Symantec NetBackup™ Bare Metal Restore™ Administrator's Guide

UNIX, Windows, Linux

Release 7.5

Symantec

Symantec NetBackup™ Bare Metal Restore™ Administrator's Guide

Documentation version: 7.5

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

Introducing Bare Metal Restore

This chapter includes the following topics:

About Bare Metal Restore

NetBackup Bare Metal Restore (BMR) is the server recovery option of NetBackup. BMR automates and streamlines the server recovery process, making it unnecessary to reinstall operating systems or configure hardware manually. You can restore servers in a fraction of the time without extensive training or tedious administration.

BMR restores the operating system, the system configuration, and all the system files and the data files with the following steps:

- Run one command from the NetBackup master server.
- Reboot the client.
  Separate system backups or reinstallations are not required.

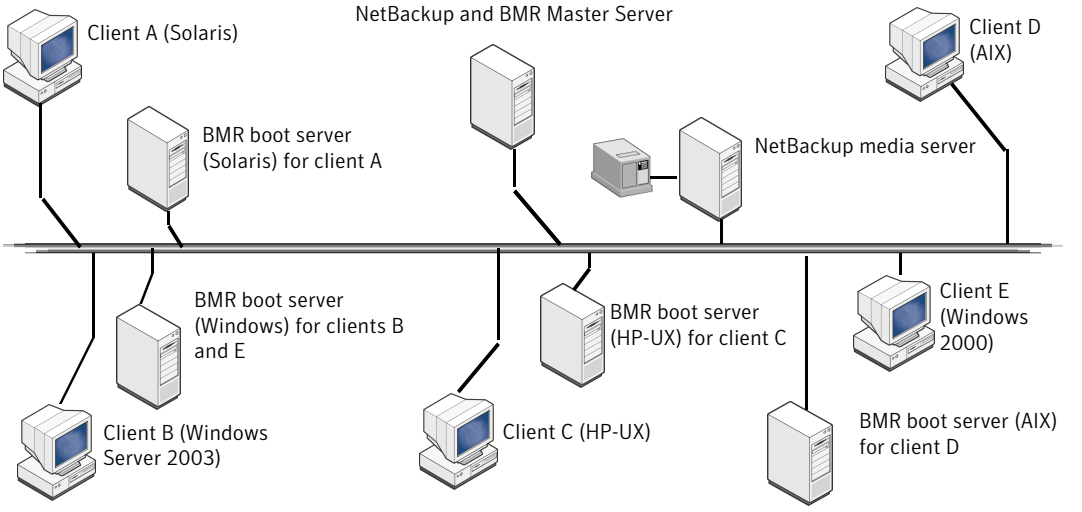
Table 1-1 shows the components of a BMR protection domain.

Table 1-1 BMR components

Component	Description
NetBackup and BMR master server	The NetBackup master server manages backups and restores of the protected client systems. A NetBackup master server also hosts the BMR master server then manages BMR operations.
NetBackup media servers	NetBackup media servers control storage devices on which the client files are stored.
BMR boot servers	Boot servers provide the environment that is required to rebuild a protected client, including resources such as shared resource trees (SRTs). Shared resource trees contain the software that is used to rebuild the protected system so that NetBackup can restore the original files. The software includes the operating system software and the NetBackup client software.
Clients	Clients are the systems backed up by NetBackup and protected by BMR. A client may also be a server for other applications or data, a NetBackup media server, or a BMR boot server.

Depending on your environment, the server components can be located on the same computer, on separate computers, or on a combination of computers.

Figure 1-1 Example of BMR protection domain



New features in NetBackup 7.5 Bare Metal Restore

This section provides brief descriptions of the Bare Metal Restore 7.5 features.

Table 1-2 New features in NetBackup 7.5 Bare Metal Restore

Feature	Description
Support for RHEL 6 and AIX 7.1	BMR can now restore RHEL 6 and AIX 7.1 clients. BMR 7.5 also supports boot servers with RHEL 6 and AIX 7.1 platforms.
Support for Solaris 10 ZFS (Sparc / x64)	In BMR 7.5, support for ZFS (Zettabyte File System) storage pools. With this added support, BMR can now restore clients that are attached to ZFS storage pools with the following configuration: ■ Solaris 10 Update 8 or later ■ Solaris Sparc or x64 architecture See "About ZFS storage pool support" on page 170.
Support for Linux native multi-path	Support for Linux native multipath is added in case of BMR client See "About the support for Linux native multipath in BMR" on page 15.
Auto Image Replication support (AIR) for BMR images	In NetBackup 7.5, support for AIR is added for BMR images. For more details on Auto Image Replication (AIR), refer to *Symantec NetBackup™ Administrator's Guide, Volume I.*

About the support for Linux native multipath in BMR

In the data storage domain, multipathing is the ability of a server to communicate with its mass storage devices using more than one physical path; through the buses, controllers, switches, and bridge devices connecting them.

Multipathing protects against the failure of paths but not from the failure of a specific storage device. Another advantage of using multipath connectivity is the increased throughput by way of load balancing.

Until now, BMR supported EMC Powerpath solution. But the demand for native multipath is increasing, which is a platform-independent technique. To cater to

this demand, support for native multipath is added in BMR 7.5 for the Linux platform.

Once the System Administrator has configured the Linux native multipath on the client systems, no additional installation, un-installation, or configuration steps are required from the BMR side to enable this feature. The native multipathing ability is already integrated with BMR 7.5.

Chapter 2

Installing BMR

This chapter includes the following topics:

About installing BMR software

Bare Metal Restore includes the following software components:

- A master server that controls the operation of BMR. In Bare Metal Restore 7.5 master server is bundled with NetBackup master server and is installed along with NetBackup master server. BMR master server should be configured after the installation of NetBackup master server.
- Boot servers that manage and provide the resources that are used to rebuild systems. In Bare Metal Restore 7.5 Boot server is bundled with NetBackup client and is installed along with NetBackup client. BMR boot server should be registered after the installation of NetBackup client.
- Client software that is installed when the NetBackup client software is installed. No special installation or configuration is required.

Subsequent sections contain instructions for installing BMR.

Before installing BMR

Before you install BMR software, read the *NetBackup Release Notes*. It contains information about supported systems and clusters, dependencies, limitations, and operating system installation prerequisites for BMR.

About installing BMR on UNIX and Linux systems

Bare Metal Restore components are installed when you install NetBackup. However, you must do the following to use BMR:

- Create the BMR database on the master server.
  See "Creating the BMR database" on page 18.

Creating the BMR database

After you activate BMR by entering the license key, setup the BMR master server and create the BMR database.

The BMR master server daemon must be running. Bare Metal Restore master server gets installed with NetBackup master server. After the installation you have to configure the Bare Metal Restore master server.

See the *Symantec NetBackup Administrator's Guide* for information about NetBackup master server installation.

In a cluster environment, start the daemon and create the database on the active node only.

To create the BMR database and setup the BMR master server

1. Log on as the root user on the system on which the NetBackup master server is installed.
2. Run the following command to start the BMR master server daemon, if it is not running:

   ```
   /usr/openv/netbackup/bin/rc.bmrd start
   ```

3. Run the following command to create the BMR database:

   ```
   /usr/openv/netbackup/bin/bmrsetupmaster
   ```

   After you have setup the BMR master server, you can configure backup policies to collect BMR required information from NetBackup clients.

About BMR boot servers on UNIX and Linux systems

The BMR boot server software is installed when you install the NetBackup client. No separate installation is required. However, you must register the boot server.

Every NetBackup server includes the NetBackup client software by default. Therefore, you can run a BMR boot server on either a NetBackup server or a client (if BMR supports that platform).

About choosing boot server hosts

BMR requires specific systems and environments for boot servers. Before you choose the hosts on which to run boot servers, review the boot server requirements.

See "Boot server requirements" on page 201.

About UNIX and Linux prerequisites for boot servers

Bare Metal Restore boot server is a bundled installation with NetBackup client. You must license BMR and create the BMR database before you set up BMR boot servers.

Also see the following subsections for additional prerequisites.

UNIX system prerequisites

The following system prerequisites apply to UNIX systems:

- The `tftp` service and the `bootp` service must be available. On some operating systems, these services are commented out of the `/etc/inetd.conf` file. They must be uncommented and `inetd` needs to be refreshed for the BMR boot server to function.
- The following NFS services are required unless the boot server is used only to create local SRTs for media boot:
  - NFS server services are required to support a network boot of BMR clients.
  - NFS client and server services are required to copy SRTs between boot servers.

  No `/etc/exports` configuration is required; BMR adds and removes specific export permissions as required.
  Look for the `nfsd` process in the process table. If it is not present, ensure that the NFS server is installed and configured. (Solaris automatically starts the NFS server if it is installed normally.)
  If the boot server is used only to create local SRTs for media start, NFS services are not required.

