TBMR For AIX

Bare Machine Recovery for IBM Spectrum Protect

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

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 TBMR for AIX

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

TBMR 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**

Stages 1 and 3 may be performed using the Graphical User Interface run from the command tbmr. The disaster recovery backup must be performed using the IBM Spectrum Protect backup tools - please refer to your IBM Spectrum Protect documentation for instructions on how to do this.

> *Note: TBMR 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 and IBM Spectrum Protect client/server support and minimum hardware requirements for TBMR Version 9.1.

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

TBMR 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 must be installed prior to the installation of TBMR.

Otherwise the TBMR 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 TBMR 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 tbmr-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 TBMR for AIX Software

At the moment TBMR 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:

```
tbmr-9.1.3266.aix.tar.gz
```

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

TBMR 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 TBMR 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 -l 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

TBMR 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 TBMR 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

TBMR 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 TBMR.

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 tbmr --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 tbmr
```

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

6 Product Licensing

When first installed, TBMR may be used for a trial period of 30 days. During that period TBMR 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.

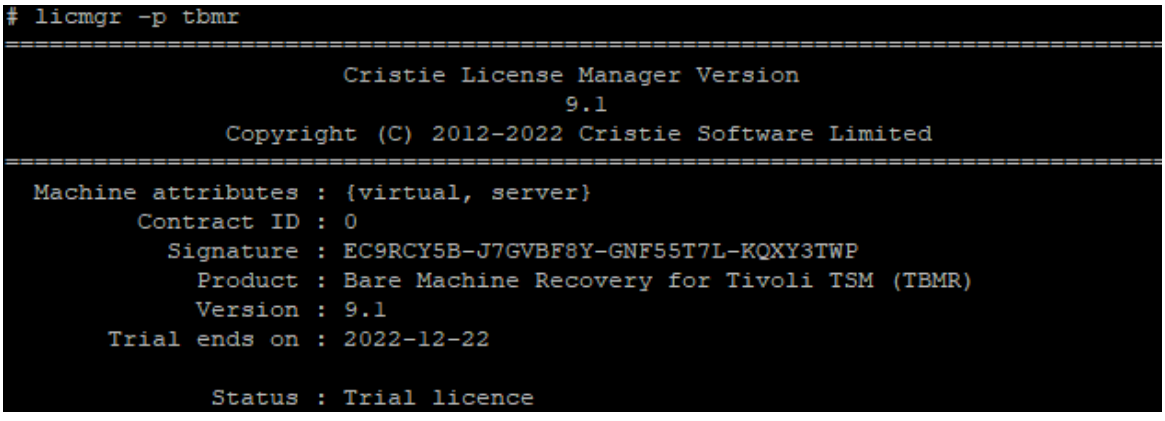
6.1 Trial License

A 30-day trial license commences from the date of installation. The TBMR configuration file generator tbmrcfg 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 tbmr
```

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.



The TBMR 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 TBMR is already installed on a Customer production machine.***

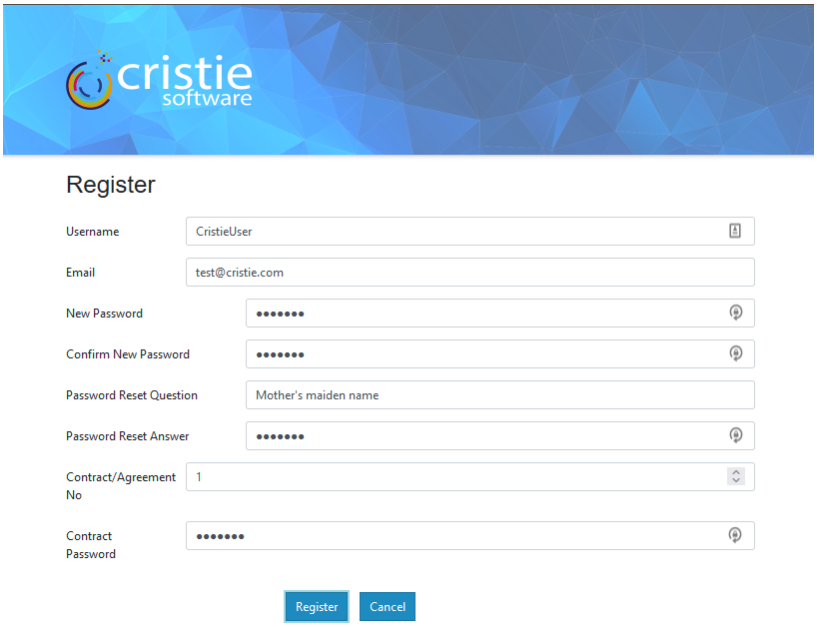
6.2.1 Setting up a Cristie Licensing Portal account

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.

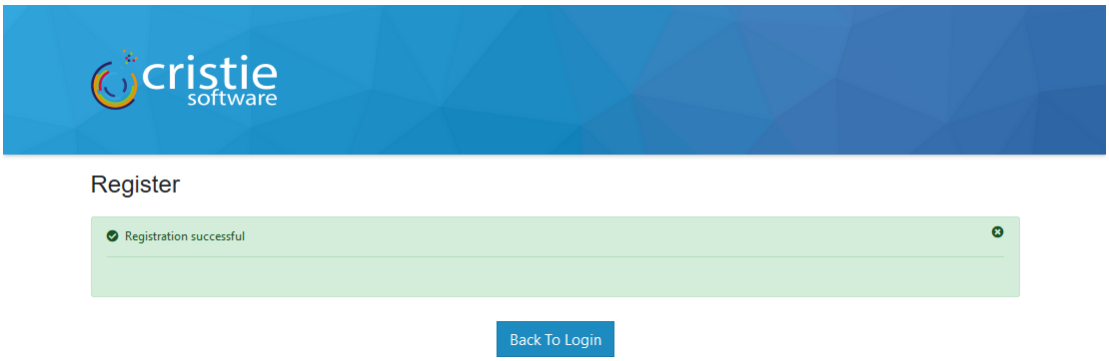
> ***Note: Your Contract ID may have been supplied to you as your contract Agreement Number. In that case please use your Agreement number in place of the Contract ID throughout.***

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):



Then click Register. 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.

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 TBMR host machine by opening up a terminal and entering:

```
licmgr -p tbmr --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 tbmr output.

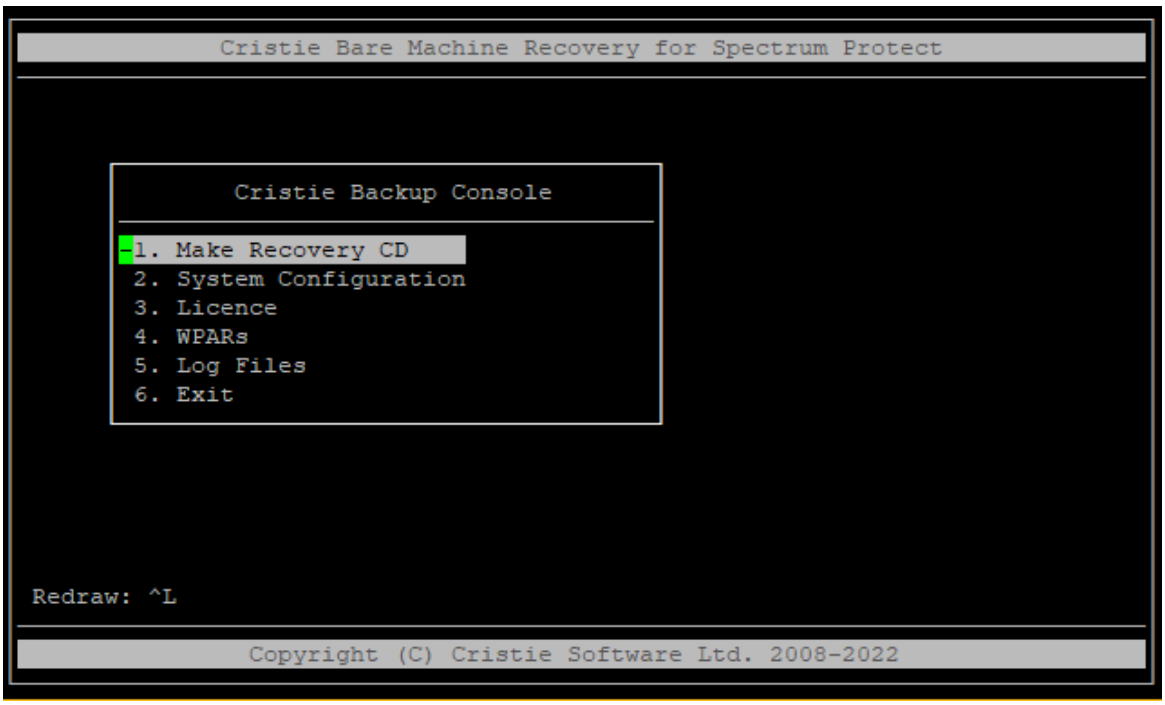
```
# licmgr -p tbmr
================================================================================
                      Cristie License Manager Version
                                      9.1
               Copyright (C) 2012-2022 Cristie Software Limited
================================================================================
  Machine attributes : {virtual, server}
         Contract ID : 0
           Signature : EC9RCY5B-J7GVBF8Y-GNF55T7L-KQXY3TWP
             Product : Bare Machine Recovery for Tivoli TSM (TBMR)
             Version : 9.1
       Trial ends on : 2022-12-22

              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.

