



NBMR For Solaris

Bare Machine Recovery for Dell EMC NetWorker

Quick Start Guide

Version 9.2 released December 2025

Revised 2025

Copyright © 2003-2026 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 Storage Protect is a trademark of the IBM Corporation.*
- *IBM Virtual I/O Server (VIOS) is a trademark of the IBM Corporation.*
- *NetWorker and Avamar are trademarks of the Dell EMC Corporation.*
- *vSphere, vCenter and vCloud are trademarks of VMware Inc.*
- *Hyper-V is a trademark of Microsoft Corporation.*
- *Azure is a trademark of Microsoft Corporation.*
- *Amazon Web Services (AWS) and Amazon Elastic Compute Cloud (EC2) are trademarks of Amazon.com, Inc.*
- *Cohesity DataProtect is a trademark of Cohesity Inc.*
- *Rubrik is a trademark of Rubrik Inc.*
- *CloneManager® is a registered trademark of Cristie Software Ltd.*
- *SysBack is a registered trademark of Cristie Software Ltd.*

PC-BaX, UBax, Cristie P4VM (Protect for VMs), Cristie Storage Manager (CSM), SDB, ABMR (Bare Machine Recovery for EMC Avamar), NBMR (Bare Machine Recovery for EMC NetWorker), TBMR (Bare Machine Recovery for Storage Protect/TSM), CBMR (Cristie Bare Machine Recovery), CoBMR (Bare Machine Recovery for Cohesity DataProtect), RBMR (Bare Machine Recovery for Rubrik) and CRISP (Cristie Recovery ISO Producer) are all trademarks of Cristie Software Ltd..

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

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



Contents

1	Document Conventions	4
2	About NBMR	5
3	System Requirements	6
4	Installation	7
	4.1 Checking Prerequisites	7
	4.2 Installation	7
	4.3 Upgrading	8
	4.4 Uninstall	8
	4.5 Zones	9
5	Product Licensing	10
	5.1 Trial License	10
	5.2 Full License	10
	5.2.1 Setting up a Cristie Licensing Portal account	11
	5.2.2 Manual Activation	13
6	Creating a Recovery Image	14
	6.1 Creating a Recovery CD	16
	6.2 Creating a Recovery Miniroot	16
	6.3 Adding Additional Drivers	16
	6.4 Create CD from Miniroot	17
7	Performing a DR backup	18
	7.1 Recording System Information	18
	7.2 Perform a Networker Backup	20
	7.3 Server Trust Authentication Database	20
8	Performing a Recovery	21
	8.1 Starting the Recovery Environment	21
	8.2 Automatic Recovery	23
	8.2.1 Recovery with the Auth Database	23
	8.2.2 Recovery without the Auth Database	30
	8.2.3 Start Recovery	37
	8.2.4 Log Files	38
	8.2.5 Post Recovery Steps	39
9	Troubleshooting	42
10	Cristie Technical Support	43



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 ></code>	used to signify clickable buttons on a GUI dialogue
Note:	describes something of importance related to the current topic



2 About NBMR

This quick start guide describes how to save system configuration information and backup and recover a Solaris machine using NBMR. Please note that this guide does not cover the full functionality of the product.

NBMR for Solaris provides a file-based backup and disaster recovery (DR) system for Solaris 10, 11.3, 11.4 and 11.4 SRU (Support Repository Updates) on both SPARC and Intel (64-bit only).

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

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

Step 1 is performed using the Graphical User Interface run from the command `nbmr`. Step 2 is performed using the Dell EMC NetWorker product. Please consult manufacturer's documentation on how to set up scheduled and scripted backups in this case. Step 3 is performed using the DR environment created from step 1.

Use the command `man nbmr` to get an overview of NBMR functionality and the command line tools available.

Further information and advice on using NBMR may be found in the Cristie Knowledge Base (<https://kb.cristie.com>) or the Cristie Forum (<https://forum.cristie.com>).

Note: NBMR must be installed and run by a user that has root access



3 System Requirements

NBMR for Solaris supports 10, 11.3, 11.4 and 11.4 SRU (Support Repository Updates) on both SPARC and Intel hardware.

A minimum of **4 GB RAM** is required for booting the recovery environment and running a recovery.

Please refer to the following web page for the latest information regarding supported platforms:
<https://www.cristie.com/support/matrix/>

Software Dependencies

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

Libxml2 and Mkisofs are included in the NBMR package and can be installed at the same time as NBMR. Modern Solaris distributions also include the open source packages on the installation media



4 Installation

On default installations of Solaris 10, 11.3, 11.4 and 11.4 SRU (Support Repository Updates), all of the necessary prerequisites should be available.

However, if a minimal installation was performed, then the prerequisites must be checked.

4.1 Checking Prerequisites

Verifying Required Packages

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

For example:

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

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

```
> cd nbmr-9.2.4144.sunos
> ./checkpackages.sh
```

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
```

Backup Client Prerequisites

An appropriate version of the Dell EMC NetWorker must be installed prior to the installation of NBMR.

4.2 Installation

NBMR 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 NBMR 9.2 for Solaris:

Note that there is one package file for both SPARC and Intel versions of NBMR, for example: `nbmr-9.2.4144.sunos.tar.gz` contains a `sparc` folder and an `i86` (Intel) folder (see the below screenshot). Navigate into the appropriate folder to find the packages for that architecture.

Intel

```
> pkgadd -d CSTEnbmr-9.2.4144-i86pc.pkg
for Intel machines
```

SPARC

```
> pkgadd -d CSTEnbmr-9.2.4144-sparc.pkg
in the case of SPARC hardware
```

Example output:



```

root@PJ-SOL114-D0CU:/# tar -zxf nbmr-9.2.4144.sunos.tar.gz
root@PJ-SOL114-D0CU:/# cd nbmr-9.2.4144.sunos
root@PJ-SOL114-D0CU:/nbmr-9.2.4144.sunos# ls
checkpackages.sh  i86          sparc
root@PJ-SOL114-D0CU:/nbmr-9.2.4144.sunos# ./checkpackages.sh
All required libraries and binaries check OK
root@PJ-SOL114-D0CU:/nbmr-9.2.4144.sunos# cd sparc/
root@PJ-SOL114-D0CU:/nbmr-9.2.4144.sunos/sparc# ls
CSTEnbmr-9.2.4144-sparc.pkg  SMCcdrt-2.01-sparc.pkg  SMCxml2-2.4.23-sparc.pkg
root@PJ-SOL114-D0CU:/nbmr-9.2.4144.sunos/sparc# pkgadd -d CSTEnbmr-9.2.4144-sparc.pkg

The following packages are available:
  1  CSTEnbmr      Cristie Bare Machine Recovery for Dell/EMC Networker
                        (sparc) 9.2.4144.53447

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:

Processing package instance <CSTEnbmr> from </nbmr-9.2.4144.sunos/sparc/CSTEnbmr-9.2.4144-sparc.pkg>

Cristie Bare Machine Recovery for Dell/EMC Networker(sparc) 9.2.4144.53447
Cristie Ltd.
Using </> as the package base directory.
## Processing package information.
## Processing system information.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.

The following files are being installed with setuid and/or setgid
permissions:
  /usr/sbin/mkdracd <setuid root>

Do you want to install these as setuid/setgid files [y,n,?,q] y

This package contains scripts which will be executed with super-user
permission during the process of installing this package.

Do you want to continue with the installation of <CSTEnbmr> [y,n,?] y

Installing Cristie Bare Machine Recovery for Dell/EMC Networker as <CSTEnbmr>

```

4.3 Upgrading

Please note that it is not possible to upgrade NBMR on Solaris (due to the process in which upgrades are carried out in Solaris). You must first uninstall the existing NBMR version (see the uninstall section below) and then install the 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 them after the new installation is complete.

4.4 Uninstall

The NBMR package can be uninstalled by running the following command:

```
> pkgrm CSTEnbmr
```



```
root@PJ-NBMR-DOCU:/nbmr-9.2.4146.sunos/sparc# pkgrm CSTEnbmr

The following package is currently installed:
  CSTEnbmr  Cristie Bare Machine Recovery for Dell/EMC Networker
            (sparc) 9.2.4146.53451

Do you want to remove this package? [y,n,?,q] y

## Removing installed package instance <CSTEnbmr>

This package contains scripts which will be executed with super-user
permission during the process of removing this package.

Do you want to continue with the removal of this package [y,n,?,q] y
## Verifying package <CSTEnbmr> dependencies in global zone
## Processing package information.
## Executing preremove script.
```

4.5 Zones

As Solaris **Zones** are not bootable from installation media, NBMR 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, NBMR may be used for a trial period of 30 days. During that period, NBMR is fully functional. If the software is subsequently uninstalled and later reinstalled 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 Trial Version of the software can be obtained by completing a form on the Cristie website: <https://www.cristie.com/request-a-trial/>

A 30-day trial license commences from the date of installation. The NBMR configuration file generator (**nbmrcfg**) 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 nbmr
```

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

```
root@PJ-NBMR-DOCU:/nbmr-9.2.4146.sunos/sparc# licmgr -p nbmr
=====
Cristie License Manager Version
                        9.2
Copyright (C) 2012-2026 Cristie Software Limited
=====
Machine attributes : {virtual, server}
Contract ID : 0
Signature : GLZBAX2R-V7FSKU8M-EBPJJSAS-VZ7MXLTZ
Product : Bare Machine Recovery for NetWorker (NBMR)
Version : 9.2
Trial ends on : 2026-02-26

Status : Trial licence
```

The NBMR 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 have been entered via the Cristie License Manager.

5.2 Full License

A Full license entitles the holder 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.

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

Contract ID: A 4-digit number supplied by Cristie Software Ltd.