Red Hat Linux system prerequisites

The following system prerequisites apply only to Red Hat Linux systems:

- Install the following RPM packages (unless already installed):
  - `compat-libstdc++`
  - `tftp-server`
  - `dhcp`
- Enable the `tftp` service as follows:
  - Edit the `/etc/xinetd.d/tftp` file and change `disable = yes` to `disable = no`.
  - Start the service by running the following command:
    `/etc/init.d/xinetd restart`
- Create a `/etc/dhcpd.conf` file and configure it to define the networks it serves. You do not have to define host information; hosts are added and removed as needed by the BMR software. The following is an example configuration:

```
log-facility local7;
ddns-update-style none;
ignore unknown-clients;
subnet 10.10.5.0 netmask 255.255.255.0 {
default-lease-time            600;
max-lease-time                7200;
option domain-name            "example.com";
option broadcast-address      10.10.5.255;
option domain-name-servers    10.10.1.4,10.88.24.5;
option routers                10.10.5.1;
}
```

  To verify the `/etc/dhcpd.conf` file syntax, restart the daemon and ensure that it starts successfully by running the following command:
  `/etc/init.d/dhcpd restart`

SUSE Linux system prerequisites

The following system prerequisites apply only to SUSE Linux systems:

- Install the following RPM packages (unless they are installed already):
  - `nfs-utils`
  - `dhcp-base`
  - `dhcp-server`

- inetd
- tftp

- Enable the tftp service by doing the following:
  - Edit the /etc/inetd.conf file and uncomment the tftp line.
  - Start the service by running the following command:
    /etc/init.d/inetd restart
- Modify the /etc/dhcpd.conf file to define the networks it serves. You do not have to define host information; hosts are added and removed as needed by the Bare Metal Restore software. The following is an example configuration:

```
log-facility local7;
ddns-update-style none;
ignore unknown-clients;
subnet 10.10.5.0 netmask 255.255.255.0 {
default-lease-time            600;
max-lease-time                7200;
option domain-name            "example.com";
option broadcast-address      10.10.5.255;
option domain-name-servers    10.10.1.4,10.88.24.5;
option routers                10.10.5.1;
}
```

  To verify the /etc/dhcpd.conf file syntax, restart the daemon and ensure that it starts successfully by running:
  /etc/init.d/dhcpd restart

Setting up a BMR boot server on a UNIX or Linux system

Use the following procedure to set up a BMR boot server on an existing NetBackup system.

Note: The following procedure registers the boot server with the BMR master server using the last CLIENT_NAME entry in the /usr/openv/NetBackup/bp.conf file on the boot server host. That name must resolve to an IP address of one of the network interfaces (except for the loop back address) on the boot server. The bp.conf file may not have a CLIENT_NAME entry or may not meet these criteria. If so, add an entry or fix the bp.conf file before you set up the boot server.

If you do not follow these guidelines, the boot server does not function.

To set up a BMR boot server on a UNIX or Linux system

1. Navigate to the directory where NetBackup is installed. For example:
   `/usr/openv/netbackup/bin`
2. Run the following command on the boot server host:

   ```
   /usr/openv/netbackup/bin/bmrsetupboot -register
   ```

On successful execution of the command you can see the boot server name in the NetBackup Administrator console: **NetBackup Administrator > BMR Menu > Boot server**. This command starts the BMR Boot server daemon running.

About BMR boot servers in a UNIX cluster

The following are general instructions for using a BMR boot server in a clustered environment:

- In the clustering application, set up a virtual IP address on the nodes that provide the BMR boot server functionality.
- Install the NetBackup client software on each node. You can register the Bare Metal Restore boot server on each node that has NetBackup client installed.
  See the *NetBackup Installation Guide for UNIX and Linux*.
  The NetBackup client software includes the BMR boot server software (if BMR supports that platform).
- On each node, configure the NetBackup client name to be the name that resolves to the virtual IP address. Use that name for the last `CLIENT_NAME` entry in the `bp.conf` file on the system.
- Set up the boot server on each node.
  See "Setting up a BMR boot server on a UNIX or Linux system" on page 21.
- Create a cluster application resource that calls the following start and stop scripts for the boot server daemon:

  ```
  /usr/openv/netbackup/bin/rc.bmrbd start
  /usr/openv/netbackup/bin/rc.bmrbd stop
  ```
- When you create SRTs, choose a location on a file system on the shared disk.
- If a boot server fails over and restore tasks are not completed, perform a new prepare-to-restore operation for each incompleted restore task.

About uninstalling BMR on UNIX or Linux systems

You do not uninstall BMR components. Rather, you deactivate them. In NetBackup7.5 BMR master server is bundled with NetBackup master server and

BMR boot server is installed with NetBackup client. If you uninstall NetBackup master server and client, BMR master server and boot server are removed from the system. Refer to the *Symantec NetBackup 7.5 Administrator's Guide* for information about uninstalling NetBackup.

Deactivating the BMR master server on a UNIX or Linux system

Deactivate the BMR master server by deleting the license key from the list of current NetBackup licenses. Before you delete the license key, you should remove the BMR database.

Use the following procedure to remove the BMR database and delete the BMR license key.

After you delete the license key, BMR is no longer available for use.

You can delete the BMR license key only if BMR was licensed with its own key, separate from the base NetBackup product license key.

To deactivate the BMR master server on a UNIX or Linux system

1. Log on as the root user on the system on which the NetBackup master server is installed.
2. To remove the BMR database, execute the following command:

   ```
   /usr/openv/netbackup/bin/bmrsetupmaster -undo -f
   ```

3. To list and delete keys, enter the following command:

   ```
   /usr/openv/netbackup/bin/admincmd/get_license_key
   ```

Deactivating a BMR boot server on a UNIX or Linux system

Deactivate a BMR boot server by using the following procedure.

To deactivate a BMR boot server on a UNIX or Linux system

1. On the NetBackup BMR master server, run the following command to determine the boot server name:

   ```
   /usr/openv/netbackup/bin/bmrs -o list -r bootserver
   ```

   This command lists all BMR boot servers.
2. Log on as the root user to the BMR boot server host.
3. On the NetBackup BMR master server, run the following command to delete the boot server name from the BMR database:

   ```
   /usr/openv/netbackup/bin bmrsetupboot -deregister
   ```

On successful execution of the command, the boot server instance is not visible in NetBackup Administrator Console: **NetBackup Administrator > BMR Menu > Boot server**. Unregistering stops the BMR Boot server daemon running.

Note: BMR Boot server deactivation does not remove SRTs hosted by the BMR Boot server. The SRTs will exist in case they need to be imported by another BMR Boot server or the same Boot server if enabled again in the future.

About installing BMR on Microsoft Windows systems

Bare Metal Restore components are installed when you install NetBackup. However, you must do the following to use BMR:

- Set up BMR on the master server.
  See "Setting up the BMR master server on a Windows system" on page 24.
- Install BMR boot servers.
  See "About understanding BMR boot server installation on Windows systems" on page 25.

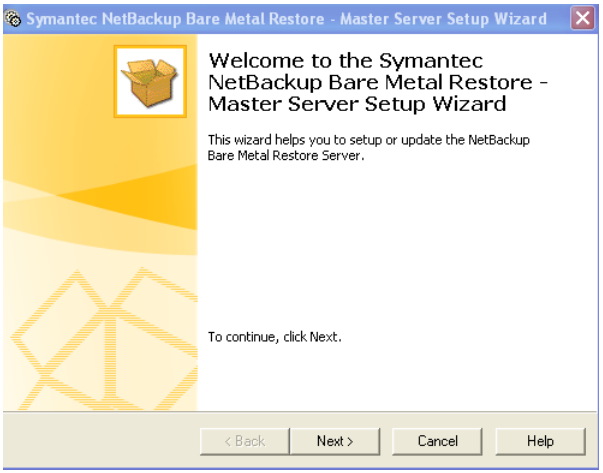
Setting up the BMR master server on a Windows system

Use the Master Server Setup Wizard to set up the Bare Metal Restore master server on a Windows system.

To set up the BMR master server on a Windows system

1 On the Windows BMR master server, select **Programs > Symantec NetBackup > Bare Metal Restore -- Master Server Setup** from the **Start** menu.

The Master Server Setup Wizard **Welcome** panel appears:



2 Follow the prompts to set up the BMR master server.

You do not have to enter any information; the wizard performs all the steps required to set up the master server.

3 If you want to license and set up BMR in a cluster environment, unfreeze the active node after you complete this process.

More information is available about how to unfreeze a service group for the cluster software you are running.

See the clustering section in the *NetBackup High Availability Administrator's Guide*.

About understanding BMR boot server installation on Windows systems

Boot servers provide the environment that is required to rebuild a protected client, including resources such as shared resource trees (SRT).

The BMR boot server software is installed when you install the NetBackup client. No separate installation of the BMR boot server is required. However, you must register the boot server. Every NetBackup server includes the NetBackup client software by default. Therefore, you can run a BMR Boot server on either a NetBackup server or a client (if BMR supports that platform).

See "Boot server requirements" on page 201.

See "Boot server installation prerequisites for Windows systems" on page 26.

See "About BMR boot servers in a Windows cluster" on page 26.

See "Registering a BMR boot server on a Windows system" on page 27.

See "Removing a BMR boot server from a Windows system" on page 31.

Boot server installation prerequisites for Windows systems

Boot server installation prerequisites for Windows systems are as follows:

- Install and configure the BMR master server for the environment before you register the BMR boot servers.
- Disable any PXE services and TFTPD services that are running on the system before you install the boot server package.
- If the boot server is to be installed on an Active Directory Server, let the legacy (DOS) restore method to share SRTs with restoring clients:

  Set the following security settings as shown:

  - Microsoft network server
    Digitally signed communications (always) – Disabled
  - Microsoft network server
    Digitally signed communications (if client agrees) – Enabled

About BMR boot servers in a Windows cluster

For information about the systems where BMR boot servers can be clustered, see the *NetBackup Release Notes*.