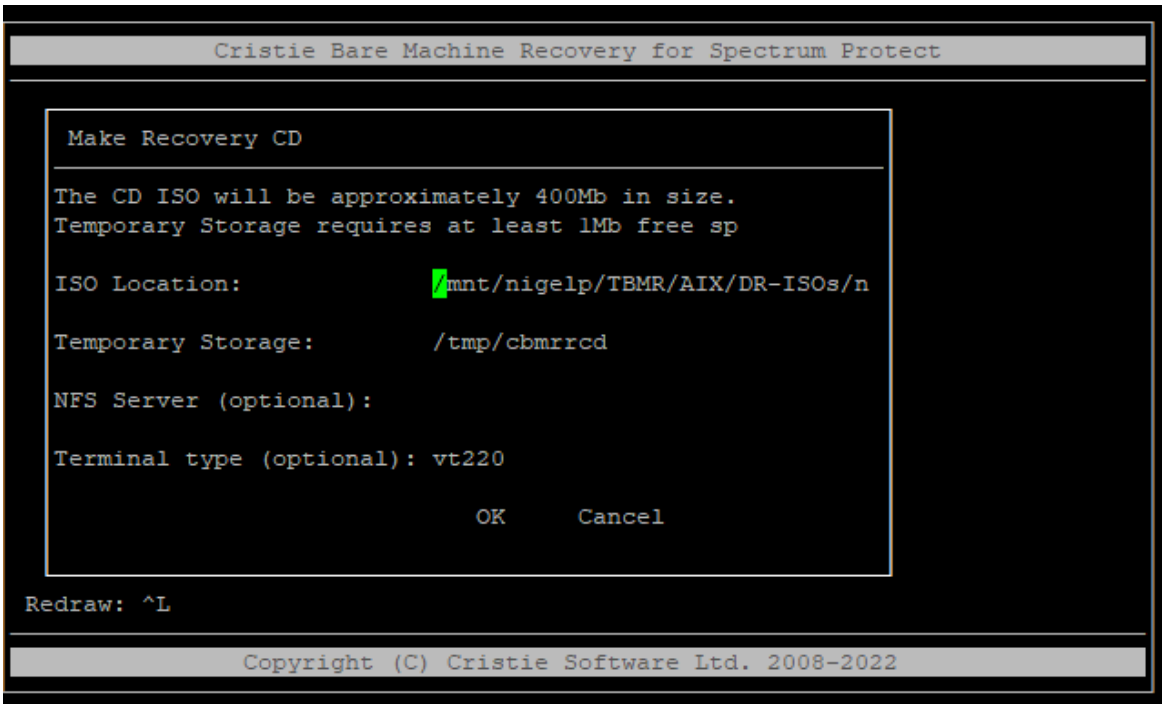
```
================================================================================
                      Cristie License Manager Version
                                      9.1
               Copyright (C) 2012-2022 Cristie Software Limited
================================================================================
Successfully applied the activation code.
  Machine attributes : {virtual, server}
         Contract ID : 3
           Signature : EC9RCY5B-J7GVBF8Y-GNF55T7L-KQXY3TWP
             Product : Bare Machine Recovery for Tivoli TSM (TBMR)
             Version : 9.1
 Maintenance ends on : 2022-12-30

     Activation code : YSRB8N2A-NJASJAUJ-8KXX7V2Z-QKYLHPGG
     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 TBMR Graphical User Interface. After entering the command '`tbmr`', the TBMR Console menu is presented:



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.



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.

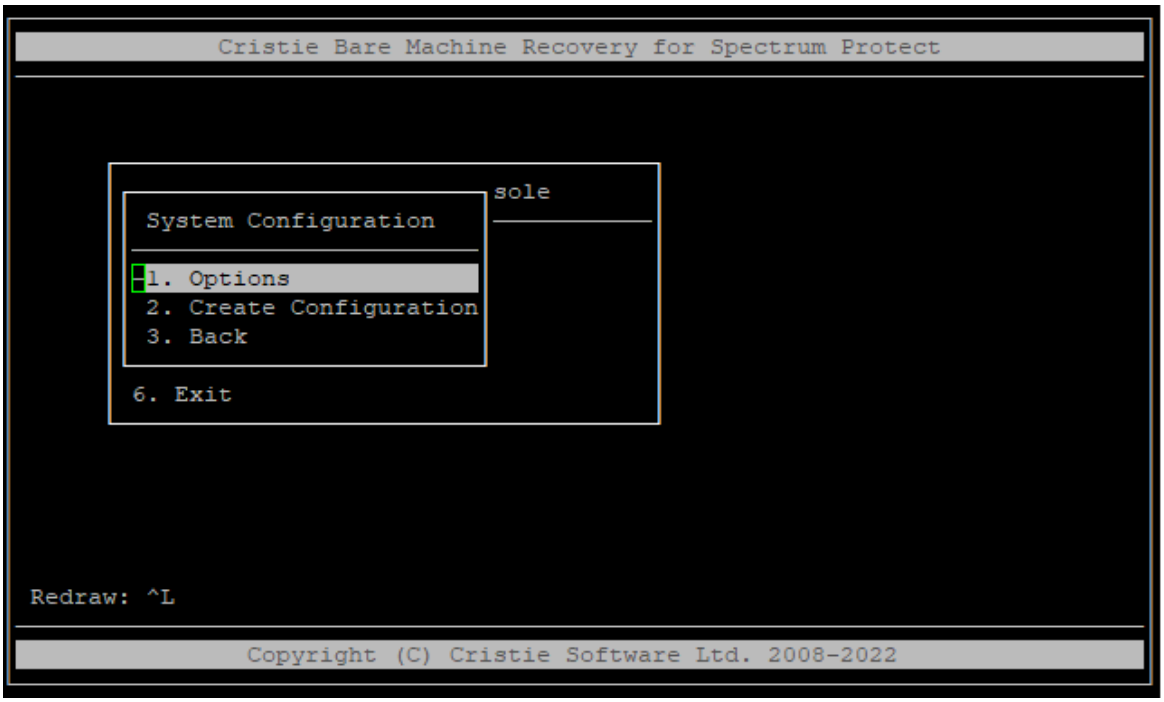
2. **Perform** the system backup using IBM Spectrum Protect.

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).

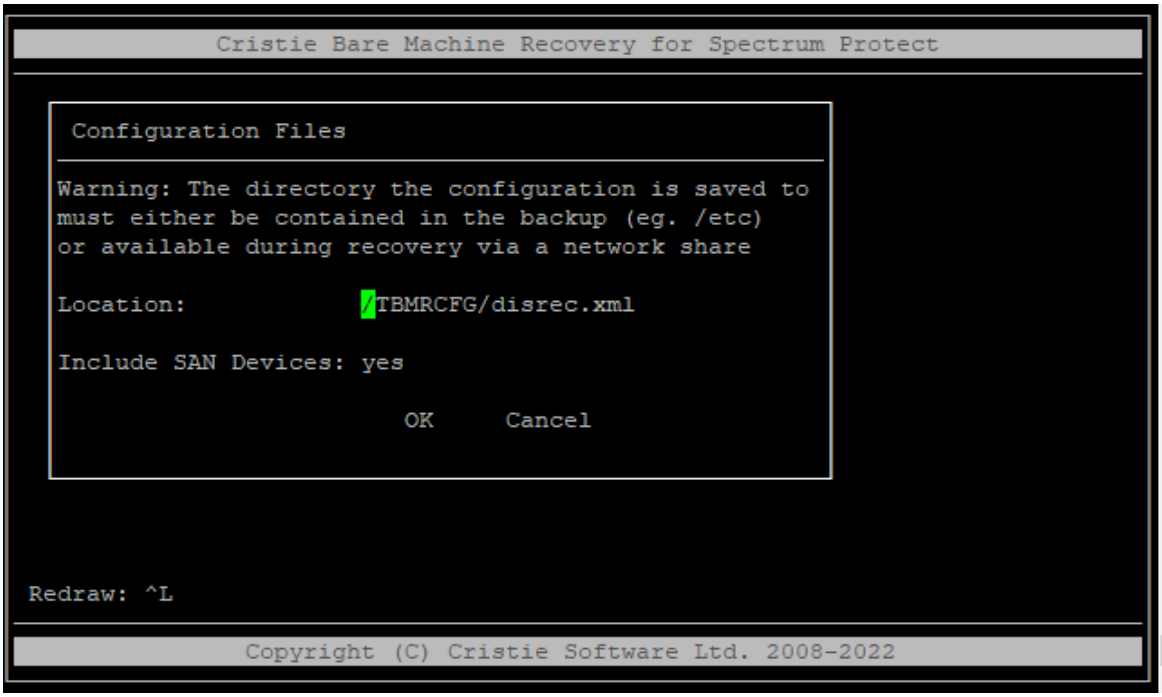
8.1 Recording System Information

The system information must be recorded and stored so that the system can be rebuilt at recovery time. This is performed using the `tbmrcfg` 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:



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



Location

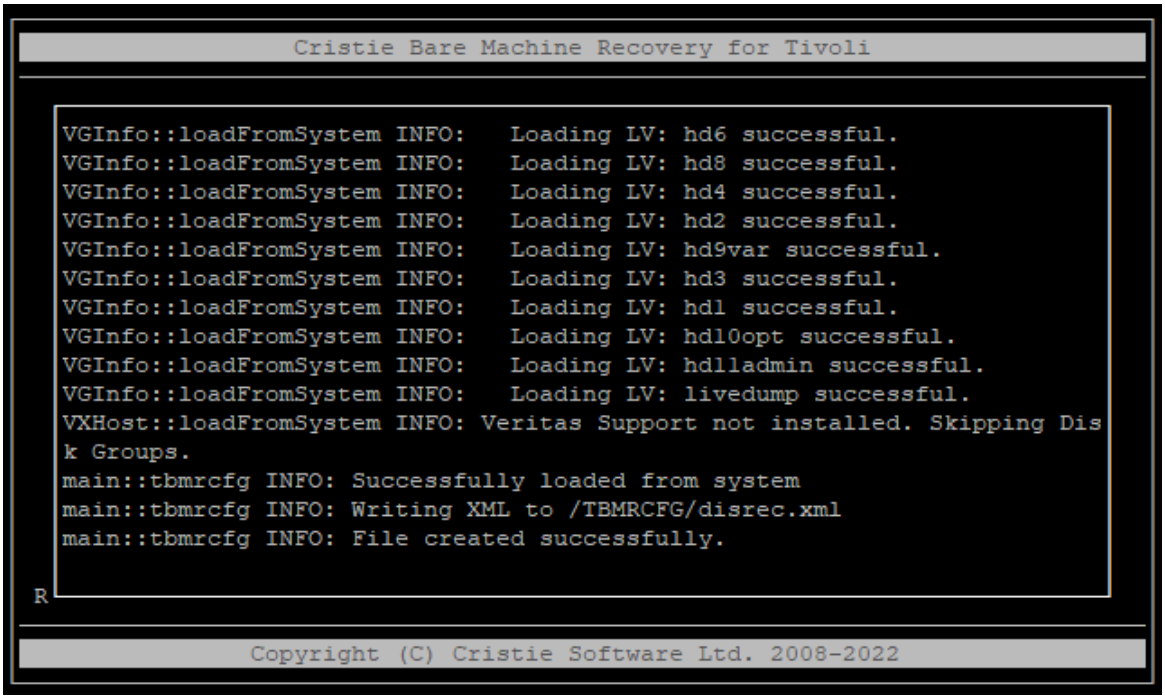