Agreement Number: Currently the same as the *Contract ID*.

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.

Existing Customers:

The software can be downloaded after logging into the Cristie licensing portal: <https://portal.cristie.com/login/>

Note that the above assumes that NBMR is already installed

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, open a web browser and navigate to the Cristie Licensing Portal web page at <https://portal.cristie.com/login>.
2. Select **Register** to create a new account:





Email

Password
[Login](#)
[Reset Password](#)
[Register](#)

3. Enter your new account details - as an example:



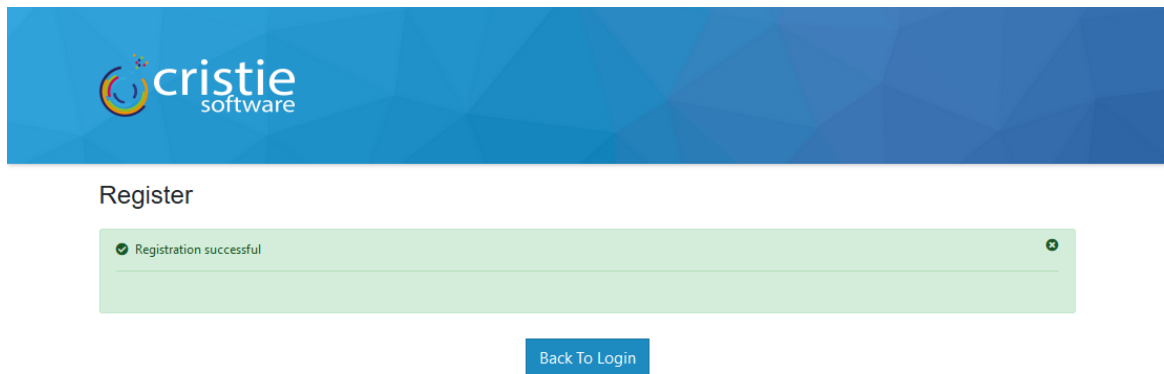
Register

Username	Cristie User
Email	test@cristie.com
New Password	*****
Confirm New Password	*****
Password Reset Question	Mother's maiden name
Password Reset Answer	*****
Contract/Agreement No	4
Contract Password	*****

[Register](#) [Cancel](#)

4. Then click **Create**. If successful, the following is shown:





At this stage, you may now log in to the Cristie Licensing Portal with the E-mail ID and password you specified in step 2.

5.2.2 Manual Activation

To activate a copy of Cristie Licensing Portal, see the following steps. The following assumes your contract is already setup on the Cristie Licensing Portal.

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

```
# licmgr -p nbmr --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 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 nbmr` output.

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
                              9.6
                  Copyright (C) 2012-2024 Cristie Software Limited
=====
Successfully applied the activation code.
  Machine attributes : {virtual, server}
    Contract ID : 1
      Signature : 7W2S29A2-ZBQU3MGE-6VZLRBSM-U46D6PPD
      Product : Cristie Bare Machine Recovery (CBMR)
      Version : 9.6
  Maintenance ends on : 2024-12-31

  Activation code : 9CP4QFRD-LPERNCZE-PE3LRDMD-7DGSU2WL
  Activation type : Product activation
  Maintenance ends on : 2024-12-31
    Attributes : {physical, server}

      Status : Full licence
```



6 Creating a Recovery Image

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

Please note that depending on the terminal and whether you are connected to the machine via telnet or ssh, the interface may look different, however the functionality will remain the same.

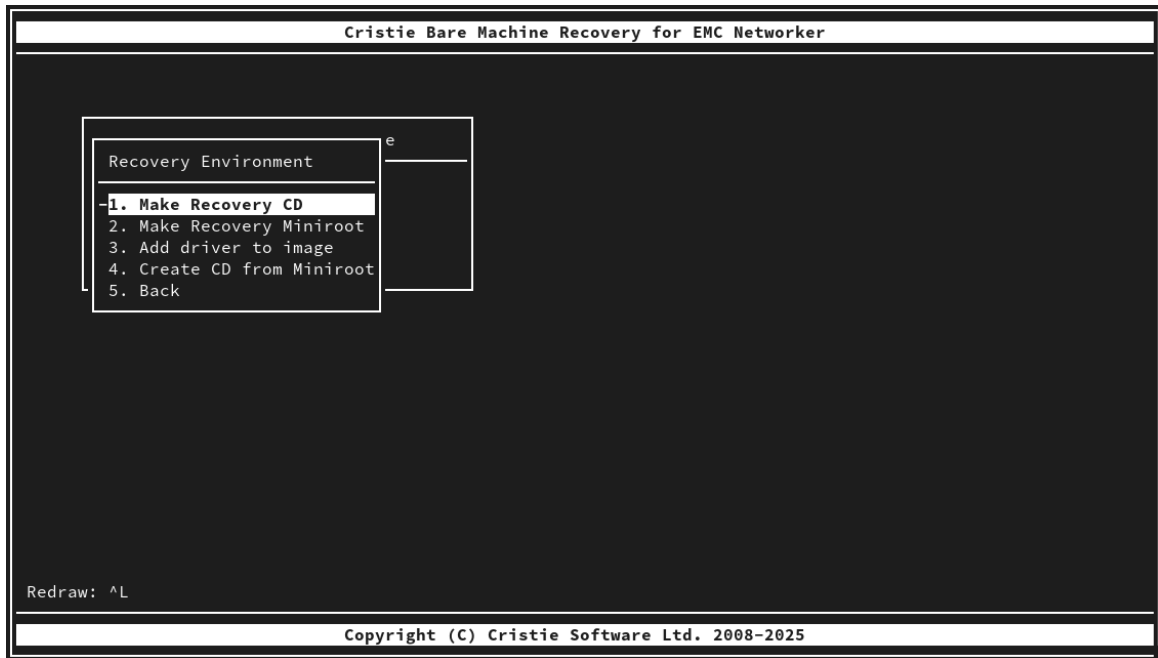


Then select **Make Recovery CD**

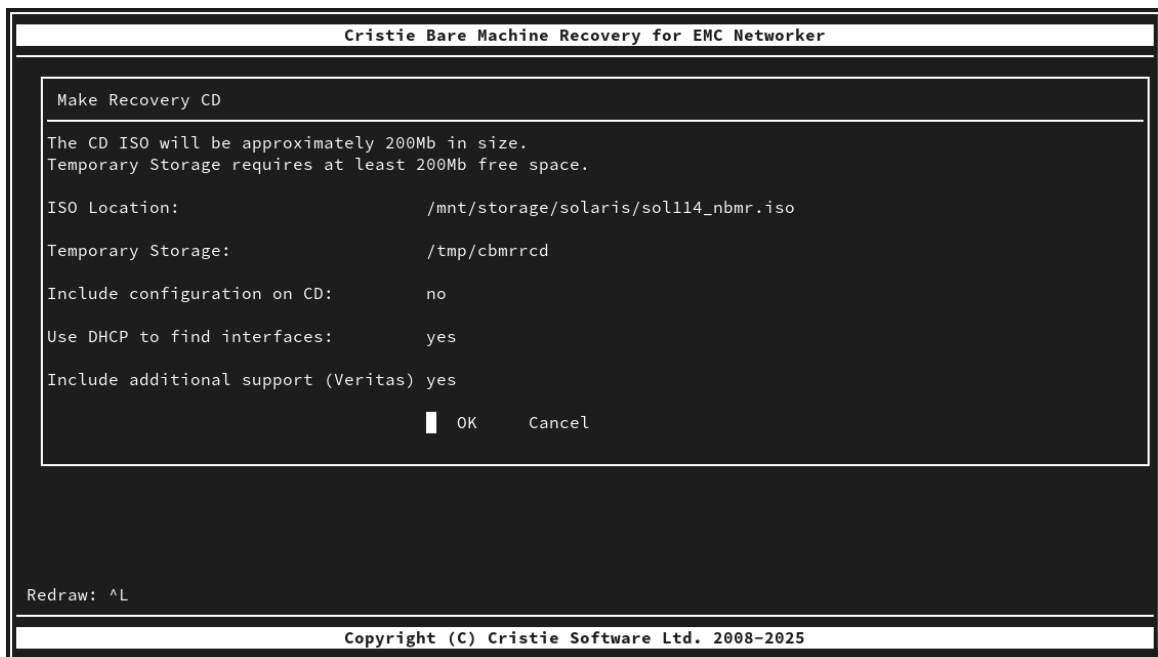
This menu presents various options for creating the recovery environment:

- **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 a driver that is not bundled with the recovery CD to support other hardware
- **Create CD from Miniroot** - create a bootable ISO from a miniroot file





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.



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



6.1 Creating a Recovery CD

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/cbmr/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.