The following are general instructions for installing and using a BMR boot server in a clustered environment:

- In the clustering application, set up a virtual IP address on the nodes that provide the BMR boot server functionality.
- Install the NetBackup client software on each node.
- On each node, do the following:
  - Configure the NetBackup client name to be the name that resolves to the virtual IP address.
  - Start the Backup, Archive, and Restore interface.
  - Enter the NetBackup client name as the client name in the **Specify NetBackup Machines and Policy Type** dialog box.

- Make the NetBackup client name the current client.

- Install the BMR boot server software on each node. Switch the virtual address to each node before you install the boot server software.
- Create a cluster application resource that calls the start and stop script for the boot server services:

```
net start "NetBackup Bare Metal Restore Boot Server"
net stop "NetBackup Bare Metal Restore Boot Server"
```

- When you create SRTs, choose a location on a file system on the shared disk.
- If a boot server fails over with restore tasks to be done, perform a new prepare-to-restore operation for each pending restore task.

Registering a BMR boot server on a Windows system

In Bare Metal Restore 7.5, a boot server is bundled with the NetBackup client. You have to register a boot server once you have installed the NetBackup client. If you install the NetBackup client on a remote computer then you have to register the boot server on that system.

Every NetBackup master server includes the NetBackup client software by default. Therefore, you can run a BMR Boot server on either a NetBackup master server or a client (if BMR supports that platform).

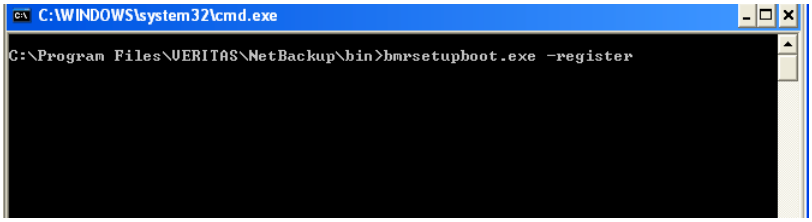
To register a BMR boot server on a Windows system

1. Log on as Administrator on the server where you plan to install the BMR boot server.
2. Open a `command` prompt and navigate to the NetBackup directory.

```
C:\Program Files\Veritas\NetBackup\bin>bmrsetupboot.exe -register
```

3 The **BMR Boot Server** is registered. You can close the command prompt.

The following screenshot shows the registration of **BMR Boot Server**.



4 The BMR boot server is registered.

Note: To install Symantec NetBackup 7.5, refer to the *Symantec NetBackup 7.5 Administrator's Guide*.

Setting up a BMR boot server on a Windows system

Use the following procedure to set up a BMR Boot server on an existing NetBackup system.

Note: The following procedure registers the boot server with the BMR master server using the last `CLIENT_NAME` entry in the `/usr/openv/NetBackup/bp.conf` file on the boot server host. This name must resolve to an IP address of one of the network interfaces (except for the loop back address) on the boot server. The `bp.conf` file may not have a `CLIENT_NAME` entry or may not meet these criteria. If so, add an entry or fix the `bp.conf` file before you set up the boot server. If you do not follow these guidelines, the boot server does not function.

To set up a BMR boot server on a Windows system

1 Navigate to the directory where NetBackup is installed.

For example: `VERITAS\NetBackup\bin`

2 Run the following command on the boot server host:

```
Veritas\NetBackup\bin\bmrsetupboot.exe -register
```

On successful execution of the command you can see the boot server name in the NetBackup Administrator Console at the following location: **NetBackup Administrator > BMR > Boot Servers**.

This command starts the BMR Boot server daemon running.

About uninstalling BMR on Windows systems

You do not uninstall BMR components. Rather, you deactivate or remove them.

Deactivating the BMR master server from a Windows system

The BMR master server software is not uninstalled. Rather, you deactivate the BMR master server by deleting the license key from the list of current NetBackup licenses. When the license key is deleted, BMR is no longer available for use. You can delete the BMR license key only if BMR was licensed with its own key, separate from the base NetBackup product license key.

Before you delete the BMR license key from NetBackup, you should remove the BMR database.

Note: If you remove BMR in a cluster environment, freeze the active node before you remove BMR so that migrations do not occur during removal. For information on how to freeze a service group, see the *NetBackup High Availability Administrator's Guide*.

To deactivate the BMR master server from a Windows system

1. If you are running BMR in a cluster environment, perform the following procedure on the active node.
2. Open a Windows command window.
3. Enter the following command:

   ```
   C:\Program Files\Veritas\NetBackup\bin>bmrsetupmaster -undo
   ```

4. In the following prompt, enter `y` to remove the BMR database.

   ```
   The current BMR database is about to be deleted. Do you want to
   continue? (y/n)
   ```

To delete the BMR license key

1. If you run BMR in a cluster environment, delete the BMR license key on every system in the cluster with the BMR master server installed.
2. On the NetBackup Administration Console, click **Help > License Keys**.

3 In the **NetBackup License Keys** dialog box, select the BMR license key from the list.

Warning: If BMR was included as part of the base product key and you perform the following step, you delete your base key. You cannot use NetBackup. If you do not want to delete the NetBackup license key, do not continue.

4 Click **Delete**.

The BMR license key is deleted from the **Current Licenses** dialog box. **Bare Metal Restore Management** is no longer appears in the NetBackup Administration Console.

In a cluster environment, unfreeze the active node after deactivating BMR from all systems. For information on how to unfreeze a service group, see the *NetBackup High Availability Administrator's Guide*.

Deactivating a BMR boot server on a Windows system

This section provides the procedure to deactivate a BMR boot server.

To deactivate a BMR boot server on a Windows system

1 On the NetBackup BMR master server, run the following command to determine the boot server name:

```
VERITAS\NetBackup\bin\bmrs.exe -o list -r bootserver
```

This command lists all BMR boot servers.

2 Log on to the BMR boot server host, as the root user.

3 On the NetBackup BMR master server, run the following command to delete the boot server name from the BMR database:

```
VERITAS\NetBackup\bin\bmrsetupboot.exe -deregister
```

On successful execution of this command, boot server instance is visible in the NetBackup Administrator console at the following location: **NetBackup Administrator > BMR > Boot server**.

Unregistering stops the BMR Boot server daemon running.

Note: Deactivating BMR Boot server does not remove SRTs hosted by the BMR Boot server. The SRTs are retained if they need to be imported by other BMR Boot server or the same Boot server if enabled again in future.

Removing a BMR boot server from a Windows system

BMR Boot server is uninstalled automatically when NetBackup client or master or media software is uninstalled.

To retain the NetBackup software and disable BMR Boot server, unregister the BMR boot server.

Note: The BMR Boot server unregistration does not remove the SRTs hosted by the BMR Boot server. The SRTs are retained, which can be imported by other BMR Boot server or the same Boot server if enabled again in future.

See the following procedures.

Warning: The following procedure removes the BMR boot server software and all of the shared resource trees on that server.

To remove a BMR boot server from a Windows system

1. Log on as Administrator on the boot server.
2. On the **Start** menu on the Windows BMR boot server, click **Programs > Symantec NetBackup > Bare Metal Restore Boot Server Assistant**.
3. In the Bare Metal Restore boot server Assistant, click **Shared Resource Tree Administration Wizard**.
4. In the Shared Resource Tree Administration Wizard **Welcome** panel, click **Next**.
5. Select **Delete a Shared Resource Tree** and click **Next**.
6. Follow the prompts to delete a shared resource tree.
7. Repeat until all shared resource trees are removed.

To remove the boot server software

Bare Metal Restore Boot server is installed with NetBackup client. You have to unregister the boot server.

1. On the Windows **Start** menu, click **Run > cmd**.

   ```
   C:\Program Files\Veritas\NetBackup\bin>bmrsetupboot.exe
   -deregister
   ```

2. Click **Remove**.

3 Follow the prompts to remove the boot server software.

4 In the NetBackup Administration Console, delete the boot server from the list of available boot servers.

Chapter 3

Monitoring Bare Metal Restore Activity

This chapter includes the following topics:

Monitoring BMR restore tasks

The **Tasks** window shows the status and the resource allocation for the prepare-to-restore and prepare-to-discover operations.

To monitor BMR restore tasks

1. In the NetBackup Administration Console, select **Bare Metal Restore > Tasks**.

   Use the **Refresh** option to update the details pane with new information retrieved from the master server. If an item is highlighted, only that item is updated.

2. To display details about a task, right-click a task in the details pane and then select **Properties**.

   You also can select one of the following other options to manage tasks:

Clean Up	The resources that are used by the task are unallocated, the **State** is set to **Done**, and **Status** is set to 150 (terminated by user). You can clean up the tasks that are in an **Active** or **Waiting** state.
Delete	You can delete the tasks that are in a **Done** state.

About monitoring backup jobs

You can monitor the jobs that back up the protected clients by using the **Jobs** tab in the Activity Monitor of the NetBackup Administration Console.