The default location for the configuration file is `/TBMRCFG/disrec.xml`. Cristie recommends leaving the location at this default value.

> ***Note: the location chosen MUST be included in the file paths specified in dsm.sys or dsm.opt. If you change the location of the configuration information, ensure this is included in the backup script***

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.

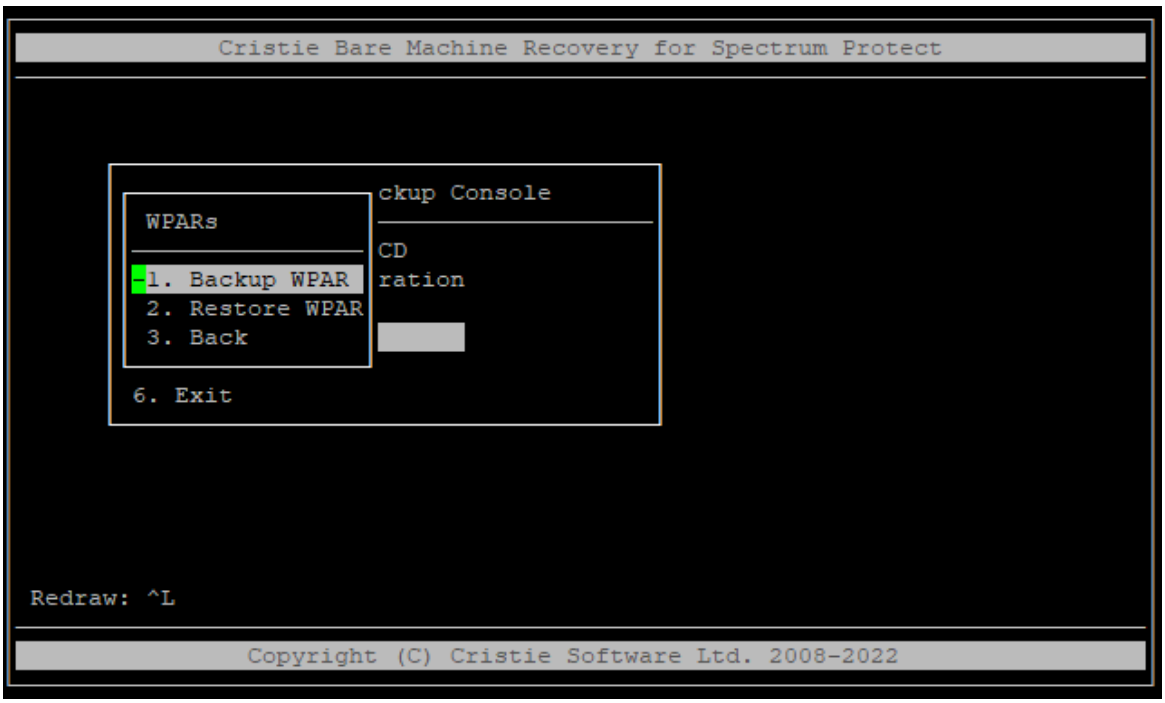
When running the configuration tool information, the current operations are displayed:



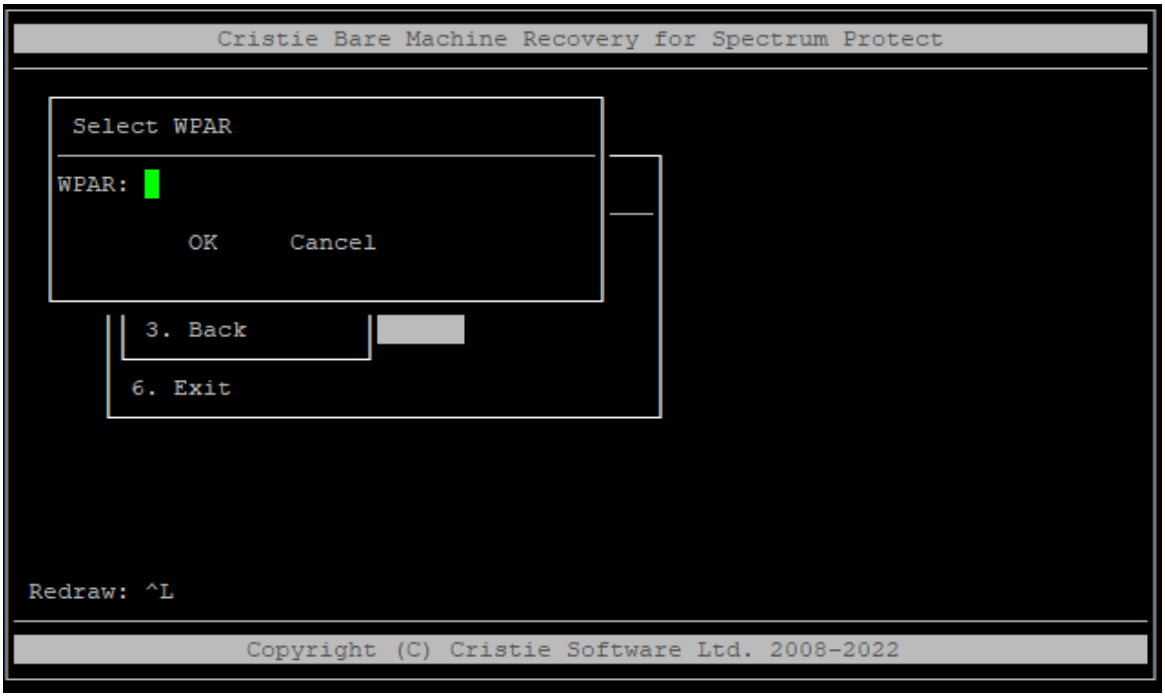
Once this operation is complete, the log fine can be found in `/var/log/cristie/tbmrcfg.log`. This may also be viewed using the **Log Files** submenu.

8.2 WPARs

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



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



8.3 Create the IBM Spectrum Protect Backup

Once the configuration is generated and saved you can now run a normal IBM Spectrum Protect backup.

Ensure you do not exclude any system directories such as `/dev`. You can use a command of the form **dsmc incremental** to perform the backup on the command line.

> ***Note: Don't forget to install any certificate you need to connect to your chose IBM Spectrum Protect server. You will also need this certificate during the recovery process.***

9 Performing a 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:

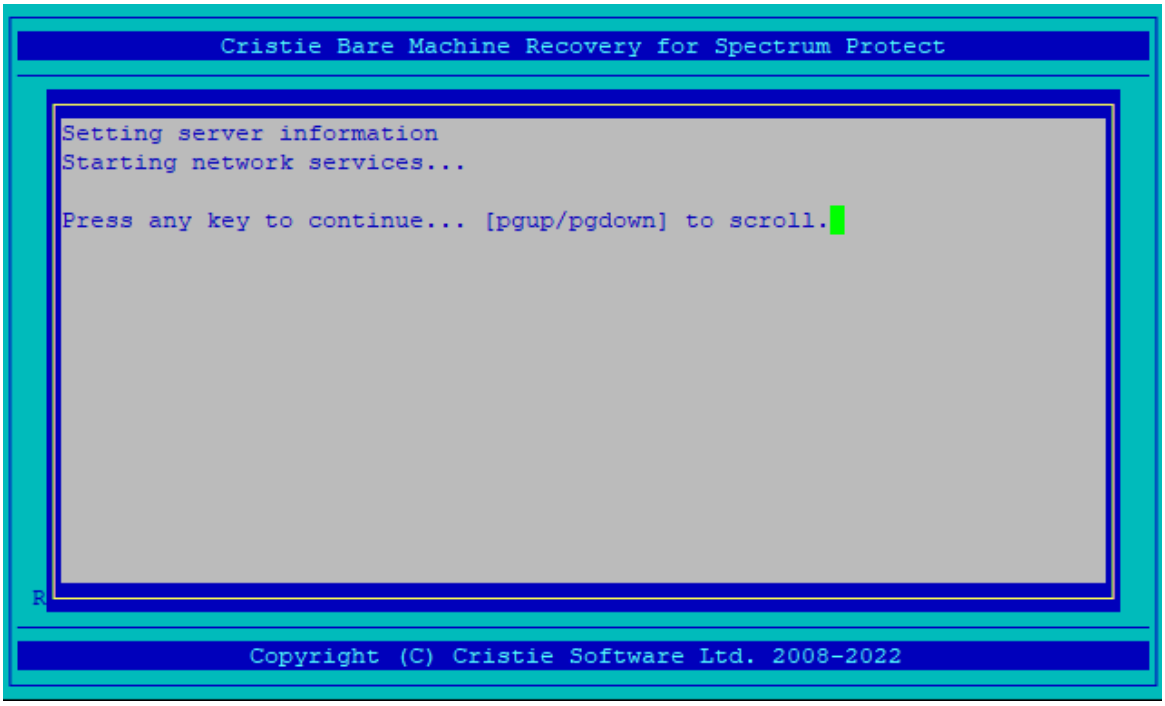
1. **VXDisks** - make disks available for use with Veritas.
2. **VXGroups** - create Veritas Volume Groups.
3. **VXVolumes** - create Veritas Volumes.

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.