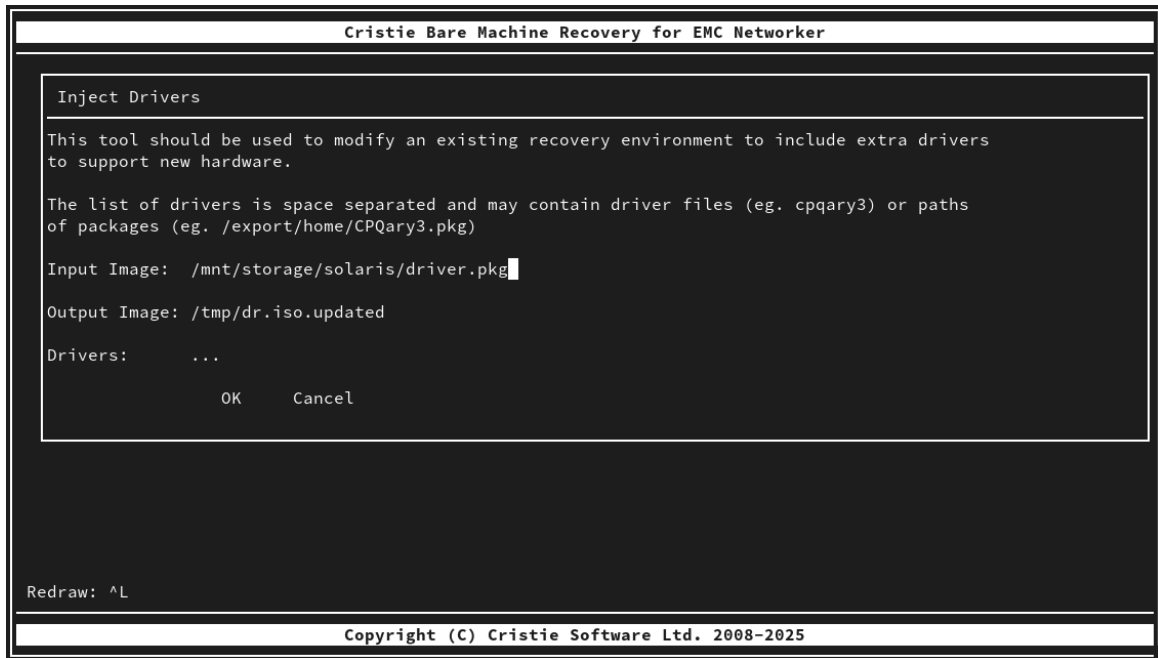
The miniroot dialogue presents the same options as the CD dialogue.

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 being restored to includes different hardware - such as storage controllers or network cards - that were not present on the original machine, then additional drivers must be installed.



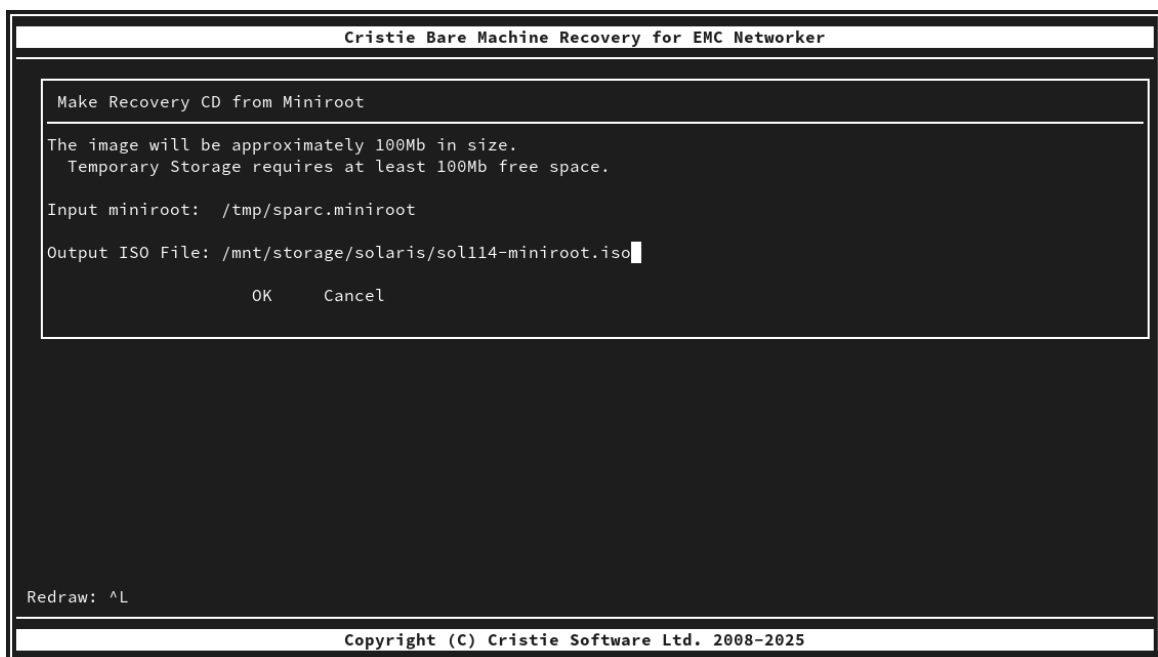


The drivers can be injected either from the running system (eg. 'cpqary3') or may be a path to a package file (eg. '/export/home/CPQary3.pkg'). It is recommended that the latter form is used wherever possible, as packages may install additional files or modify system files that cannot be picked up by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

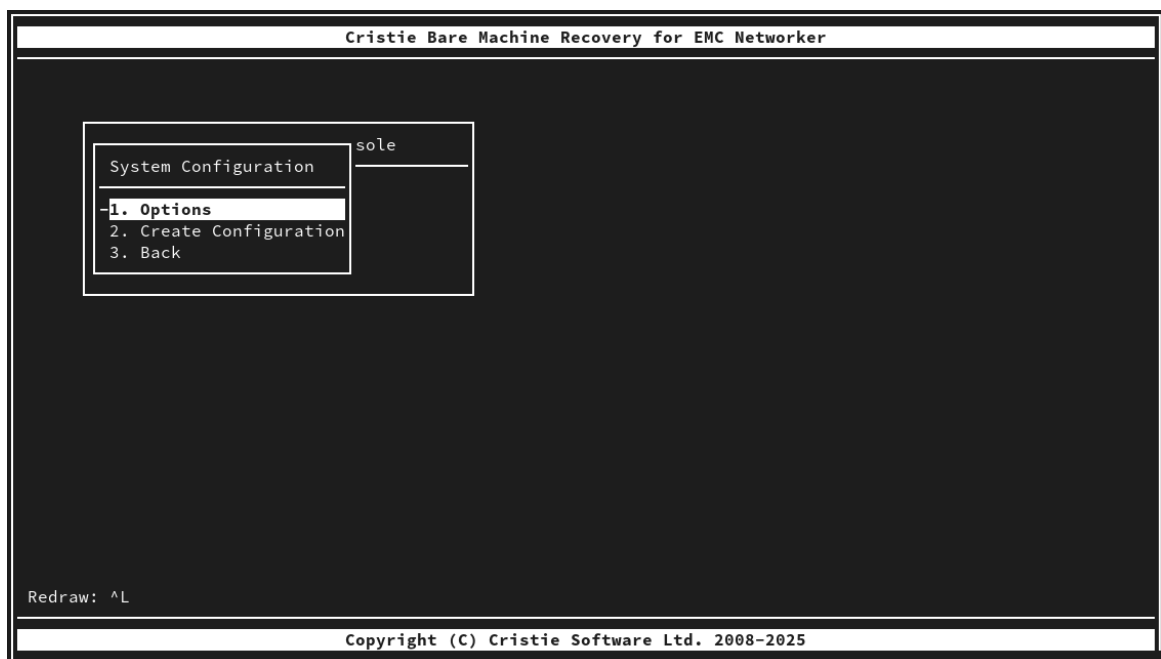
The system information is recorded to allow the recovery environment to recreate the original system environment. This will include the network configuration, the disk volume/s and filesystem configuration, as well as information about essential packages for rebuilding the system.

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 `nbmr cfg` tool, available through the **System Configuration** option of the nbmr **Backup Console**.

Please note that the config should be keep up to date, and ideally run immediately before a backup to capture the latest layout of the system.

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 `/NBMRCFG/disrec.xml`. However, the **Set Location** option will allow you to select a different location if desired.

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.



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/cbmr/nbmrcfg.log`. This may also be viewed using the [Log Files](#) submenu.



7.2 Perform a NetWorker Backup

Once the configuration is generated and saved you can now run a normal Dell EMC NetWorker backup.

To create a back up to your Dell EMC NetWorker server the following mounted partitions must be backed up as a minimum: /, /usr, /home, /var /opt, /dev

A typical backup can be performed from the host with the save or savefs command e.g.

```
savefs -v -s <NETWORKER_SERVER> <mounted partition>
```

However, Cristie Software Ltd. recommends running the backup from the Dell EMC NetWorker server.

Ensure you do not exclude any system directories such as /dev.

7.3 Server Trust Authentication Database

Required from NetWorker 19.4 onwards, a database file must be created on the client machine to allow for authentication with the NetWorker server from the recovery machine.

The following needs to be run AFTER the backup:

- Run 'nbmr_save_authdb' and specify an output directory e.g. /NBMRCFG:

```
nbmr_save_authdb /NBMRCFG
```

```
root@PJ-NBMR-DOCU:/nbmr-9.2.4146.sunos/sparc# nbmr_save_authdb /NBMRCFG
Saving NBMR authentication data to /NBMRCFG/nsrldb-PJ-NBMR-DOCU.tgz
```

- Copy the file to a network share or somewhere accessible from the recovery machine for use later

Note: It is important to note that the NetWorker Authentication database should be saved after the first backup. Doing it immediately after installing the NBMR will not produce a useable authentication database file.



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 filesystems on the volumes created in steps 5, 6 and 7
9. **Mounting** - mount the filesystems
10. **Recovery** - recover files from the backup
11. **Post-Recovery** - 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.

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

It is important that the hostname and IP address is set to the values of the original client or a client which has remote access to the original client. Otherwise the recovery will not work.



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:

For SSH access, go to Tools > Change Login Password, set a password then back in the tools menu go to Start SSH Daemon. You can then login as root with the password you set. To start the recovery environment, type `dr`

If you wish to monitor the recovery operation in the Cristie Appliance 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

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 server holding the backup
3. **Import Server Authentication Database** - establish a secure connection with the server for recovery
4. **Configuration** - read machine configuration information and set applicable options
5. **Perform Recovery** - start the recovery procedure
6. **Copy Log Files** - copy the log files generated by the recovery

Depending on whether the recovery will utilise Server Trust Authentication (Networker 19.2 onwards), follow the appropriate section below - with the database or without.