You can see information about a job by double-clicking the job, which opens the **Job Details** dialog box.

The tabs display job information, as follows:

- The **Job Overview** tab contains general information about the job.
- The **Detailed Status** tab contains detailed information about the job and about the agent that runs on the client. It collects the client configuration information and sends it to the BMR master server. On the protected systems that have uncomplicated configurations (one or a few disks), the agent only takes a few seconds. The more complex systems that have disk or volume groups may take a few minutes. Complex storage area network environments may take up to an hour.

If the **Allow Multiple Data Stream** attribute is enabled in the backup policy, NetBackup may divide backups for each client into multiple jobs. Each job backs up only a part of the backup selection list. The jobs are in separate data streams and can occur concurrently. For each client, only one of the jobs initiates the agent that collects the client configuration (normally, the job with the lowest job ID).

Investigate nonzero status of a backup job and resolve problems so backups occur and the agent collects and sends the configuration to the master server.

BMR logs

You can monitor BMR activity by viewing the messages that are generated by BMR.

BMR activity log files are stored in the following directories on the master server:

- /usr/openv/logs directory (UNIX and Linux)
- *install_path*\NetBackup\logs folder (Windows)

BMR uses a standardized naming format for log files.

The following is an example log file name:

```
51216-119-3892578826-050225-0000000000.log
```

The following are the components of this example log file name:

- `51216` is the product ID for NetBackup.

- 119 is the originator ID of the process that wrote the log (`bmrd` or `bmrbd`, the Bare Metal Restore master or boot server service).
- 3892578826 is a decimal ID for the host that created this log.
- 050225 is the date in YYMMDD format.
- 0000000000 is the rotation number indicating the instance of this log file. If the file reaches maximum size and a new log file is created for this originator, the file rotation number increases by 1.

The following types of messages can appear in unified logging files:

- Application log messages. These include informational, warning, and error messages.
- Diagnostic log messages. The amount of information that is logged depends on the logging level.
- Debug log messages. These are primarily for Symantec support and engineering. The amount of debug information that is logged depends on the logging level that is specified for the NetBackup master server.

BMR logging originator IDs

Following are the originator IDs for the BMR processes that perform logging:

119	`bmrd` and `bmrbd`. Bare Metal Restore master and boot server services. The `bmrbd` boot server process runs on a BMR boot server.
121	`bmrsavecfg`. Bare Metal Restore the agent that runs on client systems, collects the client configuration, and saves the client configuration to the master server.
122	`bmrc`. Bare Metal Restore the utility that clients use to communicate with the BMR master server during a restore. Runs on the restoring client.
123	`bmrs`. The Bare Metal Restore command line interface for the various activities that are performed by the GUIs.
125	`bmrsrtadm`. Bare Metal Restore utility that creates and manages shared resource trees and creates bootable CD media or DVD media for restores. Runs on a BMR boot server.
126	`bmrprep`. Bare Metal Restore utility that prepares BMR for a client restore or discovery. Runs on the master server.
127	`bmrsetupmaster` and `bmrsetupboot`. Bare Metal Restore master server and boot server configuration utilities.

128	Miscellaneous programs and Bare Metal Restore libraries.
129	`bmrconfig`. Bare Metal Restore utility that modifies a client's configuration.
130	`bmrcreatepkg.exe`. Bare Metal Restore utility to add Windows drivers, service packs, and hotfixes to the BMR master server so they can be used in a restore. Runs on Windows boot servers.
131	`bmrrst.exe` and `bmrmap.exe` (Windows systems only). Utilities that restore Windows Bare Metal Restore clients. Run on the restoring client.
142	`bmrepadm`. A utility that manages Bare Metal Restore the external procedures that are used during restores. Runs on the master server.
152	`bmrovradm`. A utility that manages custom override functions for Bare Metal Restore.
248	`bmrlauncher`. A utility that prompts for IP information in the new Windows Fast Restore environment.

Commands to manage unified logging and log files

The amount of information that is collected and the retention period for that information is configured on the NetBackup master server in the Host Properties **Logging** properties and **Clean-up** properties.

See the *NetBackup Administrator's Guide for UNIX and Linux, Volume I* or the *NetBackup Administrator's Guide for Windows, Volume I*.

For information about using and managing logs, see the *NetBackup Troubleshooting Guide*.

BMR activity log files are in a special format that requires you to use commands for viewing and managing.

The following commands manage unified logging and log files:

`vxlogview`	Use this command to view the logs that are created by unified logging.
`vxlogmgr`	Use this command to manage unified logging files (for example, to move or delete log files).
`vxlogcfg`	Use this command to configure logging settings.

These commands are located in the following directories:

- `/usr/openv/NetBackup/bin` directory (UNIX)
- *`install_path`*`\NetBackup\bin` folder (Windows)

About restore logs

The BMR restore process writes messages to restore logs on the master server. The following is the location and naming convention for the log files:

`/usr/openv/netbackup/logs/bmrrst/`*`client_name`*`/log.`*`mmddyy`* (UNIX)
`install_path``\NetBackup\logs\bmrrst\`*`client_name`*`\log.`*`mmddyy`* (Windows)

On UNIX and Linux systems, the messages include external procedure begin and end messages (begin and end logging is not performed by the BMR restore process running on Windows systems).

Unlike BMR activity logs, the restore log files are text files.

Chapter 4

Protecting clients

This chapter includes the following topics:

About backing up BMR clients

A client is protected after a NetBackup backup policy that is configured for BMR protection backs it up. Backups must occur before a client fails and requires a Bare Metal Restore.

Each protected client must be backed up regularly by at least one policy that performs a full backup. The policy also can perform cumulative incremental or differential incremental backups, but a full backup must occur.

The backup saves the files of the computer on a storage device that NetBackup manages. The backup saves the configuration of the client on the BMR master server.

After a client is backed up by a policy that is configured for BMR protection, the client is registered with BMR as a protected client. It then appears in the **Bare Metal Restore Clients** view in the NetBackup Administration Console.

About configuring policies to back up BMR clients

You can use one policy or multiple policies to protect a single client.

The following are the requirements for protecting BMR clients:

- A policy must be one of two types: **MS-Windows** (for Windows clients) or **Standard** (for UNIX and Linux clients).
- A policy must have the **Collect disaster recovery information for Bare Metal Restore** attribute set.

On NetBackup master servers that are licensed for BMR, NetBackup sets the following attributes automatically:

- The **Collect disaster recovery information for Bare Metal Restore** attribute (when you create a new MS-Windows or Standard policy)
- The **Collect true image restore information** and **with move detection** attributes (albeit grayed out)

These attributes enable NetBackup to restore only those files present on the system at the time of the backup. Move detection enables NetBackup to restore the files correctly that were moved, renamed, or newly installed. These attributes also ensure that all of the restored files fit in the volumes and the file systems that BMR created during the recovery.

If the **Collect disaster recovery information for Bare Metal Restore** attribute is not set, BMR does not protect the client.

User-initiated backups do not provide BMR protection because true image restore information is not collected during a user-initiated backup.

- The operating system files must be backed up by a single policy. For Windows clients, include `SYSTEM_STATE` in the policy that backs up the operating system.

Consider the following when you create policies to protect BMR clients:

- For non-clustered clients, specifying `ALL_LOCAL_DRIVES` is the simplest and most thorough way to obtain a complete backup. If you back up a client with database or application files using a NetBackup database agent or other policy, use an exclude list to exclude them from the policy that specifies `ALL_LOCAL_DRIVES`.
- For clustered clients, the most effective backup strategy uses multiple policies. Each node should have its own policy that backs up local file systems. Shared file systems should be backed up by the additional policies that back up the node that currently owns the resources.
- The logical volumes that are not part of the operating system can be backed up with different policies. However, each logical volume must be backed up by a single policy.
- Schedule all policies that back up a single client to run at the same time.
- NetBackup media servers can be protected as BMR clients. Media servers that back up to their own storage devices (either SCSI-attached or SAN-attached) require special procedures for restores. If you understand these procedures, you can configure NetBackup to minimize the time and effort that the restores require.

  See "About restoring NetBackup media servers" on page 84.

Information about configuring backup policies is available.

See the *NetBackup Administrator's Guide for UNIX and Linux, Volume I* or the *NetBackup Administrator's Guide for Windows, Volume I*.

About performing complete backups

To restore all files on the client, you must back up all of the files on the client. If you exclude files during the backup, those files are not backed up and therefore are not restored.

About performing a full backup after a restore

You must perform a full backup of a client immediately after you restore the client and before any incremental backups occur. If the client fails again after an incremental backup but before a full backup, BMR cannot restore the client.

You can perform a manual backup of a specific client. The policy must be set to **Active** and the **Go into effect at** attribute must not be set to a future date and time.

Ensuring successful backups

Schedule backups when the risk of an incomplete backup is minimized. If a client cannot be forced into an inactive state during a backup, do the following:

Table 4-1 Steps to ensuring successful backups

Step	Action	Reference
Step 1	For UNIX clients, configure NetBackup to retry file backups if a file changes during the backup attempt. More information is available on busy file properties.	See the *NetBackup Administrator's Guide for UNIX and Linux, Volume I* or the *NetBackup Administrator's Guide for Windows, Volume I*.
Step 2	For Windows clients, configure NetBackup to use a **Windows Open File Backup** option. More information is available on **Windows Open File Backup** properties.	See the *NetBackup Administrator's Guide for UNIX and Linux, Volume I* or the *NetBackup Administrator's Guide for Windows, Volume I*.