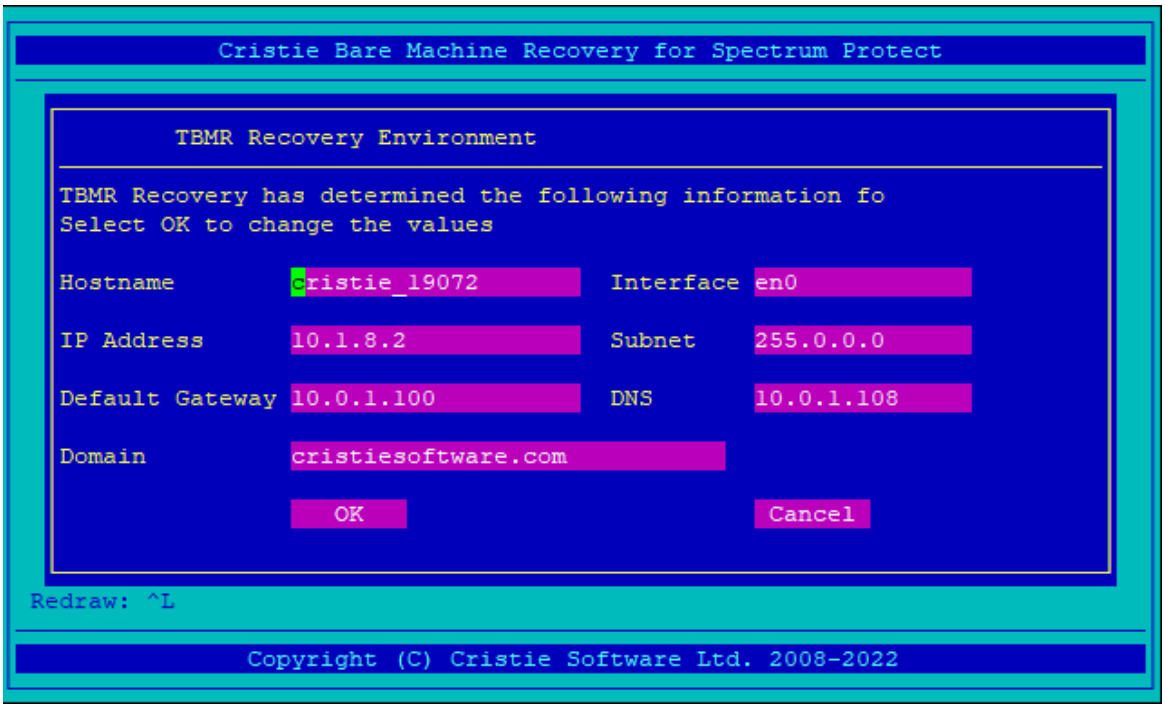
Before re-boot, however, it is very useful to make a copy of the log files generated during the recovery as shown in Copying Log Files.

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.**

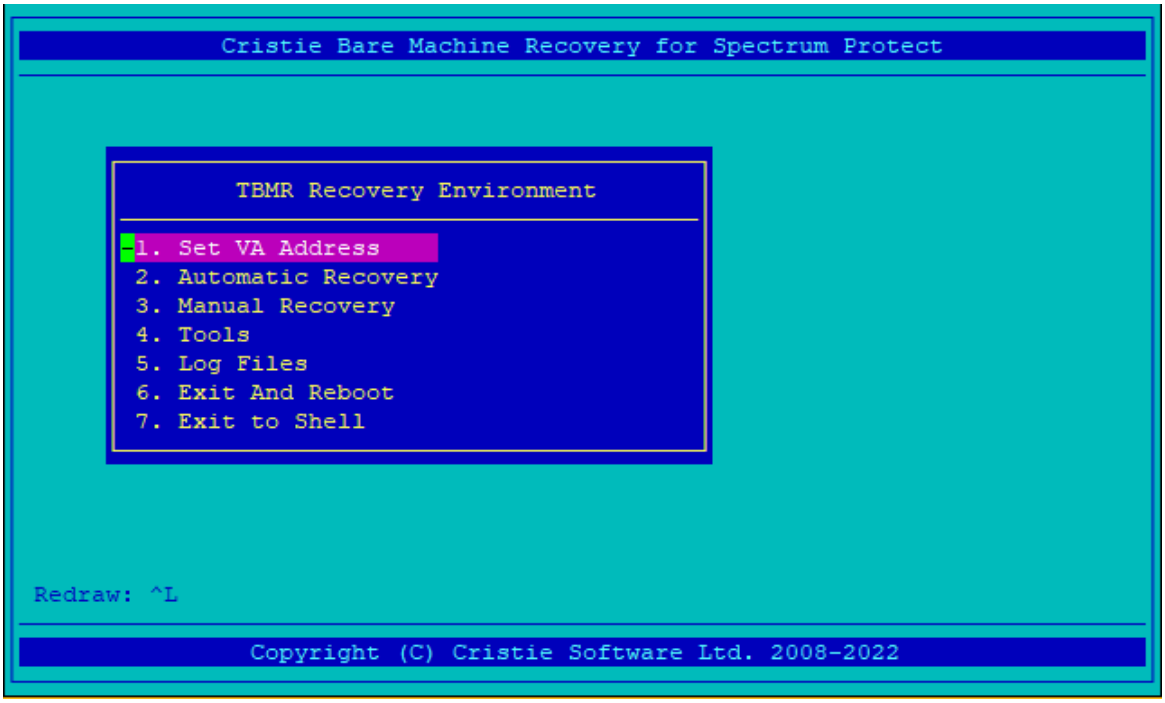


Next you should configure the recovery environment hostname and network details.



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:



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.

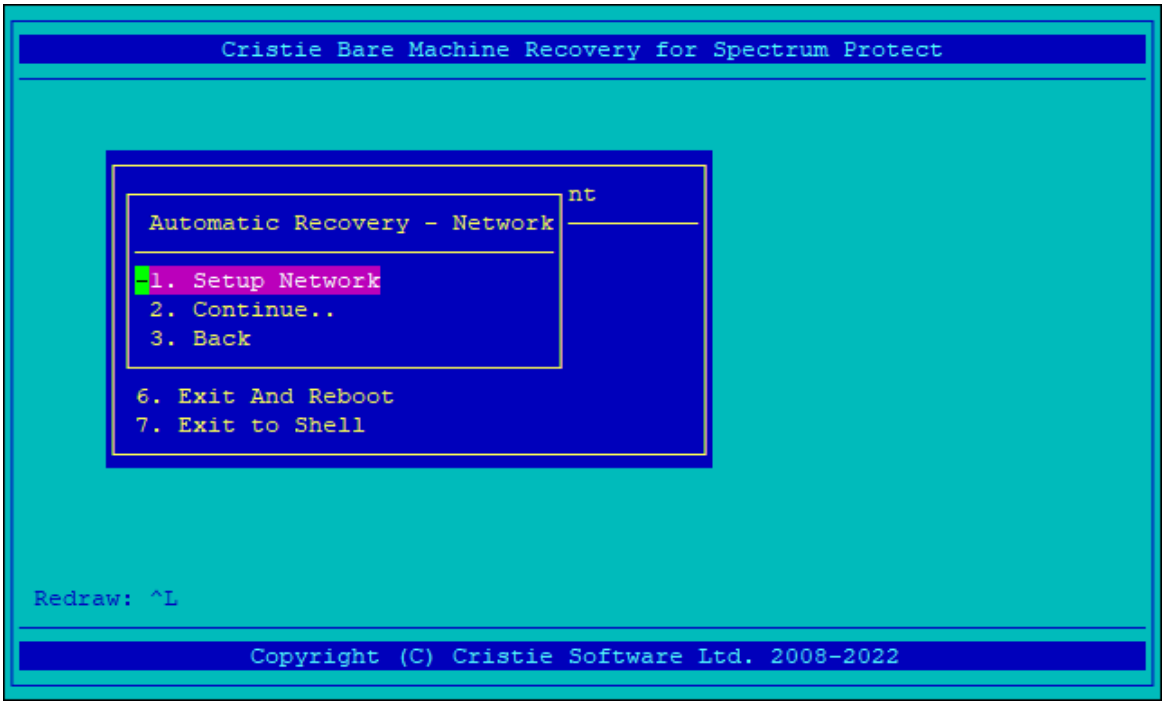
- The **Automatic Recovery** runs through all stages of the recovery and only provides options to recover just the root volume group or the whole machine
- The **Manual Recovery** allows the option of recovering only selected volume groups and running selected phases of the recovery individually

> ***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***

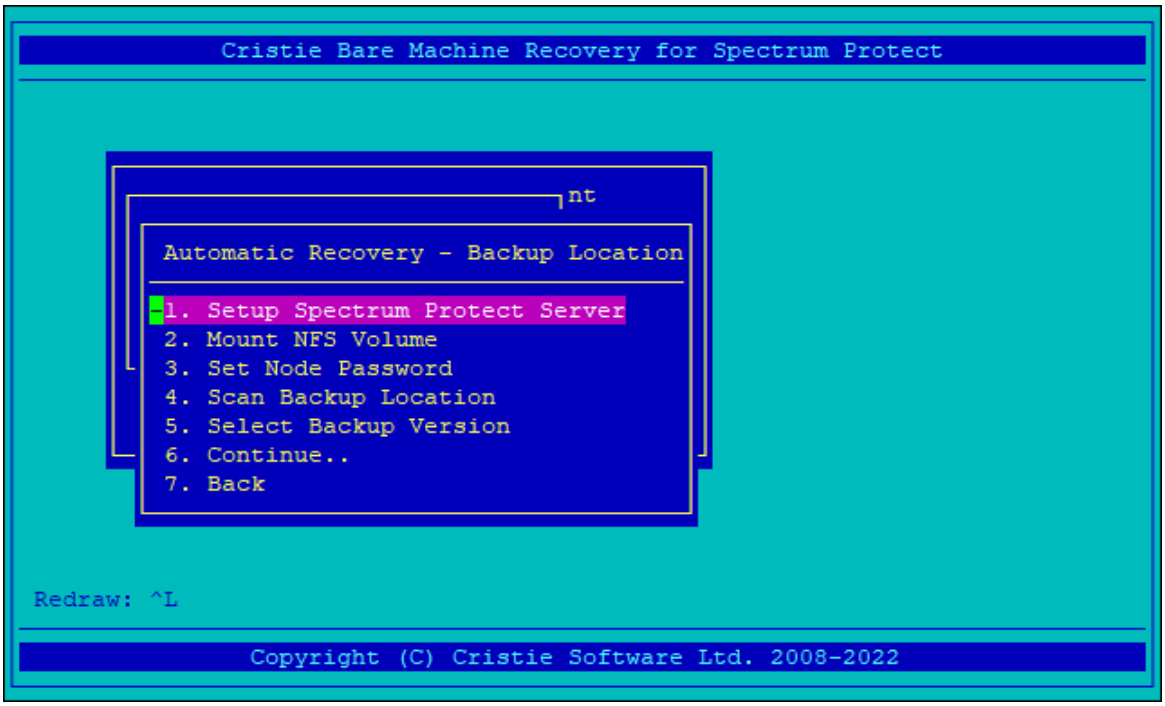
9.1.1 Automatic Recovery

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

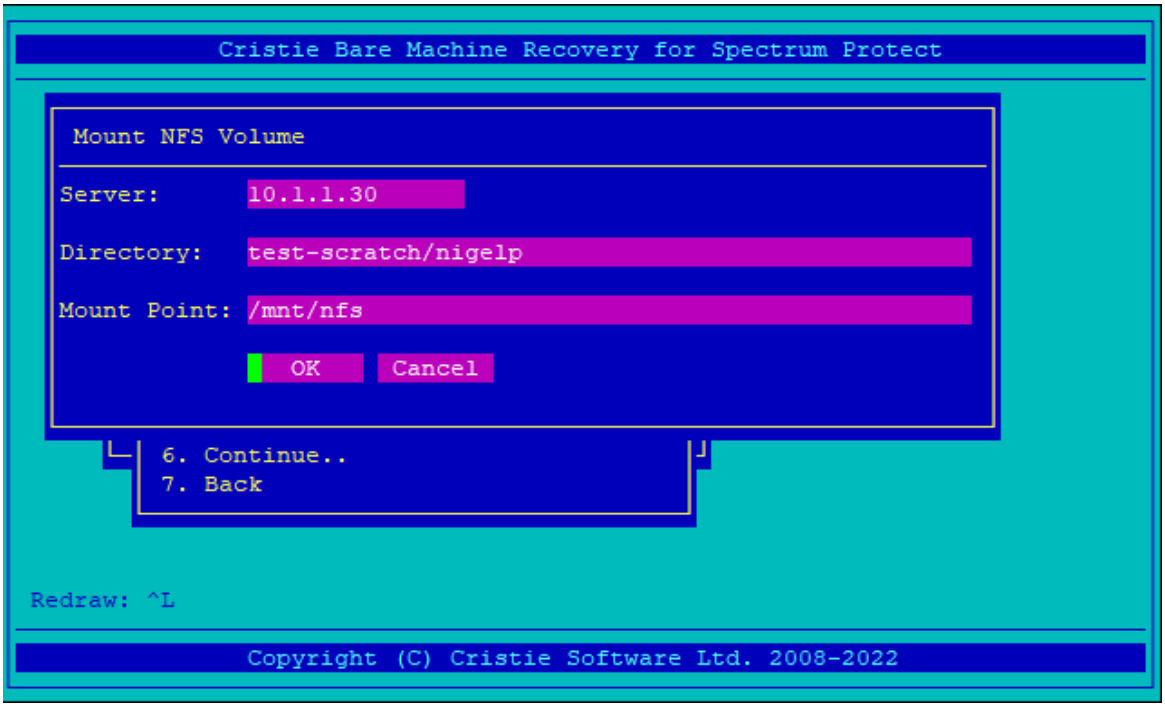
1. **Setup Network** - if initial setup was unsatisfactory
2. **Backup Location** - specify the attributes of the location containing the backup
3. **Configuration** - read machine configuration information and set applicable options
4. **Perform Recovery** - start the recovery procedure
5. **Copy Log Files** - copy the log files generated by the recovery



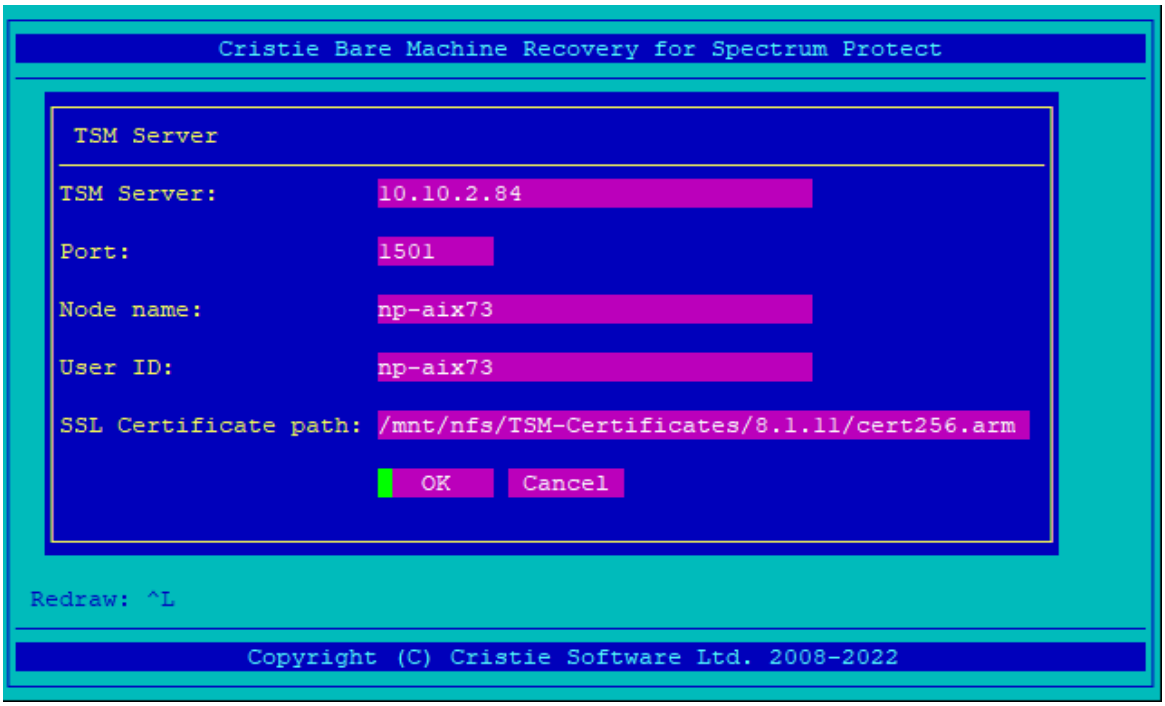
First select **Setup Network** if initial setup was unsatisfactory. Otherwise select **Continue**.