8.2.1 Recovery with the Auth Database

It is recommended that the source (backup) machine is shutdown to avoid IP conflicts with the recovery machine, due to the nature in which the recovery machine is setup for recovery.

Setup Network

The recovery machine has to be set to use the source machine's hostname and IP address so that the Networker server recognises it.

The manual configuration step is exactly the same as the initial network setup in section [Starting the Recovery Environment](#).

- Once in the recovery menu, go to Automatic Recovery > Setup Network > Manually
- Enter in the hostname and IP Address of the source machine and the other networking sections as appropriate for your network.



Cristie Bare Machine Recovery for Dell/EMC NetWorker

Network Configuration

Hostname	SOL-NBMR	Interface	net0
IP Address	10.10.10.1	Subnet	255.0.0.0
Default Gateway	10.10.10.10	DNS	10.10.10.2
Domain			

OK
Cancel

Redraw: ^L

Copyright (C) Cristie Software Ltd. 2008-2025

Hosts File Configuration

Add the hostname and IP address of the source machine to the recovery environment's host file so that NetWorker can find it:

- Go to Tools (main menu) > Open Shell
- Edit /etc/hosts with vi and add an entry for the source machine and the NetWorker Server
- Verify that the hosts file has been updated with the entries:

```
cat /etc/hosts
```

```
bash-4.4# cat /etc/hosts
10.10.10.12 NETWORKER-SERVER
10.10.10.1 SOL-NBMR
```

AuthDB Import

Import the authentication database to the recovery machine via network share or scp.

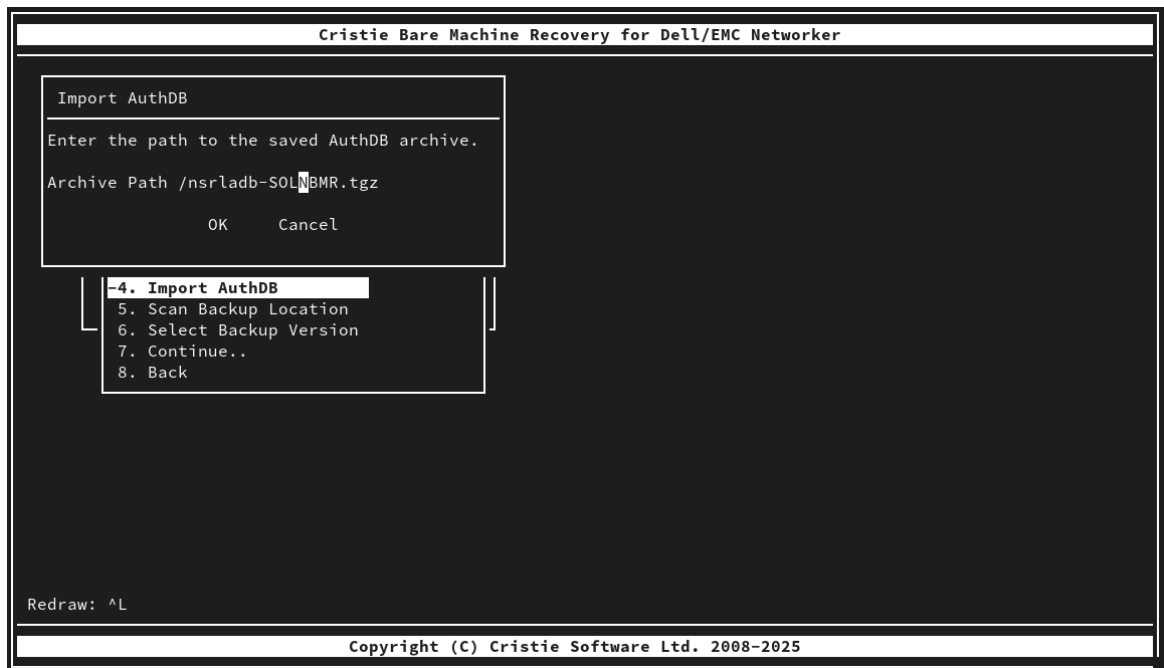
Network Share Method:

Use the 'Mount NFS Volume' tool in Automatic Recovery > Backup Location > Mount NFS Volume to configure a network share if required, then enter the full path from the share in the Archive Path field.

SCP method:

- Go to Tools > Change login password and enter a password for SSH
- Go to Tools > Start sshd daemon
- scp the authdb file from earlier to the machine
- Go to Automatic Recovery > Continue > Import AuthDB then enter the path to the file

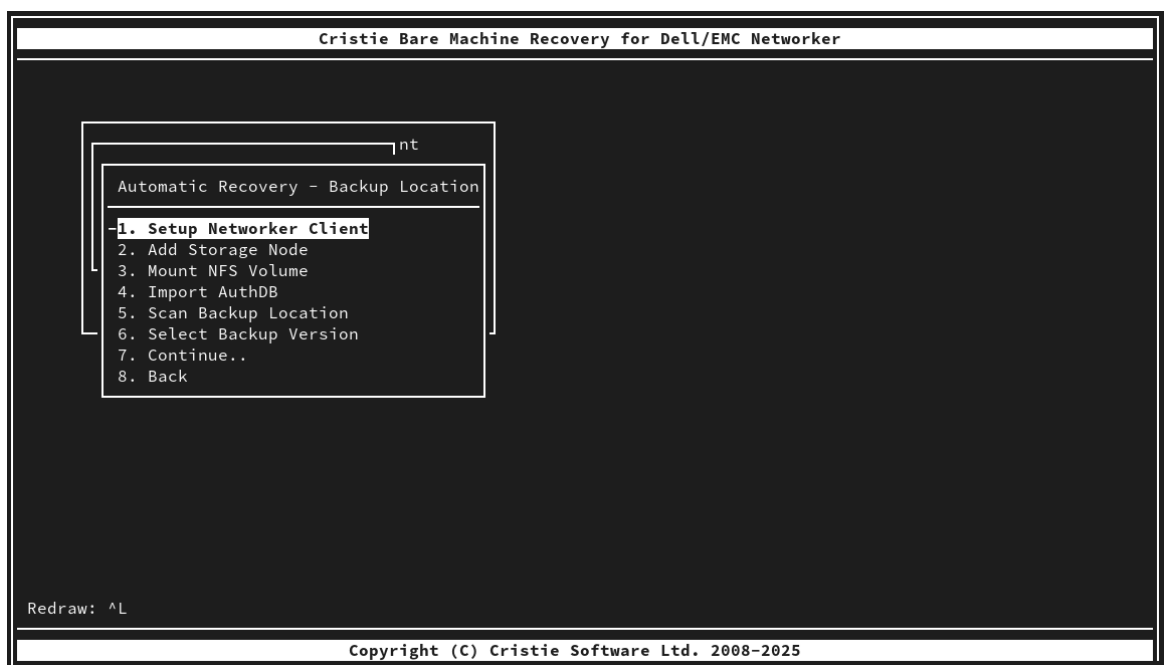




IMPORTANT: Do not add a passphrase to the passphrase section when using an AuthDB as the configuration restore step will fail. NBMR will prompt for a password during recovery - this is the appropriate time to enter it.

Backup Location

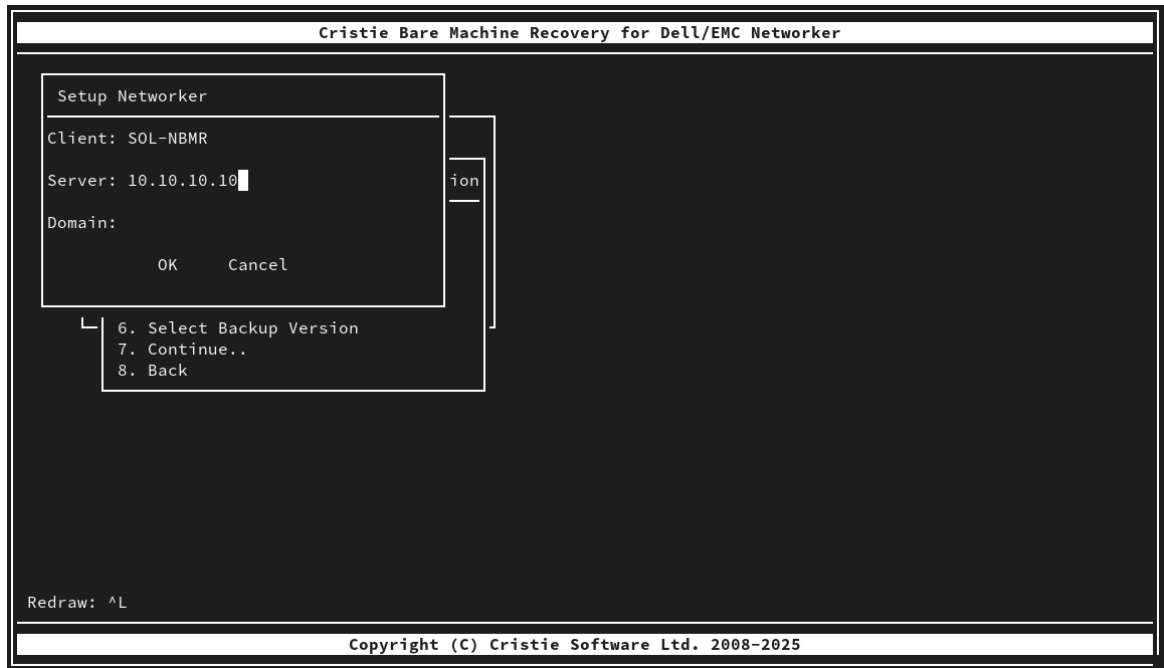
The Backup Location menu allows the user to setup the NetWorker client for access to the server.