Table 4-1 Steps to ensuring successful backups *(continued)*

Step	Action	Reference
Step 3	Examine the NetBackup log files regularly to ensure that any backup errors are corrected promptly. During backup, network or server errors can occur that affect the backup.	

About saving custom files on UNIX or Linux

The following information applies only to UNIX and Linux clients.

Usually, NetBackup restores client files as the last step in the restore process. You can specify custom files on the client so they are available in the temporary operating system environment on the client during the restore process.

For example, a specific device driver configuration from a protected client is required in the temporary operating system. You can specify those device driver files so they are included in the restore environment.

Custom files are saved as part of the client's configuration. Specify the custom files in the following text file on the client:

```
/usr/openv/netbackup/baremetal/client/data/ClientCustomFiles
```

Specify one custom file per line, using the full path name to the file. Use a pound sign (#) as the first character of comment lines.

After custom files are saved (when the client is backed up), they are copied to the SRT. They are available during the restore when you enable the SRT for exclusive use. More information is available on how to enable the SRT.

See "Enabling or disabling SRT exclusive use" on page 131.

When you specify a custom file, it does not remove it from backups. Custom files are also backed up by NetBackup and then restored when NetBackup restores the client files. (They are backed up and restored if the files or their directories are included in the backup directives of the policy.)

About monitoring client backups

You can use the NetBackup Activity Monitor to monitor the backup jobs. Details about the backup job include information about the agent that saves the protected client's configuration.

See "About monitoring backup jobs" on page 34.

About using the ALL_LOCAL_DRIVES directive to back up files on the client

To ensure complete system recovery, use the ALL_LOCAL_DRIVES directive to back up all local drives. This directive backs up all files on the client and backs up the system objects (SYSTEM_STATE) for Windows clients.

If a client has database or application files to back up using a NetBackup database agent or other policy, you can use an exclude list to exclude them from the policy that specifies ALL_LOCAL_DRIVES.

About using the same client name in multiple policies

If you use more than one policy to back up a client, use the exact same name for the client in each policy.

BMR can only restore a client using the client that is named in the policy that backed up the system files. If you use multiple policies with a different name in each policy, a client record and its associated configuration is created for each client name. If you restore a client by a name in a policy that does not back up the system files, the prepare-to-restore operation fails. It fails because BMR can only restore using the client that is named in the policy that backed up the system files.

Therefore, if you use the same name, you do not have to choose between multiple client names during a restore.

About Solaris Zone support

When using BMR to back up and restore Solaris Zones, you need to address some unique considerations.

Bare Metal Restore can restore a Solaris system running Zones. Although BMR cannot restore individual non-global zones, all non-global zones in a system are re-created as part of the global zone restoration.

To restore all non-global zones in a dissimilar disk restoration scenario

- Remap the file system that hosts the zone (also known as zone path) to restore the zone files.

  If a non-global zone imports slices from the global zone that are not remapped, BMR removes the slices from the zone configuration.

  If a non-global zone imports slices from the global zone that are remapped to different disks, BMR readjusts the zone configuration and any zone `vfstab` (`ZONEPATH/root/etc/vfstab`) entries to use the new device names.

  If a non-global zone imports systems from the global zone file that are not remapped, BMR removes any references to them in the zone configuration.

You may have to re-create and restore all file systems imported or used by a non-global zone after BMR restoration. These file systems usually don't appear in the global zone `vfstab` (`/etc/vfstab`).

BMR relies on entries in `/etc/vfstab` to document the file systems that are subject to restoration. Dynamically-created and mounted file systems that do not appear in `/etc/vfstab` (even if backed up by NBU) do not automatically restore. The easiest way to force BMR to restore such file systems is to add an entry to `/etc/vfstab` that documents the devices and mount points used, with the **Mount at boot** field set to **No**. Then, the dynamic file systems can continue to be used as before. BMR is aware of them, recreates them unless unmapped in DDR, and restores their contents if backed up by NBU.

Zone features cause dynamically mounted file systems to appear, as follows:

- FS entries that involve devices in the global zone.
- Device entries imported from the global zone but mounted either by the `/etc/vfstab` of the non-global zone, or dynamically by the zone itself.

To automate BMR zone restoration

- Add entries to the global zone `/etc/vfstab` that cause BMR to restore them (unless unmapped by DDR), as follows:
  - For FS entries, the global zone devices are used as special and raw values with a mount point that appears under the root of the non-global zone . The entry to add to the global zone's `/etc/vfstab` should use the global zone's device paths with the full path to the non-global zone mount point, including the zone path. For example, if the zone looks like:

```
zonepath=/export/zone1
fs:
  dir=/export
```

```
special=/dev/dsk/c0t9d0s6
raw=/dev/rdsk/c0t9d0s6
type=ufs
```

Then the global zone entry in `/etc/vfstab` should be as follows:

```
/dev/dsk/c0t9d0s6 /dev/rdsk/c0t9d0s6 /export/zone1/root/export ufs
- no -
```

- For device entries mounted by the non-global zone, the following issues must be dealt with when you configure for BMR restoration:
  - The dynamic mount that is used involves the imported device path under the zone path. For a device that is mounted by an `/etc/vfstab` inside a non-global zone, there are one or more device entries in the zone, such as the following:

    ```
    zonepath=/export/zone2
      device:
      match=/dev/*dsk/c0t0d0s4
    ```

    The devices that are listed are in the non-global zone's `/etc/vfstab` as follows:

    ```
    /dev/dsk/c0t0d0s4 /dev/rdsk/c0t0d0s4 /local ufs - yes -
    ```

    This command causes the global zone to dynamically mount. `/export/zone2/dev/dsk/c0t0d0s4` on mount point `/export/zone2/root/local`. However, to make BMR automatically recreate the file system, you should add the documenting entry to the global zone `/etc/vfstab` instead as follows:

```
/dev/dsk/c0t0d0s4 /dev/rdsk/c0t0d0s4 /export/zone2/root/local ufs - no -
```

    (If you use the device paths relative to the zone path, BMR only recreates the mount point instead of restoring the whole file system.)
  - The device match should not use wildcards to allow BMR to edit if DDR is used. When the device specification involves a wildcard, if DDR mapping is done that affects the zone (for example, if you unmap or move a file system from one disk to another), BMR is not able to edit the entry. The affected zone's `/etc/vfstab` is edited, but the device match entries are edited only if the match does not include a wildcard. For example, change the following entry:

```
match=/dev/*dsk/c0t0d0s4
```

The entry must use two device entries, as follows:

```
match=/dev/dsk/c0t0d0s4
match=/dev/rdsk/c0t0d0s4
```

If the entries are changed as the example shows, BMR DDR correctly updates the zone definitions and `vfstab` file.

About configuring NetBackup properties

Configure the following NetBackup properties:

- The **Allow client restore** property. The BMR restore process requires that both the BMR master server and the BMR client can request restores. The default NetBackup behavior is to allow client restores. The **Allow client restore** property is located on the **Client Attributes** tab of the NetBackup master server properties.
- Server-directed restores. Configure the NetBackup clients for server-directed restores, which allows the master server to redirect restores of client files to itself. Server-directed restores are the default NetBackup behavior; ensure that server-directed restores are allowed. For more information, see the *NetBackup Administrator's Guide, Volume I*.
- The **Keep true image restoration (TIR)** information property. This property controls how long TIR information is retained in the NetBackup catalog. TIR information increases catalog size and the disk space that is uses.

  The following settings are your options:

  - Choose a value for this attribute to match the retention policy.
  - Alternatively, if you want to minimize the size of the NetBackup catalog, set the attribute to zero days. The TIR information is also stored on the backup media, so the catalog size does not increase but restores are slower.

  Set the **Keep true image restoration (TIR)** information property on the **Clean-up** tab of the NetBackup master server properties.

For information about how to configure NetBackup, see the *NetBackup Administrator's Guide, Volume I*.

Chapter 5

Setting up restore environments

This chapter includes the following topics:

Setting up restore environments

Before you can restore a protected client, you must set up the resource environment that is used during the restore.

You can set up the environment at any time. However, if your recovery time objective (RTO) is short, you may want all of the resources in place. Your time is used in recovery rather than set up.

Table 5-1 Process for setting up restore enivronments

Step	Action	Related topic
Step 1	Install boot server software	See "About installing boot server software" on page 48.
Step 2	Create shared resource trees	See "About shared resource trees" on page 48.

Table 5-1 Process for setting up restore enivronments *(continued)*

Step	Action	Related topic
Step 3	Add client resources	See "About adding client resources" on page 48.
Step 4	Create boot media	See "When to use boot media" on page 49.
Step 5	Verify the protection	See "About verifying the protection" on page 49.

About installing boot server software

Boot servers provide the environment that is required to rebuild a protected client, including resources such as shared resource trees (SRT). You must have a boot server for each type of client that you want to protect. In addition, you must install the BMR boot server software before you can create SRTs and add resources to them.

See "About boot servers" on page 201.