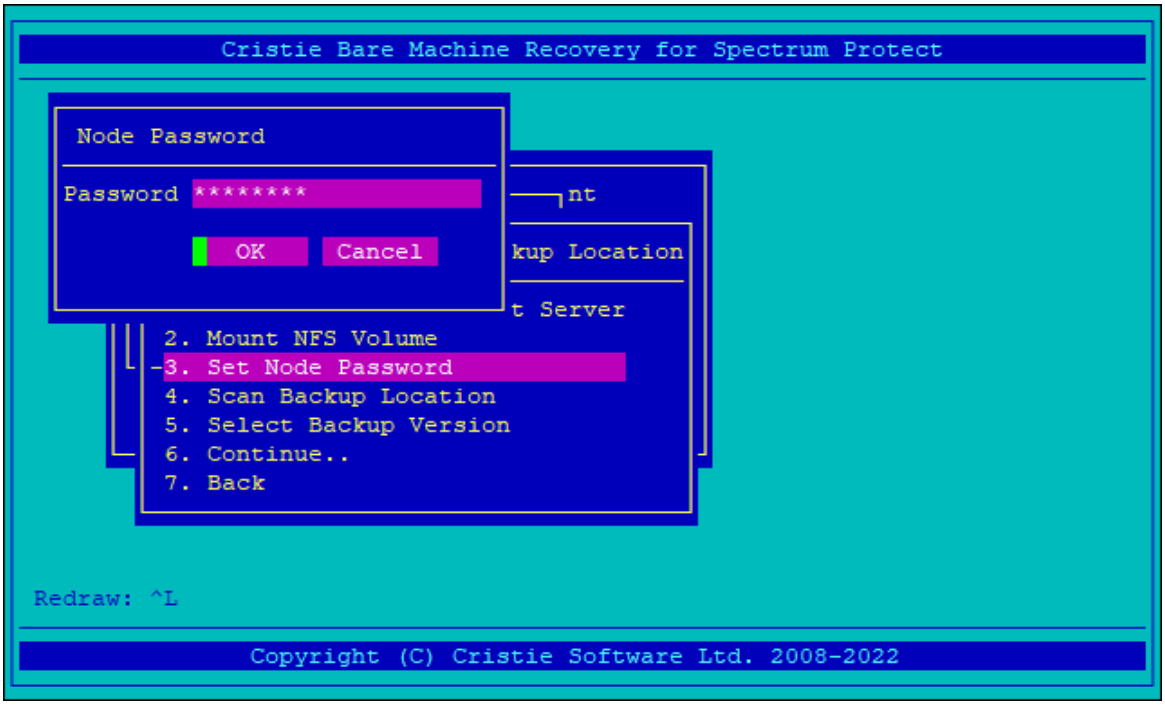
Now setup the IBM Spectrum Protect server details. If the server requires an SSL certificate that resides on a network share you will need to configure the share with **Mount NFS Volume** first.



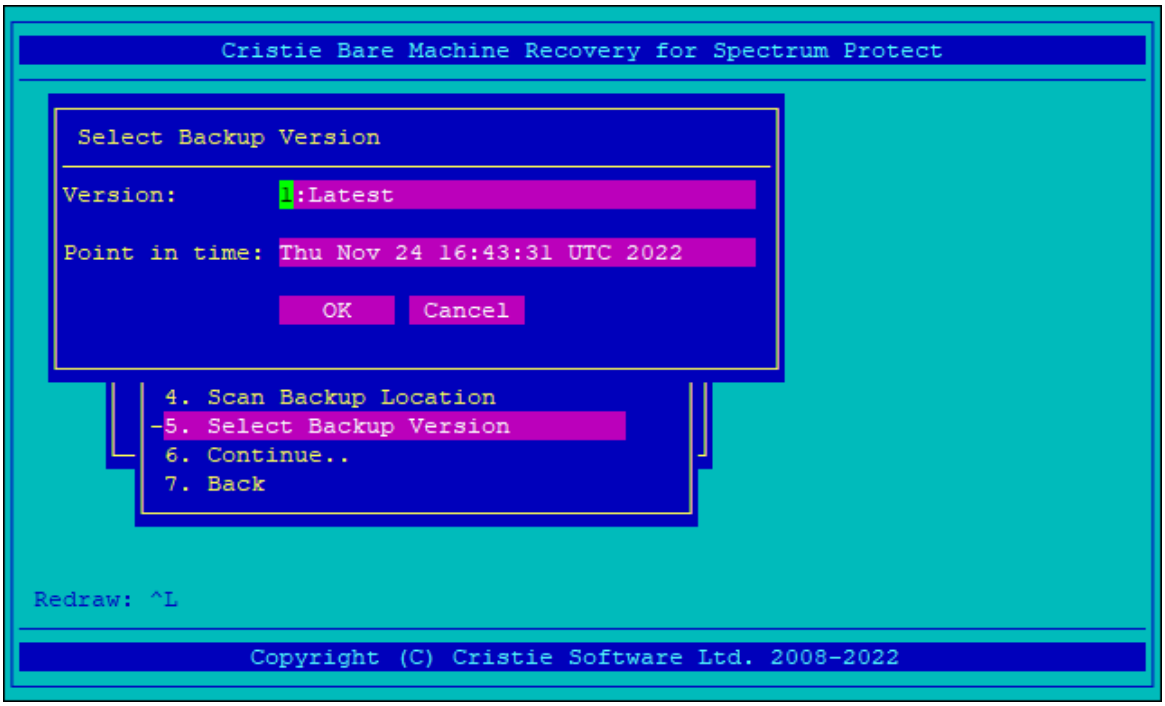
Select OK and then select **Setup Spectrum Protect Server** to add the **Server IP address**, **Port**, **Backup Node name** (and **User ID** if required) and the **SSL Certificate path**.



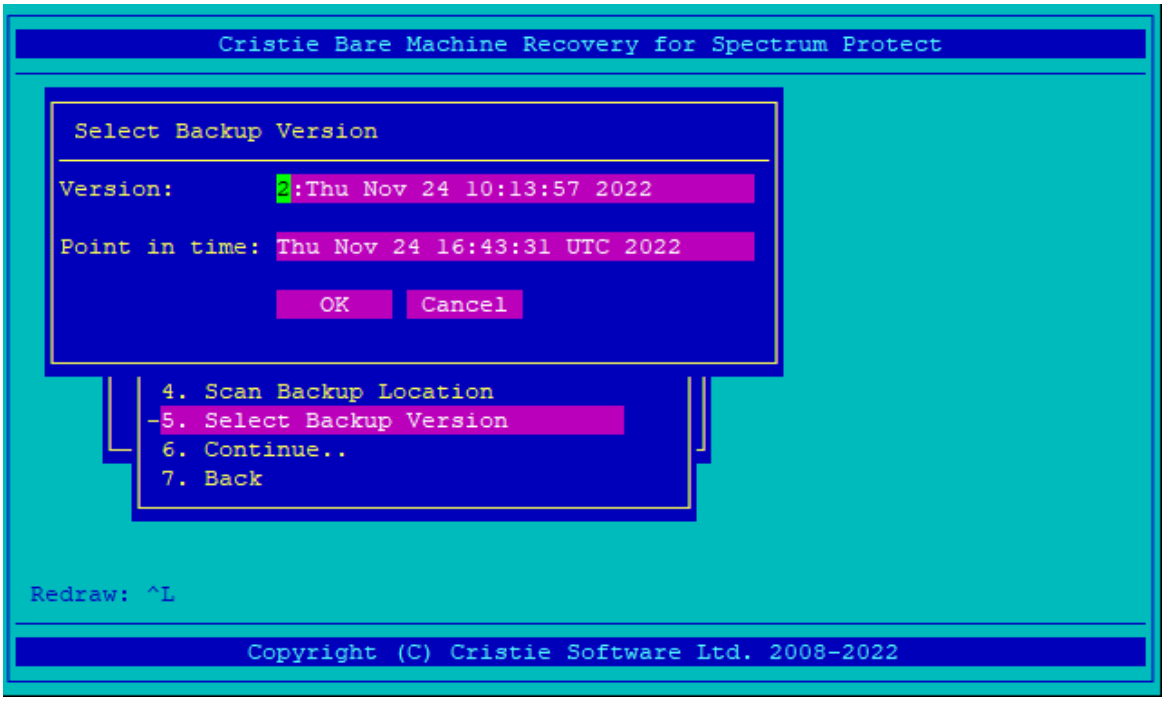
Select OK and then **Set Node Password**. Specify the password for the Node required.



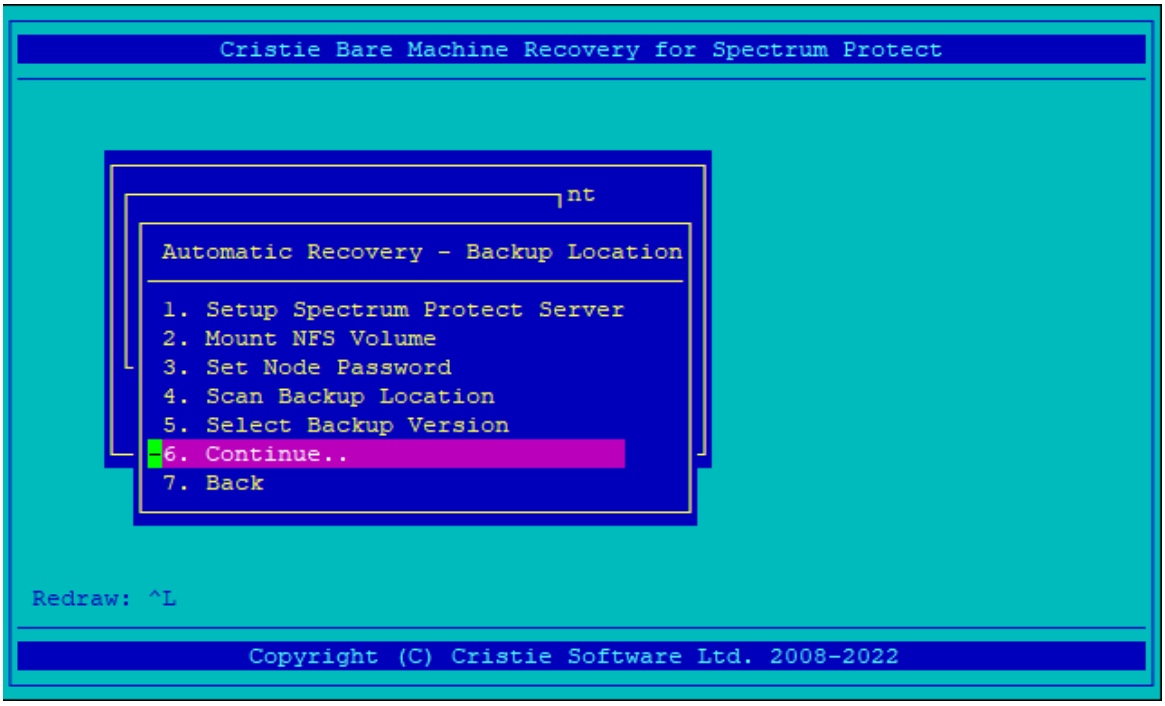
Select OK and then **Select Backup Version** if your node contains several backups and you wish to recover your system to a specific **Point In Time** (**PIT**).



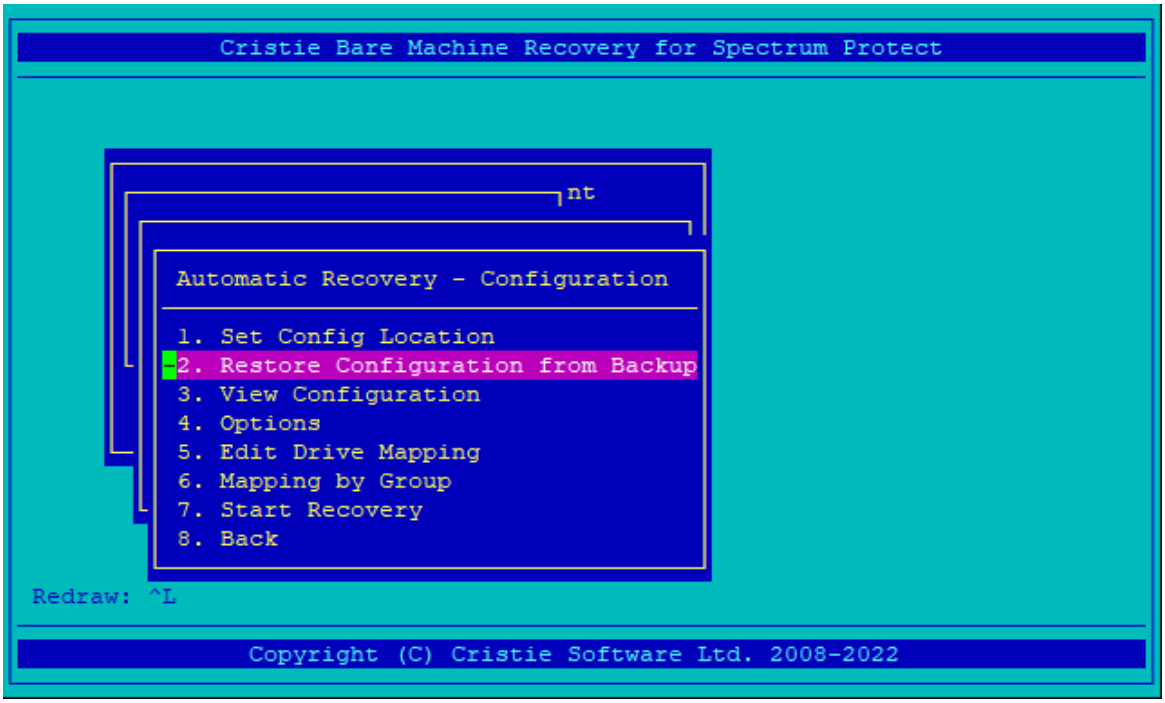
If you don't want the Latest version (the default) use the arrow keys on the **Version** field and it will show which PIT backups are available. For example:



When you have selected the required version click OK to continue. Select **Scan Backup Location** to check the IBM Spectrum Protect Server and Node is accessible. Then on the **Automatic Recovery** menu select **Continue.**



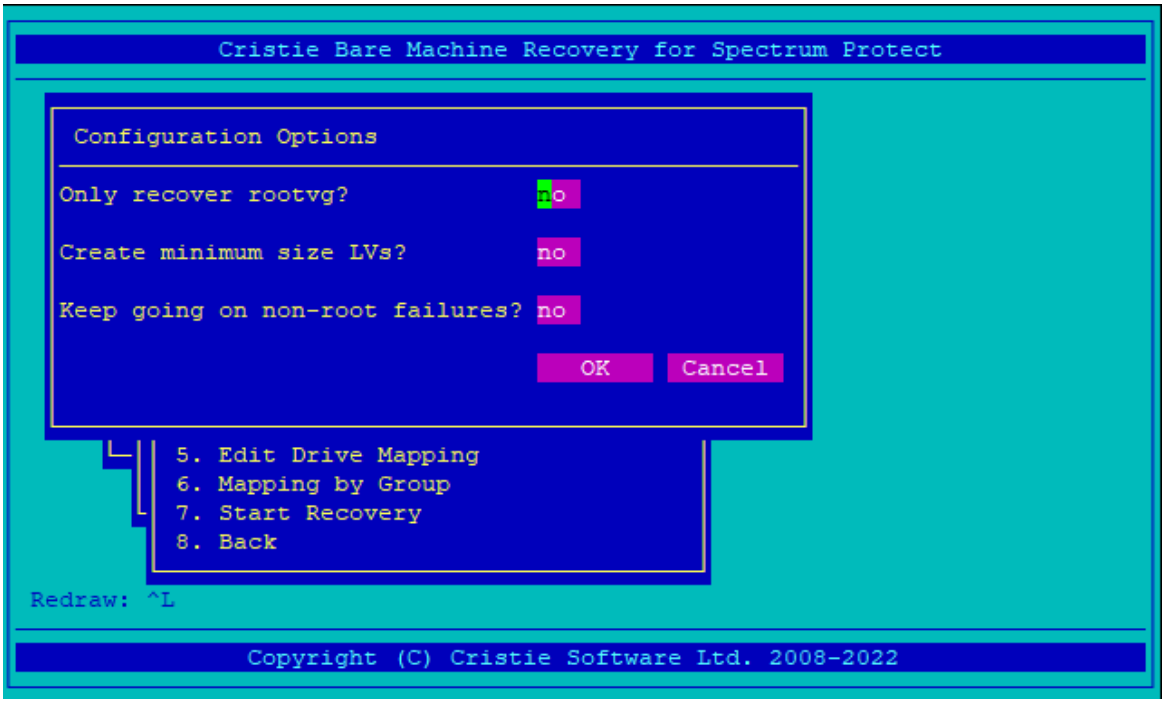
Now select **Restore Configuration from Backup**. You need to do this first so that the disk/ volume configuration can be created on the target. The server is accessed and the configuration restored according to the PIT selected.



Once the configuration has been restored successfully you may reconfigure the target disk layout.

