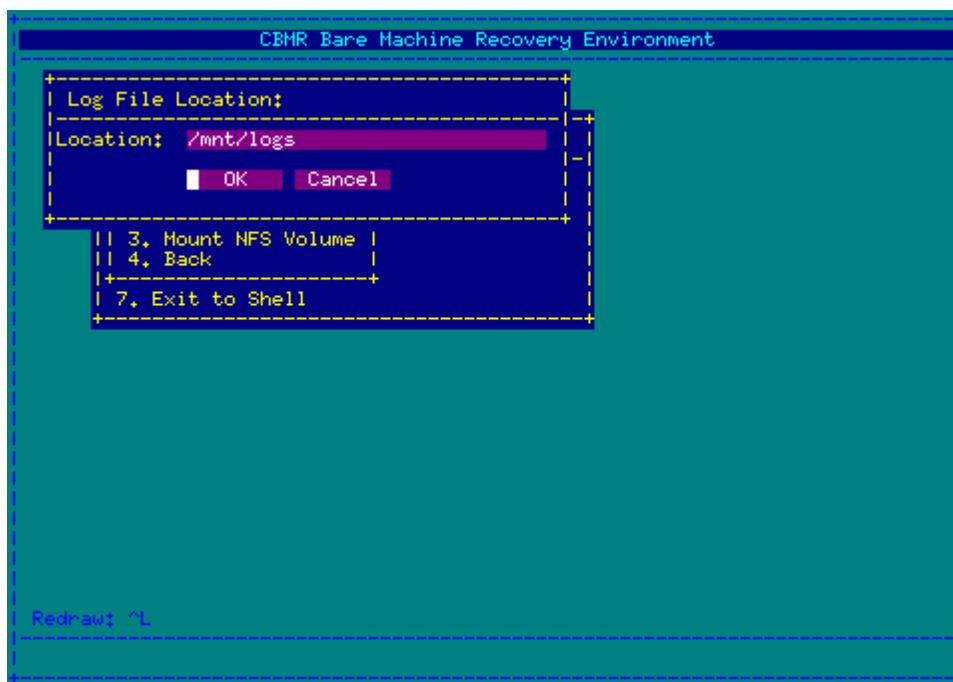
## 8.5 Copying Log Files

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 will ask for a location and create a date-stamped archive of the logs in the directory given.



The log files will be created with a filename in the form:

```
>logs-12:54-10092010.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*

## 8.6 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 operations 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, Make Bootable, has been run, then it will be possible to reboot the machine. However, it is recommended to copy log files to an accessible location (an NFS server, for example) before performing the reboot.

## 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**

<b>Technical Support</b>	+44 (0) 1453 847 009
<b>Toll-Free US Number</b>	1-866-TEC-CBMR (1-866-832-2267)
<b>Knowledgebase</b>	<a href="http://kb.cristie.com">kb.cristie.com</a>
<b>Forum</b>	<a href="http://forum.cristie.com">forum.cristie.com</a>
<b>Sales Enquiries</b>	<a href="mailto:sales@cristie.com">sales@cristie.com</a>
<b>Email</b>	<a href="mailto:support@cristie.com">support@cristie.com</a>
<b>Web</b>	<a href="http://www.cristie.com">www.cristie.com</a>

### **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/](http://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.