About shared resource trees

A shared resource tree (SRT) is a collection of the following:

- Operating system files
- NetBackup client software
- Other programs to format drives, create partitions, rebuild file systems, and restore the original files using the NetBackup client software

More information is available about SRTs and procedures to create and update SRTs.

See "About shared resource trees" on page 103.

About adding client resources

The following information applies only to Windows clients.

Dissimilar system restores may require some resources that are not included in the protected client's saved configuration. If so, you must add them to the client configuration that is used for the restore (the restore configuration).

Examples of such resources are as follows:

- Network interface card (NIC) drivers
- Mass storage device (MSD) drivers

These resources must be in the BMR packages pool so they are available to add to the restore configuration.

More information is available about how to add packages to the packages pool.

See "Adding a Windows driver package" on page 166.

Information about managing clients is available.

See "About clients and configurations" on page 169.

When to use boot media

The BMR restore process begins by booting the client (using the network boot) from a BMR boot server or from BMR prepared boot media (CD, DVD, or floppy).

If you use a network boot to begin the restore, boot media is not required.

If you have minimal network connectivity when you restore a client, Symantec recommends that you use the boot media that contains a shared resource tree.

More information is available about boot media and procedures for creating boot media.

See "About boot media" on page 157.

About verifying the protection

Optionally, you can verify that everything is in place to restore a client. BMR automates the pre-recovery verification for a client when a prepare-to-restore operation is performed.

More information is available on this subject.

See "Preparing a client for restore" on page 54.

Chapter 6

Restoring clients

This chapter includes the following topics:

About restoring clients

The process to restore a protected system depends on the type of restore you want to perform and the operating system of the client.

Table 6-1 Restore types

Restore type	Procedures
To restore to the same client and use the most recent backup	See "About restoring BMR clients using network boot" on page 60. See "About restoring BMR clients using media boot" on page 66.
To restore to a specific point in time	See "About restoring to a specific point in time" on page 72.
To restore a client in which the disks are different	See "About restoring to dissimilar disks" on page 73.
To restore to a new target system (only on Windows systems)	See "Restoring to a dissimilar Windows system" on page 78.
To restore a NetBackup media server	See "About restoring NetBackup media servers" on page 84.
To restore a BMR boot server	See "About restoring BMR boot servers" on page 86.
To customize the restore process	See "About external procedures" on page 87.
To restore to hosts with Veritas Storage Foundation for Windows.	See "About legacy restores on Windows" on page 211.

Other information is available.

See "Preparing a client for restore" on page 54.

See "About BMR disk recovery behavior" on page 56.

See "About storage area network support" on page 96.

See "Port usage during restores" on page 100.

About the restore process

The NetBackup BMR master server manages the restore process, as follows:

- The master server creates the necessary configuration files and restore scripts (on UNIX and Linux) or restore processes (on Windows) and allocates the boot server when the prepare-to-restore operation runs.
- The client boots either by network boot or media boot.

- The client accesses the shared resource tree, either on a boot server or on the boot media.
- The client runs a temporary operating system environment that is known as the restore environment. The restore environment starts from the shared resource tree.
- The client restore environment retrieves the restore script and configuration files from the master server.
- The client restore environment starts the customized restore script, which configures disks.
- The client restore environment performs an automated restore using the NetBackup client software, which restores all required files and data from the NetBackup server.
- The client reboots, which starts the restored operating system and deallocates the boot server.
- Dissimilar system restore tasks are completed (dissimilar system restore only).

Figure 6-1 shows a standard network restore.

Figure 6-1 Network restore

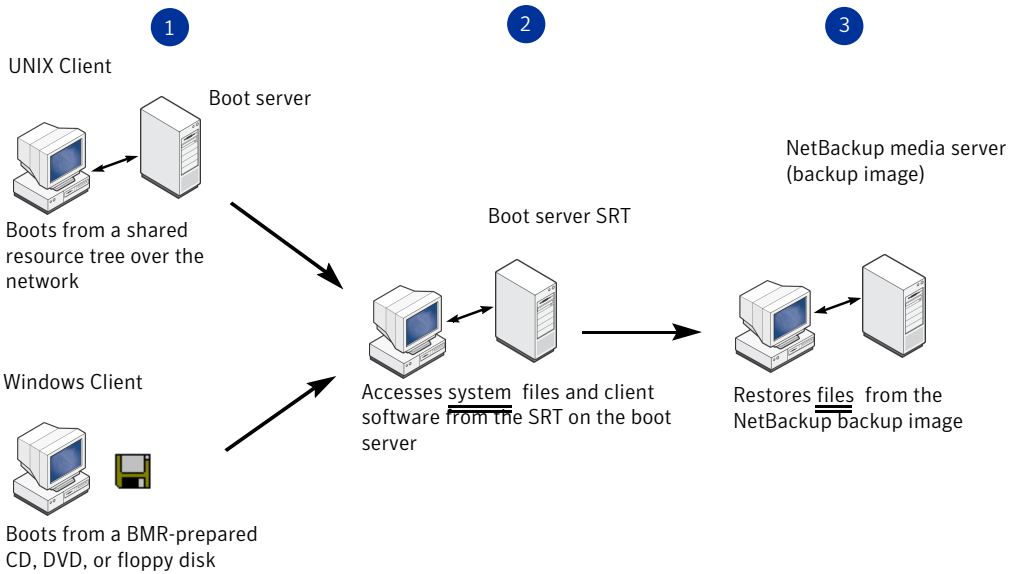
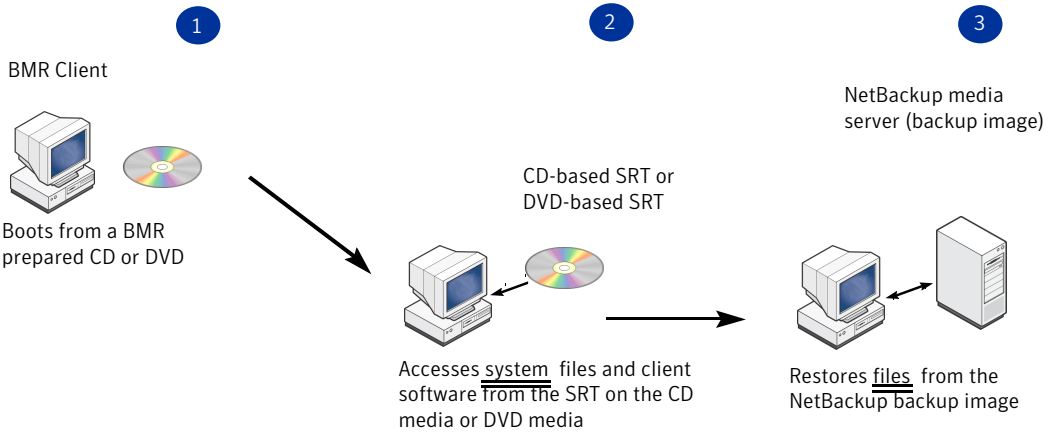


Figure 6-2 shows a media restore.

Figure 6-2 Media restore



Preparing a client for restore

Before you restore a client, you must prepare to restore the client.

During a prepare-to-restore operation, the NetBackup master server does the following:

- Retrieves the client configuration from the master server database.
- Creates the restore script and the configuration files that are used to restore the client.
- Allocates the boot server resources to the client.

When you prepare to restore a client, you select the configuration to use for the restore, as follows:

- For a standard restore (also known as a self restore, which is a restore to the same system), select the current configuration.
- For other types of restores, select the configuration that you created for the restore.

To ensure that the restore includes the most recent data, Symantec recommends that you prepare to restore immediately before you restore a system.

If you run the prepare-to-restore operation to verify the protection, you must clean up the restore configuration as shown in the following prepare-to-restore procedure.

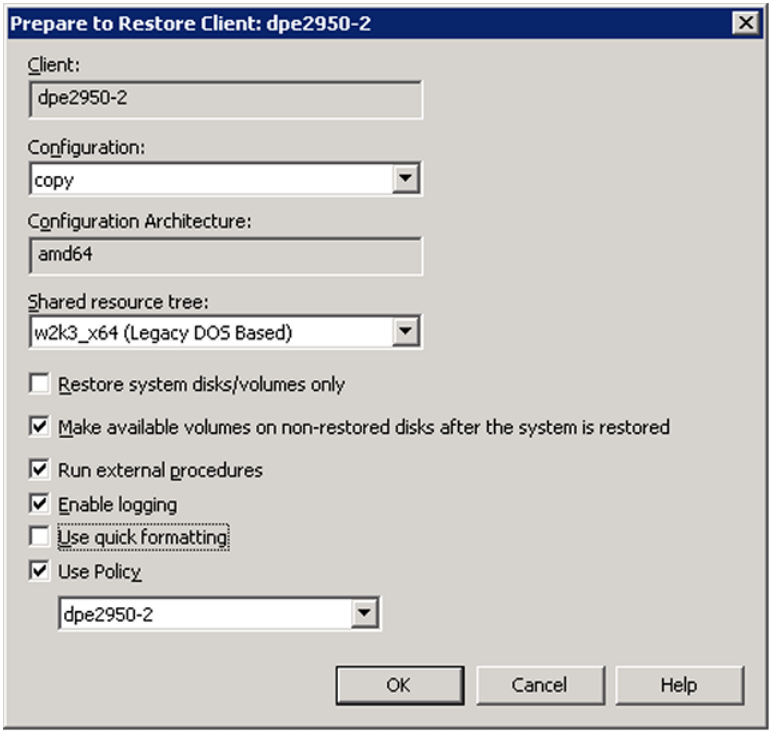
You can clean up the tasks that are in an **Active** state or a **Waiting** state.