```
  Client date/time: 11/24/22    16:56:11
(c) Copyright by IBM Corporation and other(s) 1990, 2022. All Rights Reserved. N
ode Name: NP-AIX73
Entering username
Please enter your user id <NP-AIX73>:
Entering password
Please enter password for user id "NP-AIX73":
Session established with server TSM817: Windows
  Server Version 8, Release 1, Level 14.000
  Server date/time: 11/24/22    16:31:53  Last access: 11/24/22    16:19:04
Restore function invoked.
Restoring          24,907 /TBMRCFG/disrec.xml --> /TBMRCFG/disrec.xml [Done]
Restore processing finished.

Total number of objects restored:             1
Total number of objects failed:               0
Total number of bytes transferred:        24.35 KB
Data transfer time:                        0.01 sec
Network data transfer rate:            2,344.12 KB/sec
Aggregate data transfer rate:              7.77 KB/sec
Elapsed processing time:                00:00:03
Creating disk mapping...
Press ENTER to continue...
```

Press ENTER to return to the **Automatic Recovery** menu. Selecting the **Options** item displays any additional options that can be applied at this point.

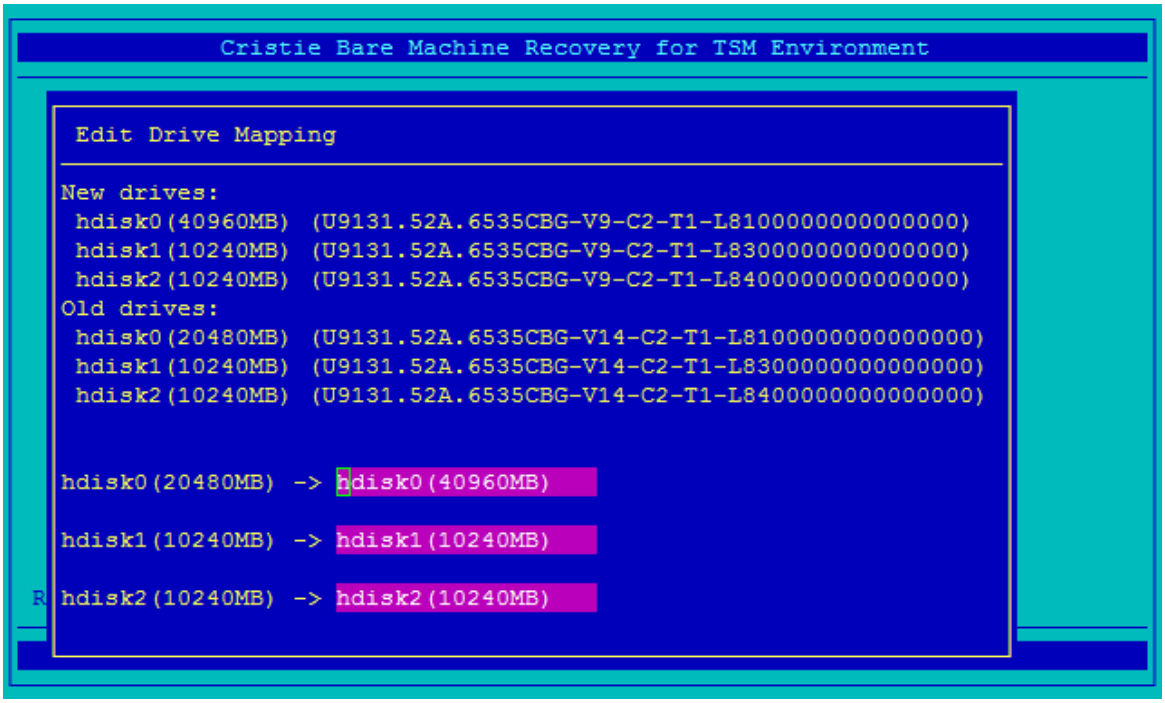


Create Minimum Size LVs: This option ensures that the logical volumes created are of the smallest size such that the data to restore fits. This option is useful if you are recovering to a machine with smaller disks.

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. if only recover root VG is selected it is possible in Group Mapping to map the rootvg disk onto a disk assigned to another volume group, thereby overwriting that disk. If an attempt is made to place rootvg onto another disk already assigned to another volume group a warning is displayed.

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.

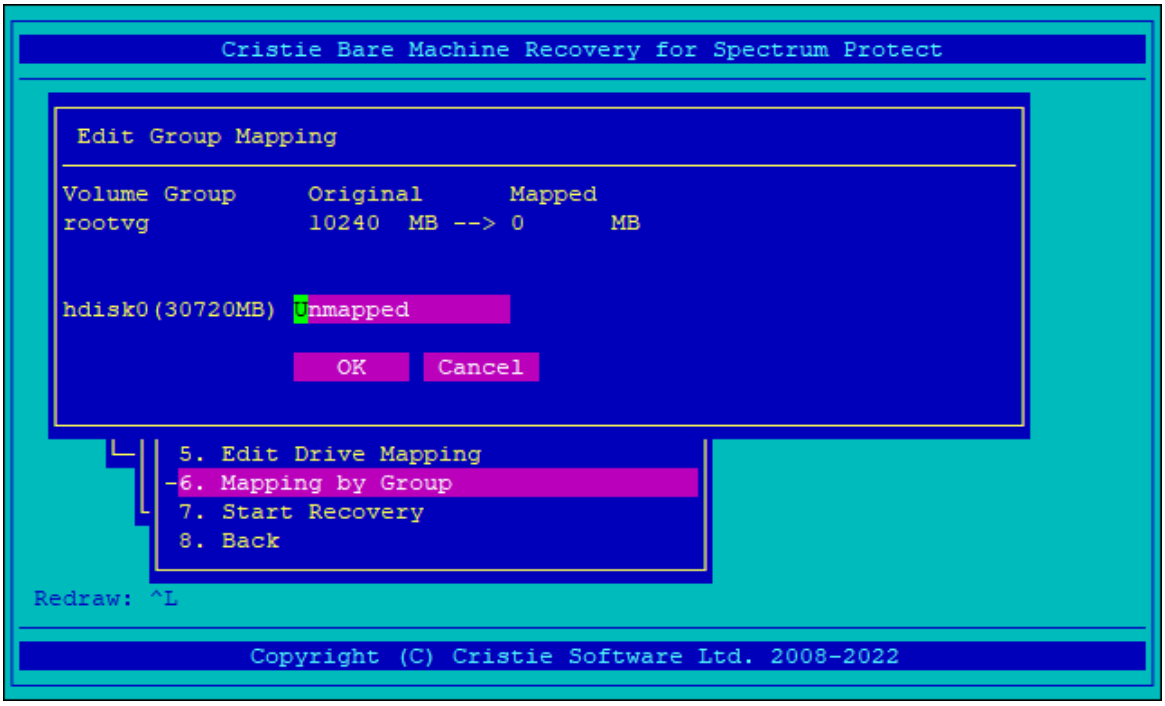
> ***Note: the minimum size calculation is performed when the configuration information is recorded but it is re-calculated when the backup is accessed.***



The **Edit Drive Mapping** menu option is used to modify the disks that the backup is restored to.

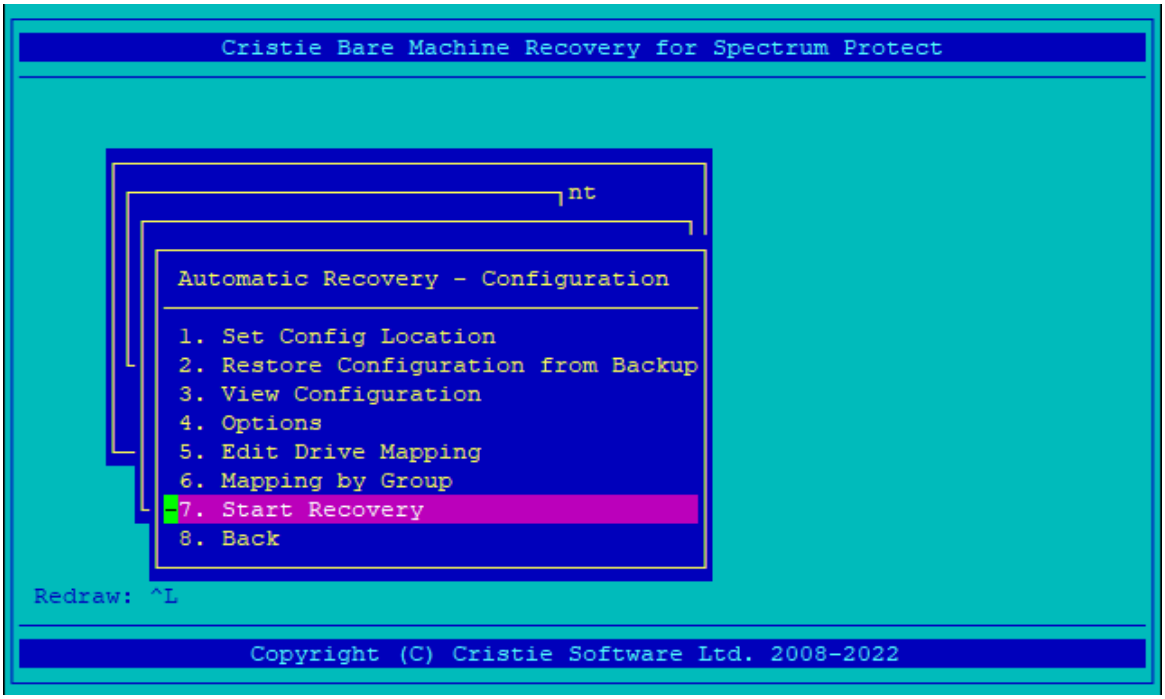
> *Note: Should the drive display spread over more than one screen you can navigate forwards Ctrl +N or the previous page Ctrl +P*

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.

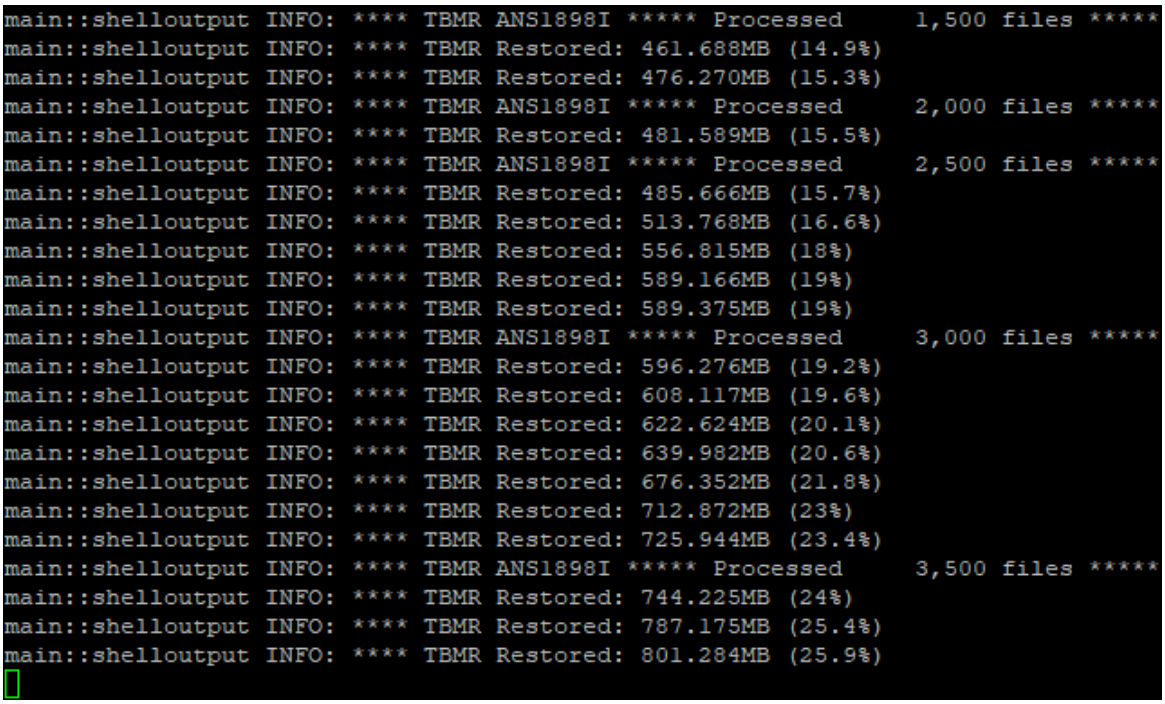


The **Edit Group Mapping** item is used to modify the disks that the backup is restored to by selecting which disks belong to which volume group. In the example given both disks are given to the rootvg volume group and the testvg volume group is given one, so is not restored. The same rules for recovering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

Now select **Start Recovery**.



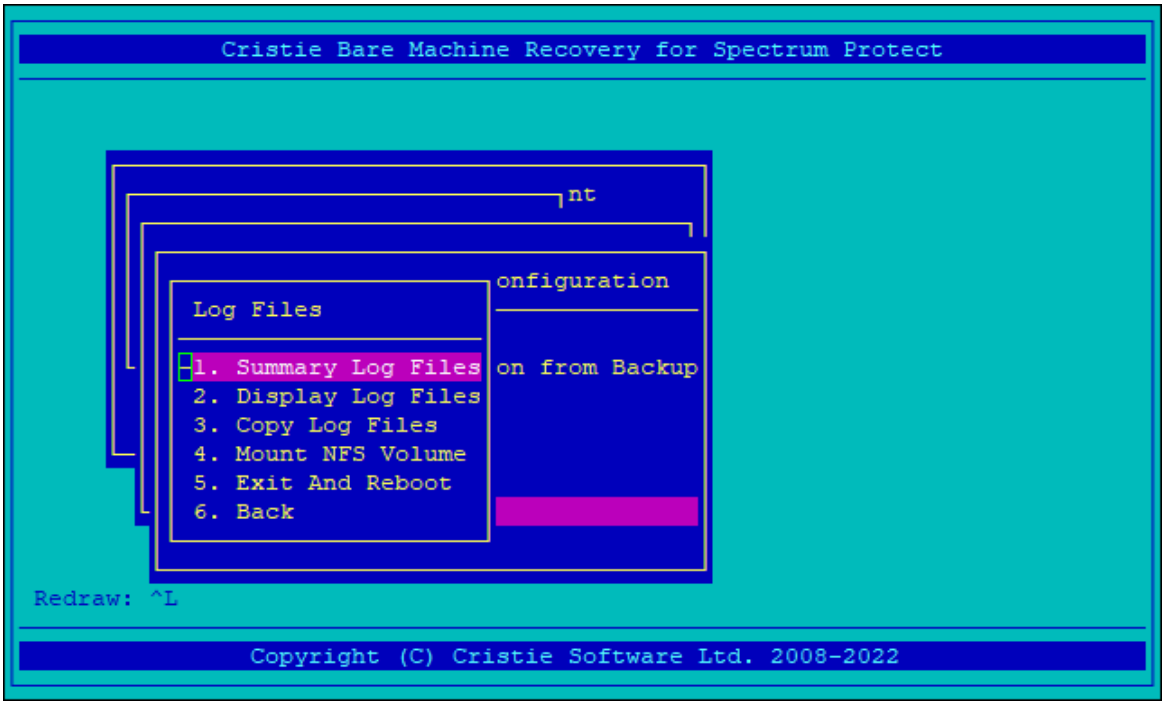
The recovery proceeds.



when complete you will see this:

```
main::shelloutput INFO: >>CS 6291826 6947308 17:10:38.090 bootlist -m normal -o
main::shelloutput INFO: >>
main::shelloutput INFO: >>CS 6619404 6422980 17:10:38.132 bootlist -m normal hdi
sk0
main::shelloutput INFO: >>
main::shelloutput INFO: >>CS 6619406 6422980 17:10:38.146 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: 2022-11-24T17:10:46Z
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...
```

Select Enter and you will then be shown the **Log Files** menu.



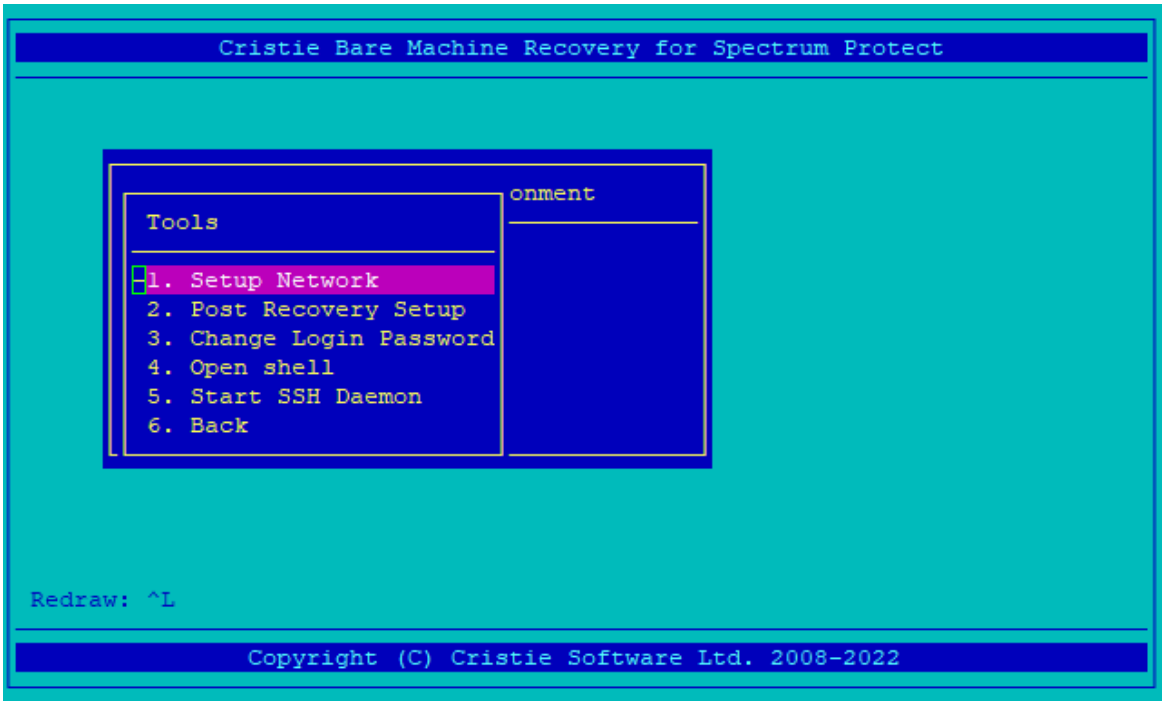
It is recommended that Log Files are copied to a network share as a precaution in case the booted system does not boot correctly or the target configuration is created incorrectly. Use **Copy Log Files** to do this but you may need to mount a network share first. Use **Mount NFS Volume** to do this.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

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

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

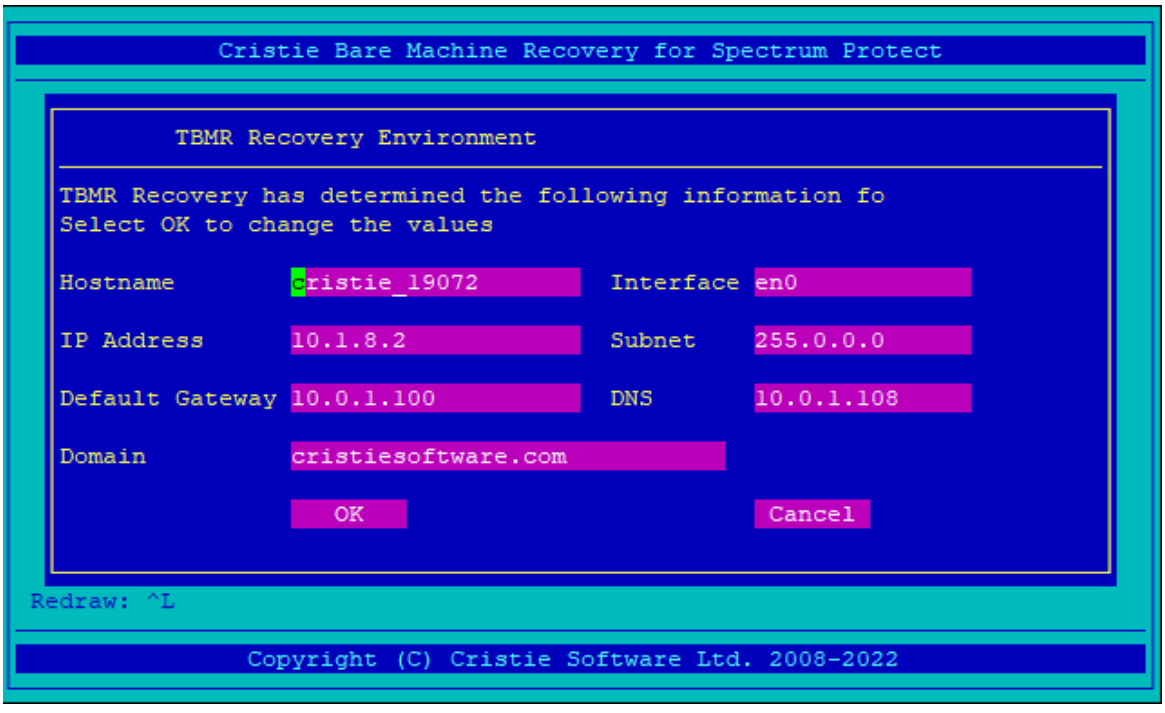
9.1.2 Tools

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



9.1.2.1 Setup Network

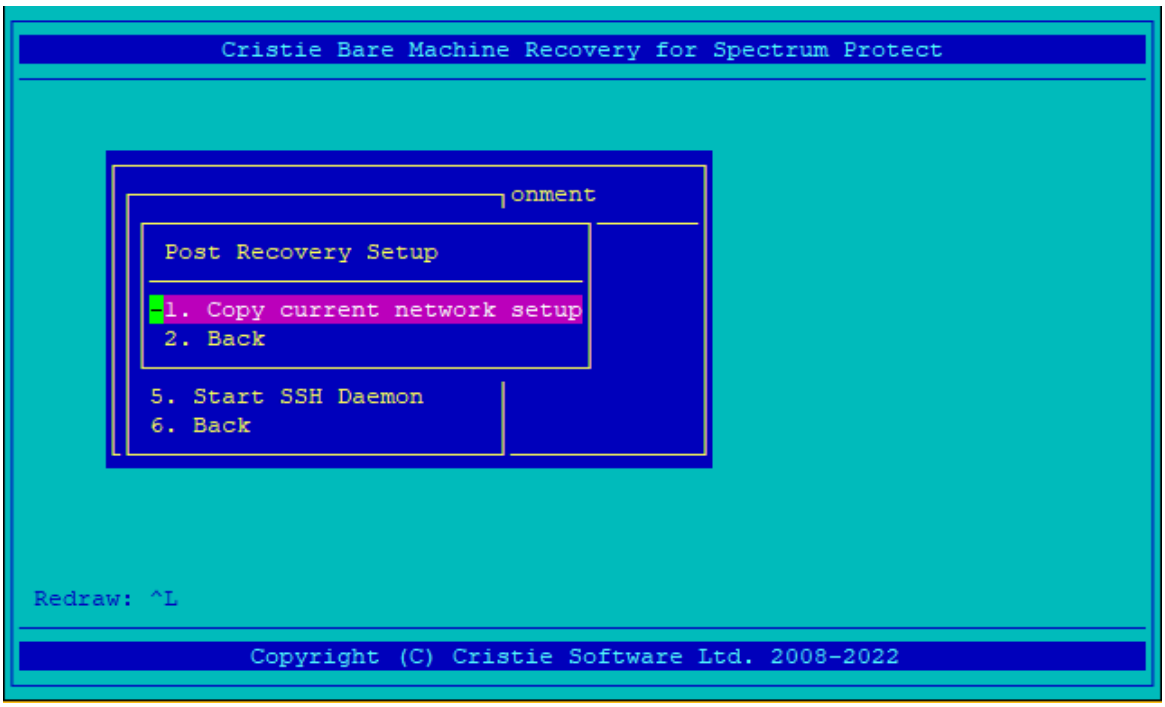
At any point you can configure the recovery environment hostname and network details.



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.

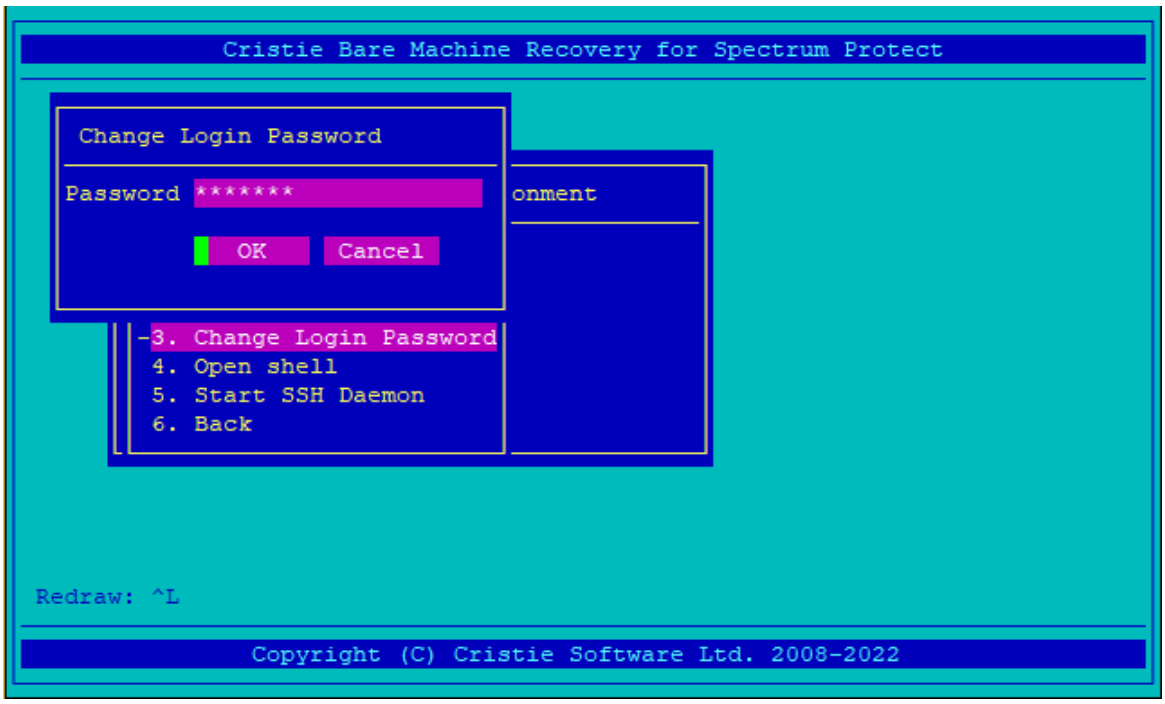


This is a useful option if you are cloning or moving a recovered machine.

> *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

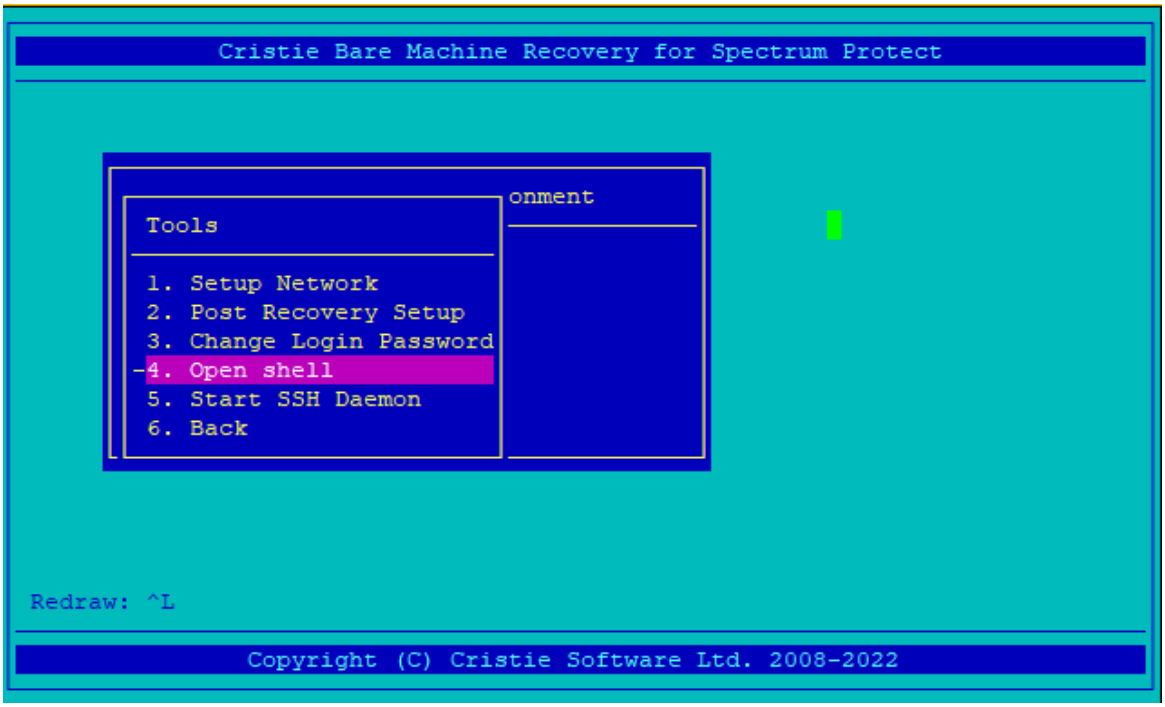
After enabling the SSH Daemon you may reset the SSH root password using this option.



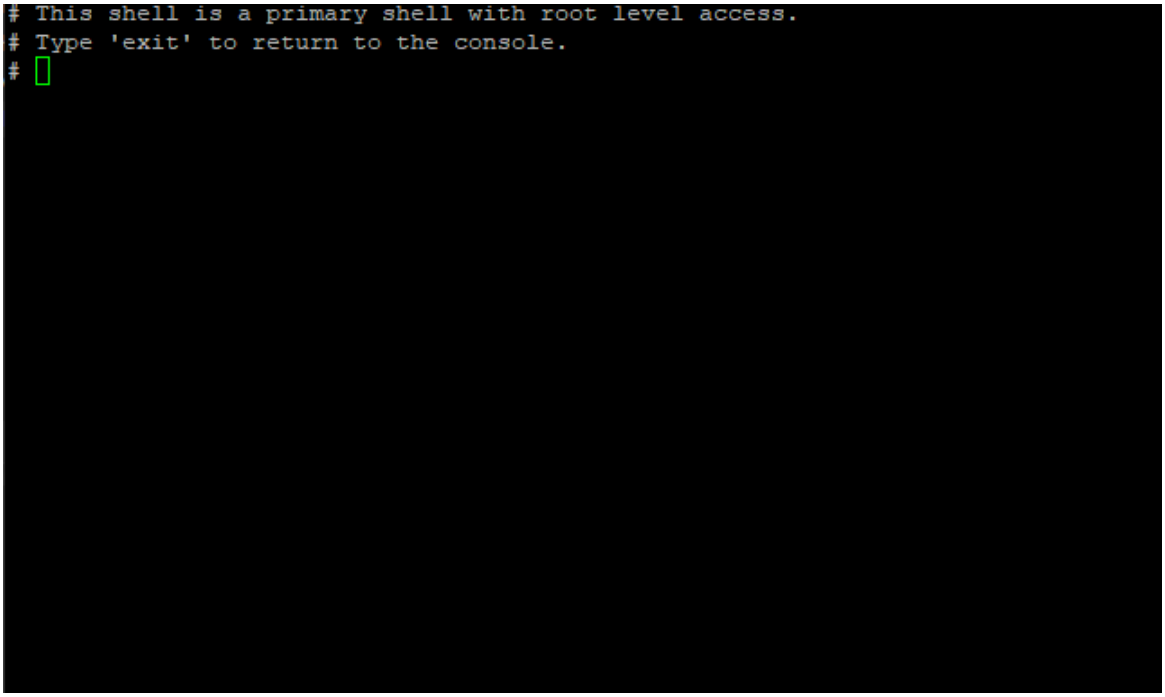