It is vitally important that the hostname and IP address of the client match that machine that backed up.

Note: if the server is specified by name, then a DNS server must have been chosen when setting up the network





It is also possible to select the version to be restored:



Instead of a particular version, the backup may be recovered from a particular point in time. To toggle between point-in-time and latest, use the up/down arrow keys.

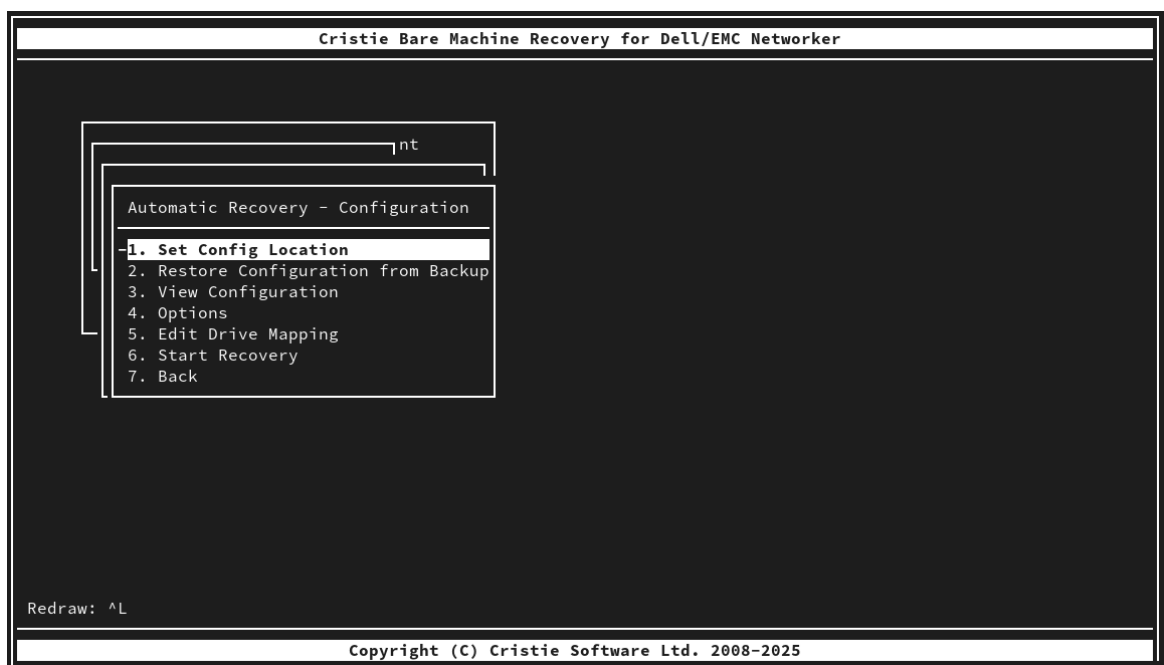




Once the backup has been successfully setup, you can move to the next stage to setup the configuration.

Configuration

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



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.

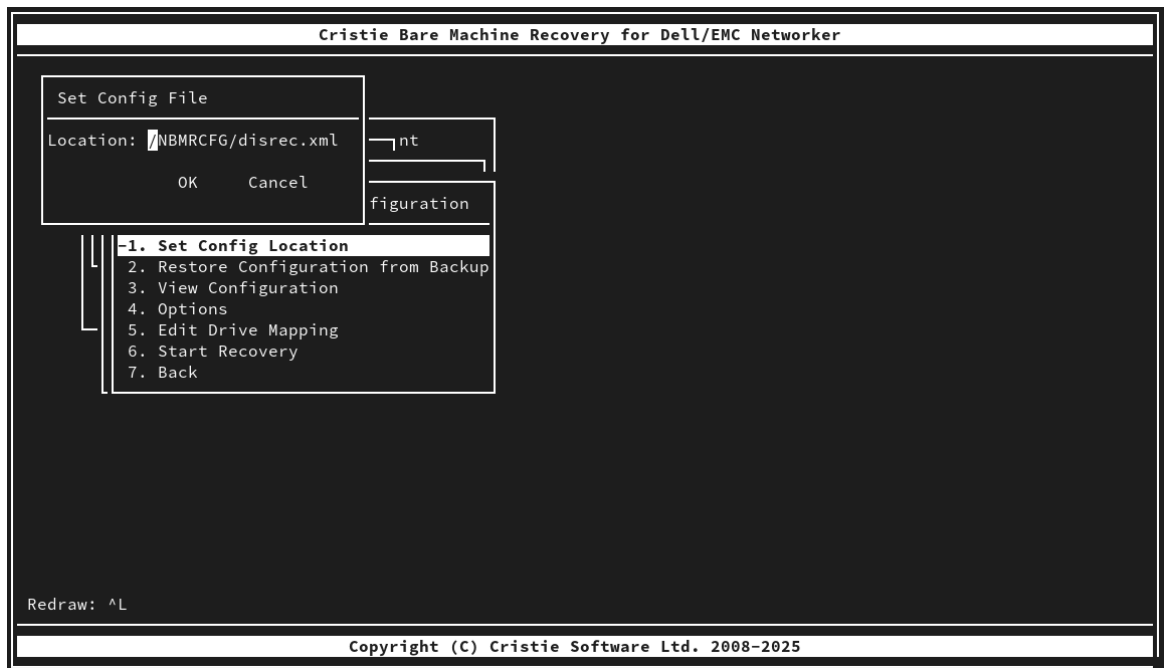
Note: this can also be achieved by setting all but the root drives to 'Unmapped' in the drive mapping

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



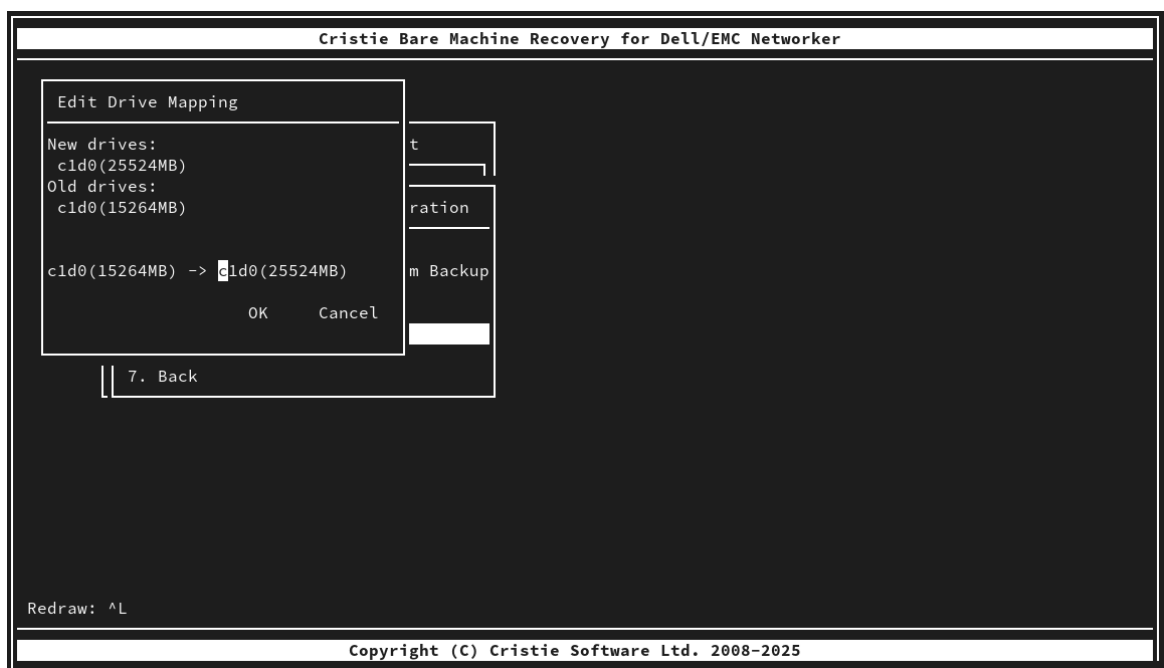


Drive Mapping

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.

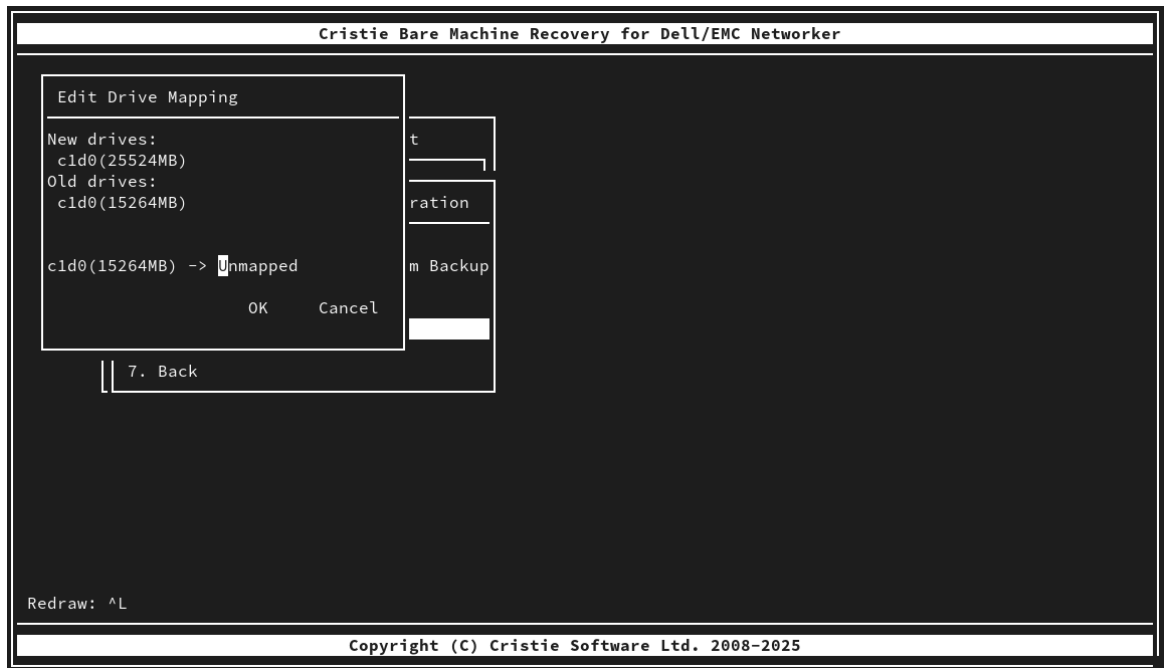
Selecting the **Drive Mapping** option will display a form matching drives in the configuration to drives on the system.