To prepare a client for restore

1 In the NetBackup Administration Console, expand **Bare Metal Restore Management > Hosts > Bare Metal Restore Clients**.

2 Select a client or a client configuration.

3 Select **Actions > Prepare to Restore**.



4 In the **Prepare to Restore Client** dialog box, select the appropriate values for the restore.

Some fields may be completed depending on whether you selected a client or a client configuration.

See "About BMR disk recovery behavior" on page 56.

5 Click **OK**.

Bare Metal Restore runs all the processes to prepare for a restore.

6 After the processes finish, in the dialog box that appears, click **OK**.

The client is listed in the **Tasks** view with a **State** of **Queued**.

To clean up the restore configuration

1. In the NetBackup Administration Console, click **Bare Metal Restore Management > Tasks**.
2. In the details pane, right-click the client for which you want to clean up the restore configuration.
3. Select **Clean Up** from the shortcut menu.

   The resources that the task uses are unallocated, the **State** is set to **Done**, and **Status** is set to 150, terminated by user.

About BMR disk recovery behavior

BMR either restores or imports disks during a restore, as follows:

- To restore a disk means that BMR formats the disk and restore files to it. No attempt is made to retain any data on the disk.
- To import a disk means that BMR tries to reuse the volumes on it (that is, mount the file systems after restore). BMR tries to reuse rather than format the disk and restore files to it.

BMR always restores the system disk. For other disks, the following two options on the **Prepare to Restore Client** dialog box control BMR behavior:

- **Restore system disks/volumes only**.

  If you select this option, BMR restores only the system disk. Otherwise, BMR tries to import (reuse) non-system disks that are based on the disk class and the following option. System disk is defined as the following:

  - On AIX and HP-UX, the root volume groups (`rootvg` and `vg00`) are restored.
  - On Solaris, all disks that have any of the root file systems (`/`, `/swap`, `/var`, `/usr`) are restored.
  - On Windows, all disks that have `%SystemRoot%`, `%SystemBoot%`, and `%TEMP%` are restored. On Active Directory servers, BMR also restores the disks that contain the Active Directory system, database, and log files.
  - On Linux, all disks that have `/`, `usr/`, `/usr/local`, `/var`, `/opt`, `/tmp`, and `/boot` are restored.

- **Make available volumes on non-restored disks after the system is restored**.

  If you select this option, BMR imports the disks. Otherwise, the action depends on the disk class.

  See "BMR disk class processing with prepare-to-restore options" on page 58.

The following are the disk classes:

- System disks contain the operating system files that are required to boot the system.
- Nonsystem disks are all other disks, as follows:
  - Restorable disks are visible in the temporary restore environment and therefore can be restored. Visible means locally attached.
  - Nonrestorable disks are not visible in the temporary restore environment and therefore cannot be restored. Typically these are SAN devices. You may not know that these disks cannot be restored until you attempt a restore. If these disks are required for a restore, you are forced to do a dissimilar disk restore (DDR).
  - Shared disks are shared with another system using clustering software. The client may not control them during or after the restore.
  - Missing disks may or may not have been used and are no longer attached to the system. These disks are in the restore configuration. More information is available about the actions to perform for missing disks. See "BMR disk class processing with prepare-to-restore options" on page 58.
  - New disks are attached to the system in previously unused locations and used by any volume or any volume group. New disks are not in the original configuration.

BMR also restricts some disks so they are not processed during a restore. For example, BMR restricts shared disks in a cluster and unused VxVM disks on Solaris systems. Additionally, you can restrict a disk so BMR does not process it.

BMR disk processing with prepare-to-restore options

Table 6-2 describes how BMR processes disks, depending on the two prepare-to-restore options.

Note the following about the restore options column:

- **System only** is the **Restore system disks/volumes only** option for prepare to restore.
- **Import** is the **Make available volumes on non-restored disks after the system is restored** option for prepare to restore.

Table 6-2 BMR disk actions

Restore options	System Disks	Nonsystem disks Restricted=false	Nonsystem disks Restricted=true
System only = **true** and **import** = **true**	Restore	Import	No action
System only = **true** and **import** = **false**	Restore	No action	No action
System only = **false** and **import** = **true**	Restore	Restore if possible otherwise import	No action
System only = **false** and **import** = **false**	Restore	Restore	No action

BMR disk class processing with prepare-to-restore options

Table 6-3 describes the actions that BMR performs for system disks and any action you should perform.

Table 6-4 describes the actions that BMR performs for nonsystem disks and any action you should perform.

Note the following about the **Restore options** columns of the tables:

- **System only** is the **Restore system disks/volumes only** option for prepare to restore
- **Import** is the **Make available volumes on non-restored disks after the system is restored** option for prepare to restore

To avoid conflicts with other cluster nodes that may use surviving shared disks during a restore, shared disks should remain restricted or be unmapped or remapped to alternate, non-shared restorable locations. Shared disks should only be unrestricted and restored in-place if other cluster nodes are do not hold the share actively during the restore.

Table 6-3 Actions for system disks

Restore options	Action
System only = **true** and **import** = **true**	Restore
System only = **true** and **import** = **false**	Restore
System only = **false** and **import** = **true**	Restore

Table 6-3 Actions for system disks *(continued)*

Restore options	Action
System only = **false** and **import** = **false**	Restore
System only = **true** and **import** = **true**	Restore

Table 6-4 Actions for nonsystem disks

Restore options	Restorable	Nonrestorable	Shared	Missing	New
System only = **true** and **import** = **true**	Import	Import	No action	Mark the restricted disk, remap to a restorable disk, or remove the disk from the restore configuration	Not imported
System only = **true** and **import** = **false**	No action	No action	No action	No action	No action
System only = **false** and **import** = **true**	Restore	Import	No action	Mark the restricted disk, remap to a restorable disk, or remove the disk from the restore configuration	Not imported
System only = **false** and **import** = **false**	Restore	Remove the disk from the restore configuration or mark the disk restricted	No action	Mark the restricted disk, remap to a restorable disk, or remove the disk from the restore configuration	No action
System only = **true** and **import** = **true**	Import	Import	No action	Mark the restricted disk, remap to a restorable disk, or remove the disk from the restore configuration	Not imported

Import actions for operating systems or volume managers

Table 6-5 describes the import action for each operating system or volume manager.

Note the following regarding import actions:

- HP-UX logical volume manager is a virtual auto import. An HP system can have VxVM managed root disks and some LVM managed disks. In a system only restore, the LVM database (the `/etc/lvmtab` file) is restored. Without any action required by BMR, these disks and their volumes are available. If entries remain in the `/etc/fstab` file for the file systems, those file systems are available.

- During a merge on Solaris systems or a merge on VxVM, BMR may remove entries in the `/etc/fstab` or `/etc/vfstab` files by commenting them out.
- Veritas Volume Manager is an auto import. VxVM has the ability (a disk group option) to import disk groups automatically. If there are entries in the `/etc/fstab` and the `/etc/vfstab` files, the file systems are available without BMR having to take action.
- For Windows imports, the following are true:
  - Without import, only the drive letters that were recreated are assigned after restore.
  - With import, the drive letters assigned to volumes on Trusted disks are assigned to the same location after the restore. If the volume does not exist or has moved, you must edit the Mount Devices registry key.

Table 6-5 Import actions

OS and volume manager	What import means
AIX logical volume manager	Run `importvg` at restore time or during first boot.
HP-UX logical volume manager	Merge `lvmtab`, merge `fstab`.
Linux	Merge `fstab`.
Solaris	Merge `vfstab`.
Veritas Storage Foundation for Windows	Assign drive letter by `MountedDevices`, run `vxdg` import.
Veritas Volume Manager	Run `vxdg` import, merge `fstab`.
Windows	Assign drive letter by `MountedDevices`.

About restoring BMR clients using network boot

Use these procedures for a standard restore (also known as a self restore, which is a restore to the same system and disks).

Note: If NetBackup access management is used in your environment, you must provide the appropriate credentials when prompted so that NetBackup can restore the client files.

Before you do a standard restore, you must run the prepare to restore operation using the current, saved configuration.	See "Preparing a client for restore" on page 54.
In a network boot, the BMR client boots from the shared resource tree on the BMR boot server. How you restore a machine over the network depends on its manufacturer and model.	See "Restoring an AIX client with network boot" on page 61. See "Restoring a Solaris client with network boot" on page 65. See "Restoring an HP-UX client with network boot" on page 62. See "Restoring a Linux client with network boot" on page 64. See "Restoring a Windows client with network boot" on page 66.
Other information about restoring clients is available.	See "About external procedures" on page 87. See "About performing complete backups" on page 41. See "About performing a full backup after a restore" on page 41. See "Ensuring successful backups" on page 41.

Restoring an AIX client with network boot

Note: If NetBackup access management is used in your environment, you must provide the appropriate credentials when prompted so that NetBackup can restore the client files.