Note: By default the SSH password is the same as the value used on the original host. However once logged in to the DR environment it is possible to change this password to a new value with this option.

9.1.2.4 Open shell

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



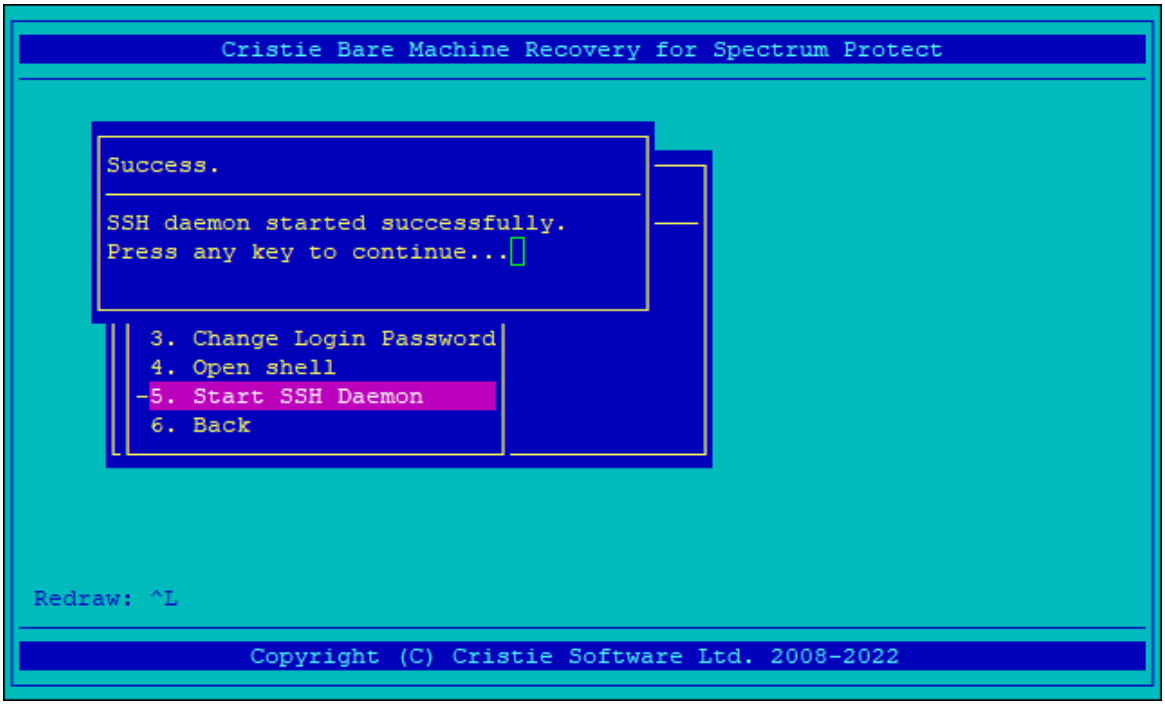
You will then see the shell window thus.



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.

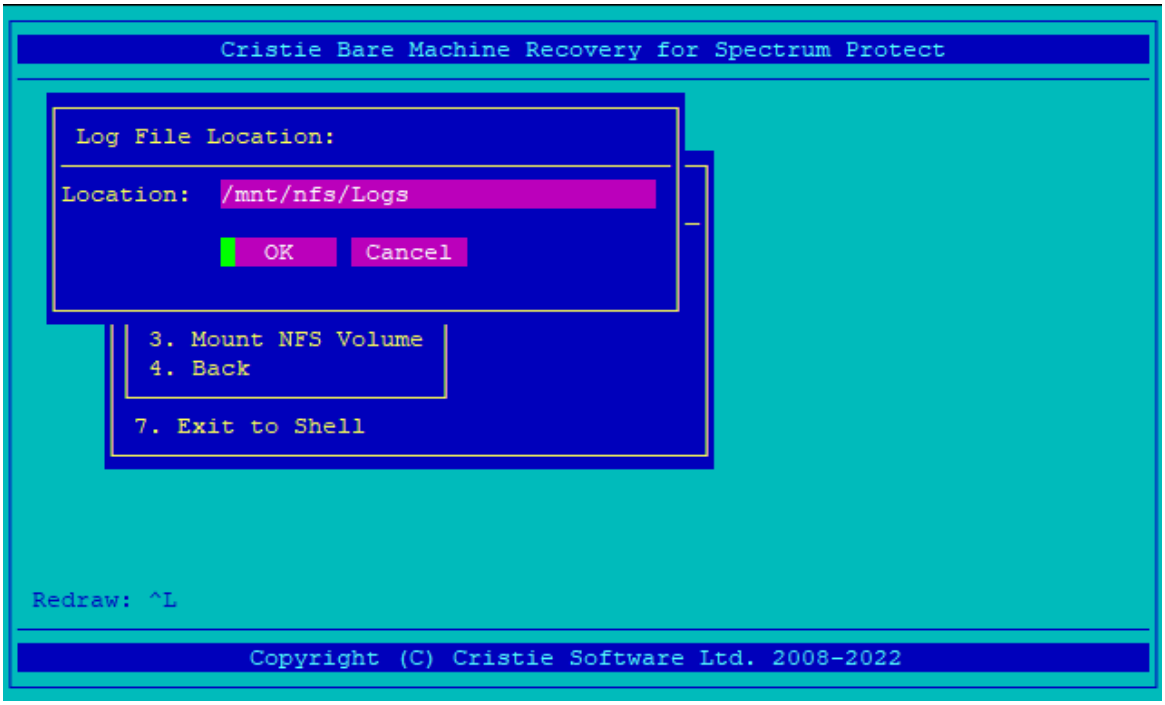


Use in conjunction with Change Login Password to set the SSH password.

9.1.3 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.



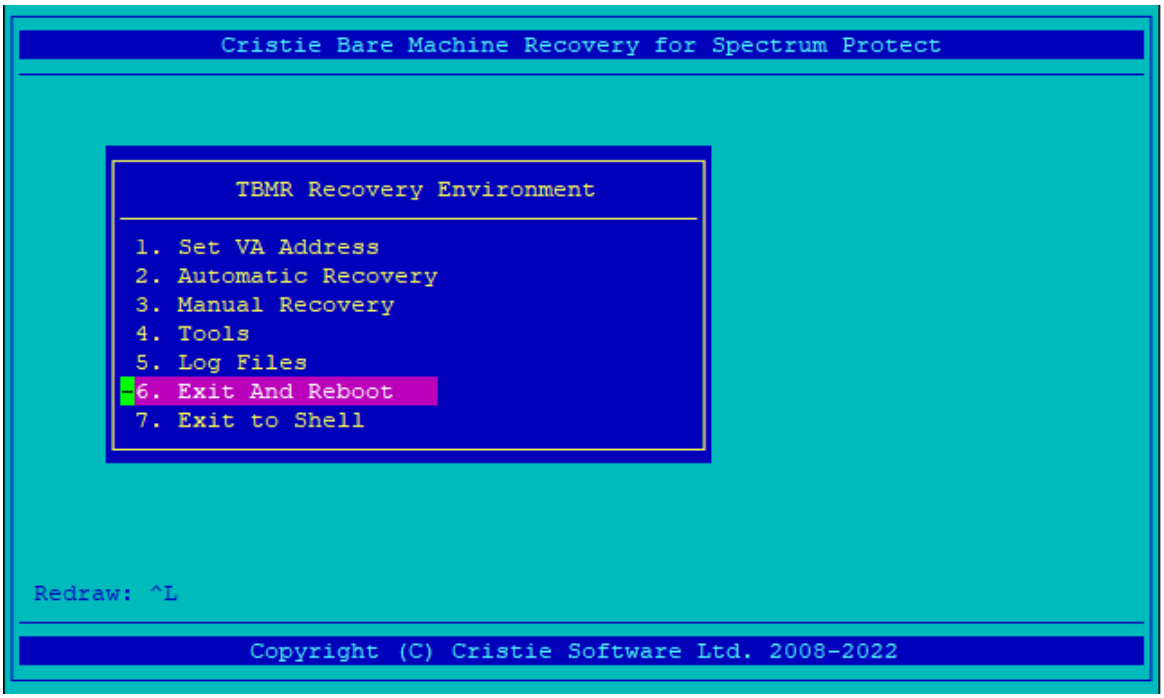
The log files are created with a filename in the form:

```
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.



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 for IBM Spectrum Protect product, please contact Cristie Technical Support. To assist us in helping with your enquiry, make sure you have the following information available for the person dealing with your call:

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

Contact Numbers - Cristie Software (UK) Limited

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

Support Hours

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

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

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

*Severity 1 issues are defined as: a production server failure, cannot perform recovery or actual loss of data occurring.
**For details on dates of UK Bank Holidays, please see www.cristie.com/support/

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