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**' (use the down-arrow or up-arrow key to change the setting):



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 Recovery without the Auth Database

Pre-recovery NetWorker Configuration

- Make a note of the DR environment's hostname and IP (network information can be found in: Automatic Recovery > Setup Network > Manually):

The screenshot shows a terminal window titled "Cristie Bare Machine Recovery for Dell/EMC Networker". Inside, there is a "Network Configuration" dialog box. The dialog box contains the following fields and values:

Network Configuration			
Hostname	SOL-NBMR	Interface	net0
IP Address	10.10.10.1	Subnet	255.0.0.0
Default Gateway	10.10.10.10	DNS	10.10.10.2
Domain			
OK		Cancel	

Below the dialog box, there is a "Redraw: ^L" prompt. At the bottom of the terminal window, there is a copyright notice: "Copyright (C) Cristie Software Ltd. 2008-2025".

- Add the IP address and hostname to the Networker server's hosts file
- Also add them to the client alias list of the backup machine in Modify client settings > (Globals 1 of 2) in Networker

Hosts File Configuration

Add the hostname and IP address of the source machine to the recovery environment's host file so that Networker can find it:

- Go to Tools (main menu) > Open Shell
- Edit /etc/hosts with vi (or type bash to change the shell to bash and use nano) and add an entry for the source machine and the Networker Server
- Verify that the hosts file has been updated with the entries:

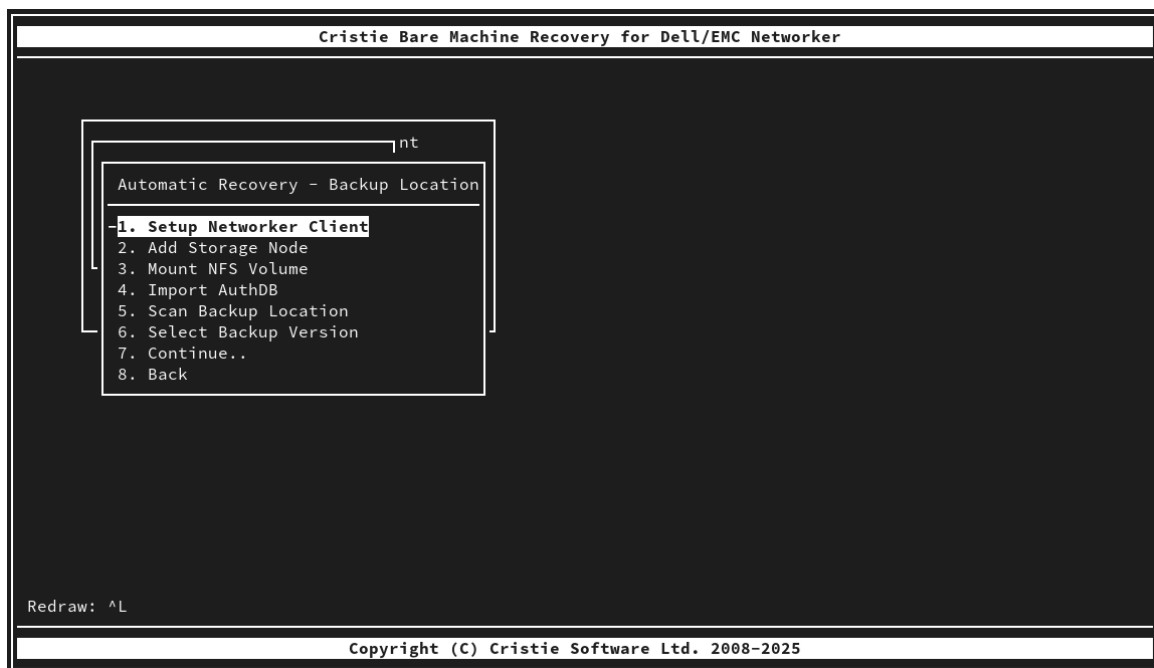
```
cat /etc/hosts
```

```
bash-4.4# cat /etc/hosts
10.10.10.12 NETWORKER-SERVER
10.10.10.1 SOL-NBMR
```

Backup Location

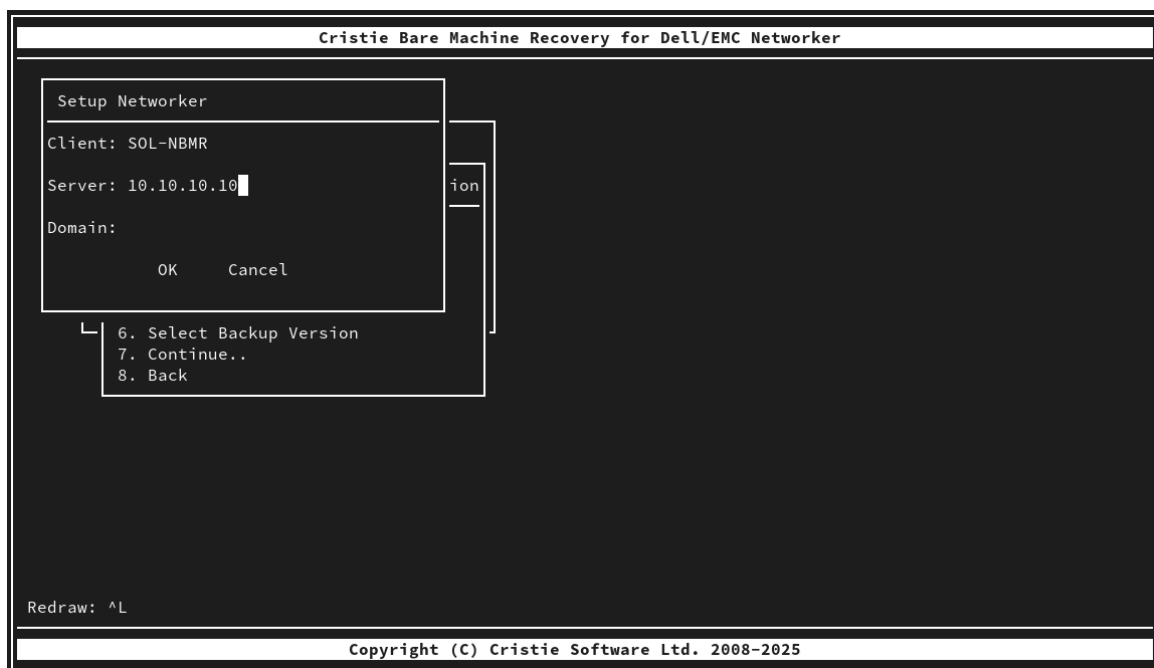
The Backup Location menu allows the user to setup the NetWorker client for access to the server.





It is vitally important that the hostname and IP address of the client match that machine that backed up.

Note: if the server is specified by name, then a DNS server must have been chosen when setting up the network



It is also possible to select the version to be restored:





Instead of a particular version, the backup may be recovered from a particular point in time. To toggle between point-in-time and latest, use the up/down arrow keys.



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

Configuration

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

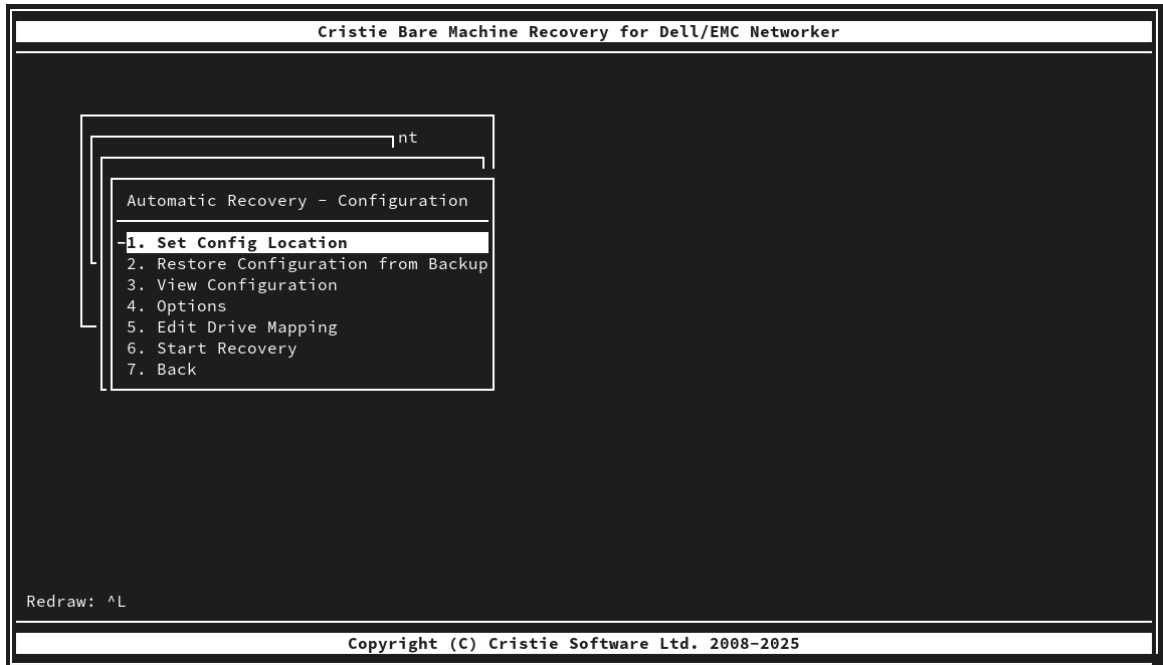
Note: if the location was saved with the recovery CD, as outlined in [Creating a Recovery](#)



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



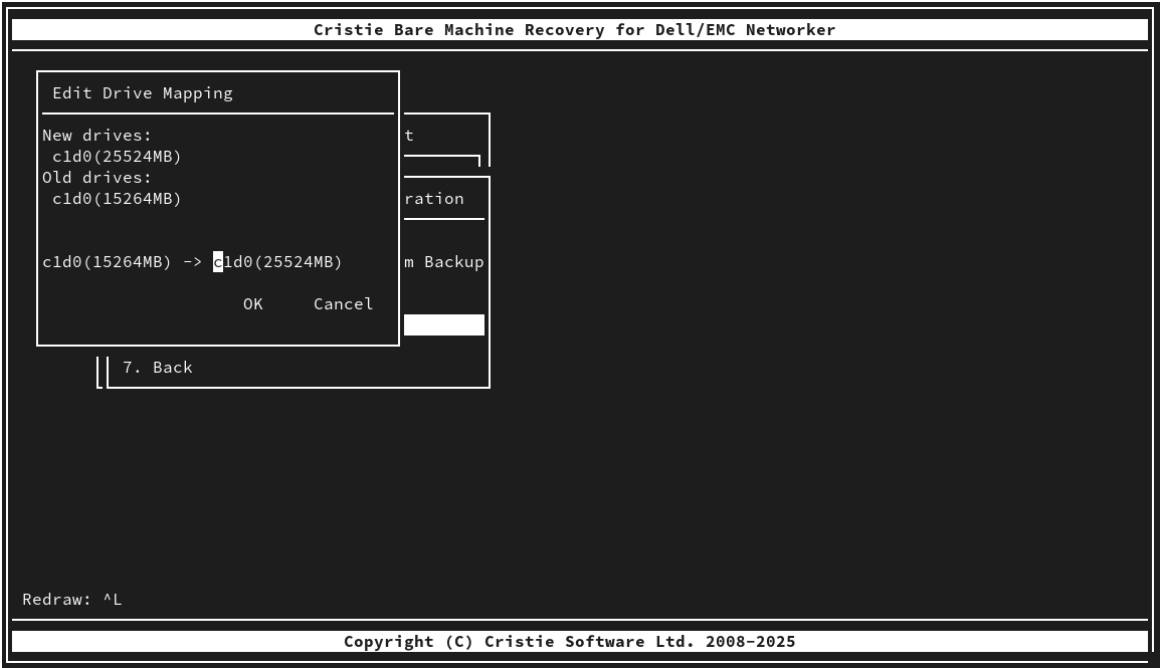


Drive Mapping

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.

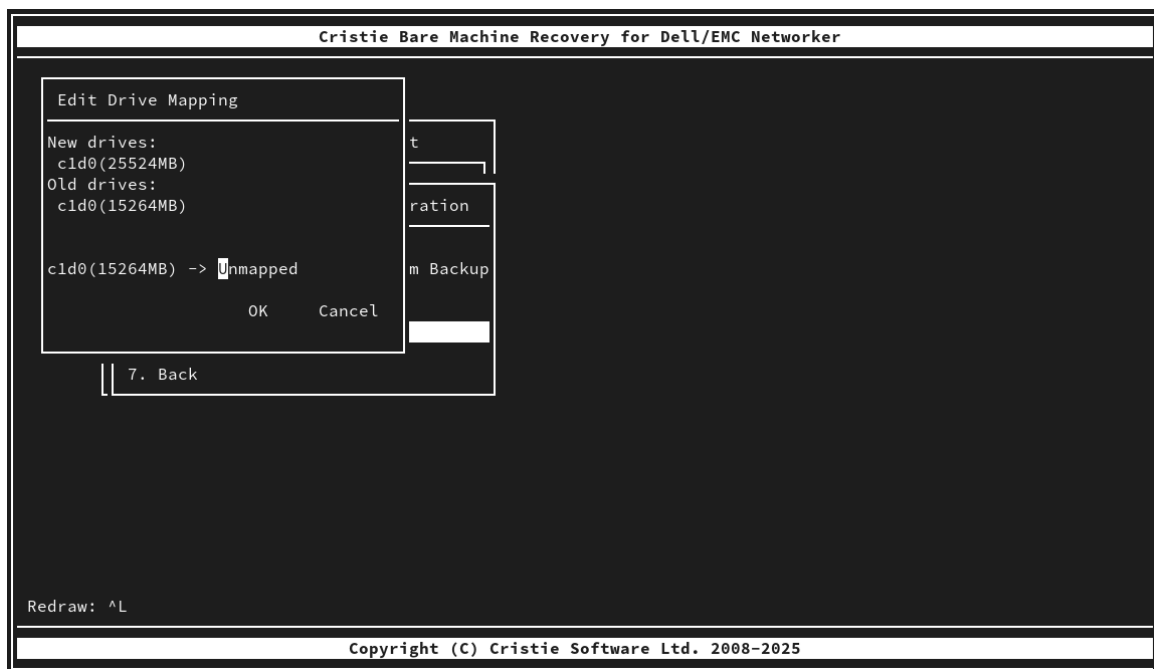
Selecting the **Drive Mapping** option will display a form matching drives in the configuration to drives on the system.



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**' (use the down-arrow or up-arrow key to change the setting):



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.



8.2.3 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

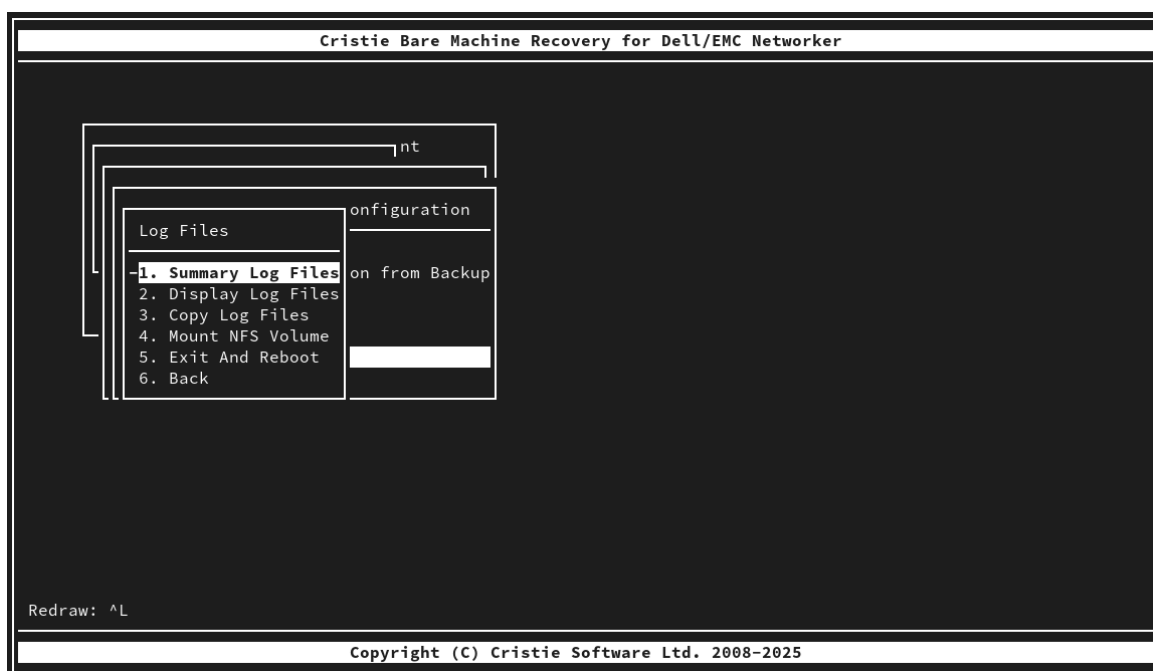
Once the recovery is complete, you will be presented with a dialogue indicating that the machine can be rebooted.





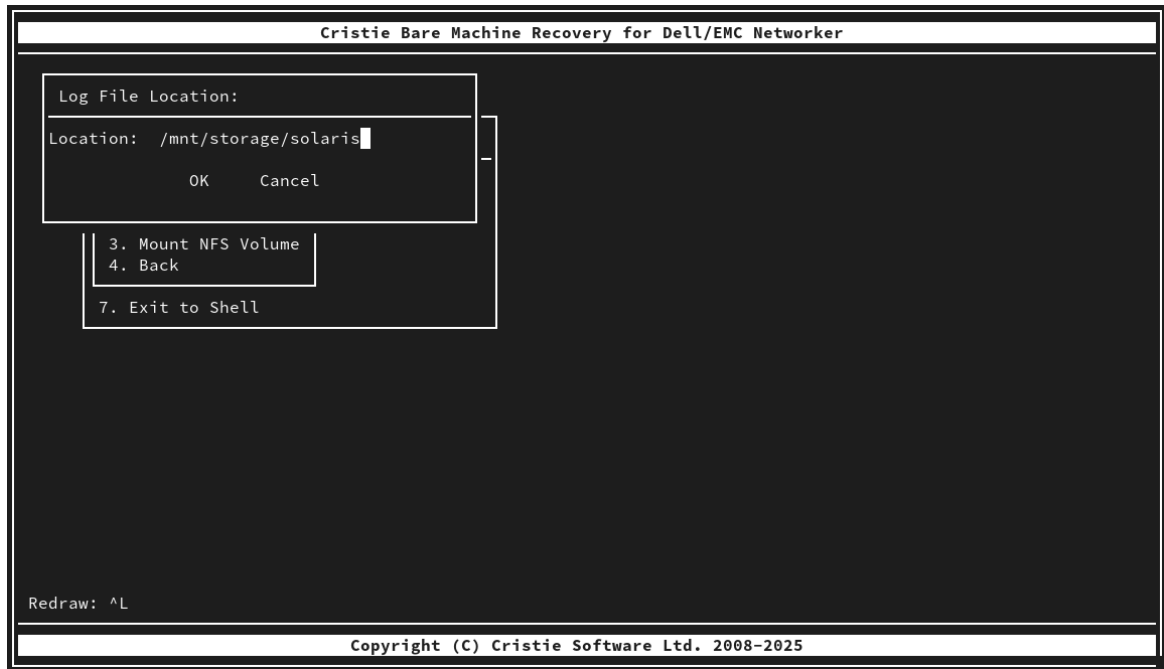
8.2.4 Log Files

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-1124-16122025.tar.gz
```

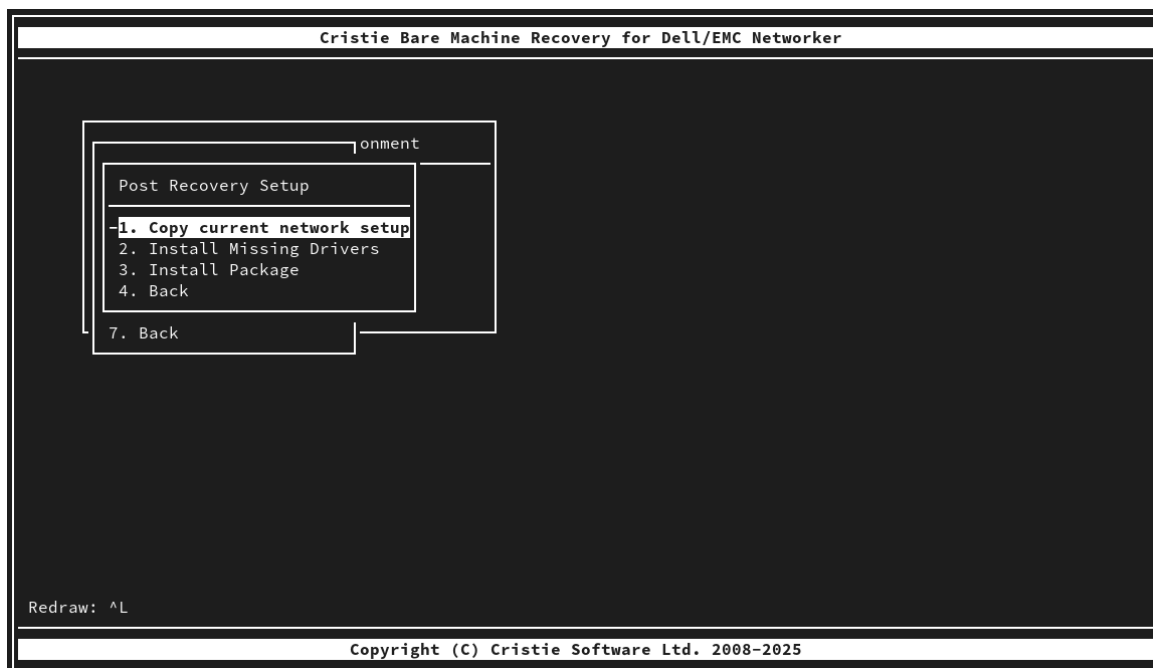
The first part '1124' being the time (11:24), and the second part '16122025' being the date (16/12/2025).

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

8.2.5 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. Select **Tools** from the main menu to display these options.





Copy current network setup

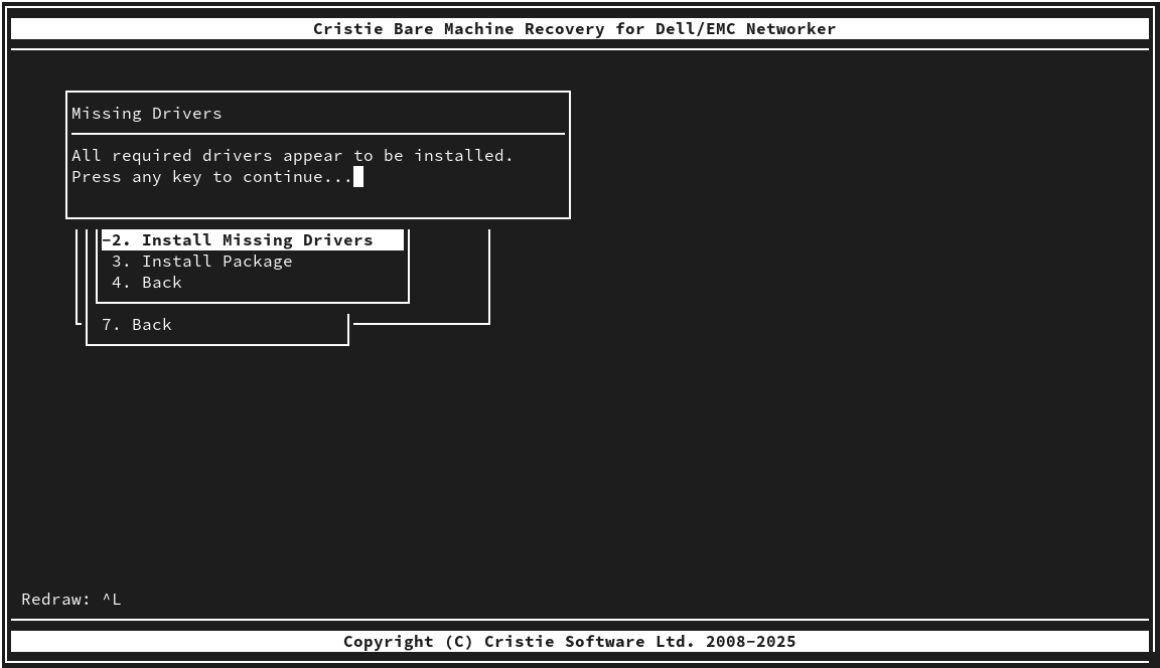
The network settings used by the recovery environment can be copied to the recovered system so that it uses those settings on boot up. If DHCP was used to obtain an IP address, then the recovered system will use DHCP on boot up.



Install Missing Drivers

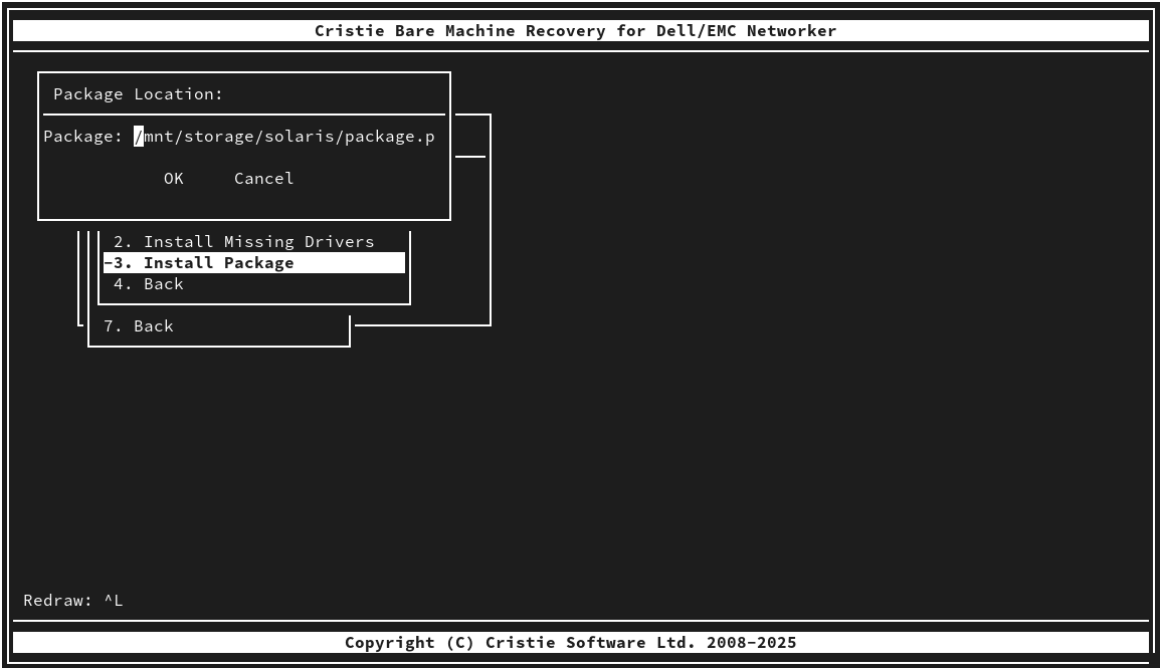
This option examines the current setup to determine which drivers were used to access the disks and the network adapters. It then examines the recovered system to determine whether these drivers were installed. Once complete, it will present a list of drivers that can be pushed from the recovery CD to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



9 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.



10 Cristie Technical Support

If you have any queries or problems concerning your Bare Machine Recovery for Dell EMC NetWorker 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:

- NBMR 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.