An AIX boot (either network boot or media boot) may set the network interface configuration, speed, and duplex mode to auto-negotiate or 10 half duplex. This setting may cause the BMR restore to run much more slowly than expected. To achieve normal restore performance, manually set the network interface configuration through the firmware before a BMR restore.

AIX system restore requires certain information and resources.

The information varies according to architecture, but can include the following:

- Network adapter type
- BMR client IP address
- BMR client subnet mask
- BMR boot server IP address
- BMR client gateway address

After you perform the network boot procedure, the remainder of the restore process is automatic and requires no manual intervention. After the restore finishes and the client reboots itself, it is completely restored.

You can network boot an AIX system that has AIX installed, which does the following:

- Updates the NVRAM with the proper addresses for the BMR boot server, client, and gateway address.
- Boots by `bootp` from the BMR boot server. If the boot server does not answer the `bootp` request, the computer boots from the hard drive.

The network boot only works when the BMR client is properly prepared for restore.

Warning: Do not perform this procedure unless you intend to do a restore. When you prepare a client for restore, the process may result in a restore.

To restore an AIX client with network boot

1. Prepare to restore the client.

   See "Preparing a client for restore" on page 54.

2. Boot from a network interface according to the procedures in the IBM hardware documentation.

Restoring an HP-UX client with network boot

Note: If NetBackup access management is used in your environment, you must provide the appropriate credentials when prompted so that NetBackup can restore the client files.

HP-UX system restore requires certain information and resources.

The information varies according to architecture, but can include the following:

- BMR client IP address
- BMR client gateway address
- BMR client subnet mask
- Ignite Server Address (usually, the BMR boot server).

To begin this procedure, the BMR client must be OFF.

After you perform the network boot procedure, the remainder of the restore process is automatic and requires no manual intervention. After the restore finishes and the client reboots itself, it is completely restored.

To restore an HP-UX client with network boot

1. Prepare to restore the client.

   See "Preparing a client for restore" on page 54.

2. Ensure that the client is turned off .
3. Turn on the client.
4. Press any key when the following message appears.

   ```
   To discontinue, press any key within 10 seconds.
   ```

5. In the **Main** Menu, do one of the following to begin the network boot process:

   - If only one Ignite server is on the subnet, enter the following boot command:

     ```
     boot lan
     ```

   - If there is more than one Ignite server on the subnet, specify the Ignite server to boot from by using the following command: (Replace *x.x.x.x* with the IP address of the Ignite server and *y.y* with the gateway.)

     ```
     boot lan.x.x.x.x.y.y
     ```

     Use the same command if you use a boot helper to boot from an Ignite server on a different subnet.

6. Enter `No` when the prompt asks if you want to interact with IPL.
7. If the client is a workstation, select the operating system language by number. For example, US English is 61.
8. After you enter the language choice, press **Enter** twice to select and confirm the choice. The HP-UX Ignite menu opens.

9 Use the arrow key to scroll to **Run a Recovery Shell**. Wait while the DHCP search occurs and until the **Network Configuration** menu opens. If you interrupt a DHCP search, the BMR restore may fail.

10 Answer the following prompts:

- `Hostname:`
- `Internet Protocol Address:`
- `Subnet mask:`
- `Ignite Server Address (typically the BMR boot server):`

11 Use the arrow key to scroll to **OK** and press **Enter**.

The system boots from the network.

Restoring a Linux client with network boot

Note: If NetBackup access management is used in your environment, you must provide the appropriate credentials when prompted so that NetBackup can restore the client files.

To network boot Linux clients, BMR requires the following:

- `PXE`
- `DHCP`

During the prepare-to-restore operation all the information is gathered that is required for a Linux network boot. After the prepare-to-restore, boot the client to start the restore.

To network boot a Linux client

1 Prepare to restore the client.

See "Preparing a client for restore" on page 54.

2 Ensure that the client is turned off .

3 Turn on the client.

4 PXE Boot the client according to the hardware vendor instructions.

On some systems, the BIOS displays a message that indicates that you can press a key to force a PXE Boot . On others, you may have to modify the settings in the BIOS to add the network card to the default boot order. Consult your hardware documentation for details.

5 When you are prompted, either press the **Enter** key or wait until the system boots.

The system boots and the restore begins with no further user intervention required.

Restoring a Solaris client with network boot

Note: If NetBackup access management is used in your environment, you must provide the appropriate credentials when prompted so that NetBackup can restore the client files.

Solaris system restore requires the name of the device that directs the client to the correct BMR boot server.

After you perform the network boot procedure, the remainder of the restore process is automatic and requires no manual intervention. After the restore finishes and the client reboots itself, it is completely restored.

To restore a Solaris client with network boot

1 Prepare to restore the client.

See "Preparing a client for restore" on page 54.

2 Ensure that the client is turned off .

3 Turn on the client.

4 Terminate the boot process by using the **Stop**+**A** key combination.

5 If the PROM monitor prompt displays a left angle bracket (<), use the N command to get to the **OK** prompt.

6 Start the network boot by entering the following command (*network_device* is the device that points to the BMR boot server):

```
boot network_device
```

Restoring a Windows client with network boot

Note: If NetBackup access management is used in your environment, you must provide the appropriate credentials when prompted so that NetBackup can restore the client files.

Windows systems network boot uses the PXE protocol. The BMR boot server provides and manages the PXE network services, but a DHCP service is required in the environment.

To restore a Windows client with network boot

1. Prepare to restore the client.

   See "Preparing a client for restore" on page 54.

2. Ensure that the client is turned off .
3. Turn on the client.
4. PXE Boot the client according to the hardware vendor instructions. On some systems, the BIOS displays a message that indicates that you can press a key to force a PXE Boot . On others, you may have to modify the settings in the BIOS to add the network card to the default boot order. Consult your hardware documentation for details.
5. When you are prompted, press the **Function 12** key and the system boots and the restore begins with no further user intervention required.

About restoring BMR clients using media boot

Use these procedures for a standard restore (also known as a self restore, which is a restore to the same system and disks).

To restore using media boot requires that you first create bootable media.	See "Creating boot media for UNIX and Linux" on page 160. See "Creating boot media for a Windows client" on page 162.
Before you do a standard restore, you must run the prepare to restore operation using the current, saved configuration.	See "Preparing a client for restore" on page 54.

The procedure for restoring the client system depends on the manufacturer and mode.	See "Restoring an AIX client with media boot" on page 67. See "Restoring an HP-UX client with media boot" on page 68. See "Restoring a Linux client with media boot" on page 69. See "Restoring a Solaris client with media boot" on page 70. See "Restoring a Windows client with media boot" on page 71.
Other information about restoring clients is available.	See "About external procedures" on page 87. See "About performing complete backups" on page 41. See "About performing a full backup after a restore" on page 41. See "Ensuring successful backups" on page 41.

Restoring an AIX client with media boot

Note: If NetBackup access management is used in your environment, you must provide the appropriate credentials when prompted so that NetBackup can restore the client files.

An AIX boot (either network boot or media boot) may set the network interface configuration, speed, and duplex mode to auto-negotiate or 10 half duplex. This setting may cause the BMR restore to run much more slowly than expected. To achieve normal restore performance, manually set the network interface configuration through the firmware before a BMR restore.

To restore an AIX client with media boot

1. Prepare to restore the client using the SRT you created on the bootable media.

   See "Preparing a client for restore" on page 54.

2. Boot the client from the boot media you created. For instructions on how to boot from a CD or from a DVD, see the IBM hardware documentation.
3. Enter the required information at the following BMR process prompts:
   - `Client name` (for a discovery boot, enter the client's name as it appears in the **Tasks** view from the prepare-to-discover operation)
   - `Client IP address`
   - `Network mask`
   - `Default gateway`
   - `NetBackup master server name`
   - `NetBackup master server IP address`
   - `NetBackup master server gateway IP address`

   The restore begins.

Restoring an HP-UX client with media boot

Note: If NetBackup access management is used in your environment, you must provide the appropriate credentials when prompted so that NetBackup can restore the client files.

To media boot an HP-UX client, do the following.

To restore an HP-UX client with media boot

1. Prepare to restore the client using the SRT you created on the bootable media.

   See "Preparing a client for restore" on page 54.

2. Insert the bootable CD or bootable DVD into the CD-ROM drive.
3. Turn off the client, then turn on.
4. When you are prompted, press the **Space** bar to stop the normal boot process.
5. Search for the location and name of the CD-ROM drive.

   The `search` utility may be useful to determine this information.

6 Find the CD-ROM drive from the list of devices and boot the computer using that device with the `boot` command.

7 In response to the `Interact with IPL` prompt, type `No`.

8 In response to the `Run a Recovery Shell` prompt, type `Yes`.

9 In response to the `Start Networking` prompt, type `Yes`.

10 In response to the `Choose the Network Interface` prompt, type the default LAN device to boot from.

You must enter the default LAN because the firmware uses this address for booting from the Ignite server. Note that any network interface card can be used for accessing the SRT or backups, but the default LAN must be used for booting.

11 Enter the following information when prompted:

- `Hostname`
- `IP address`
- `Default gateway`
- `Subnet mask`

12 At the `Is this network information temporary` prompt, type `No`.

13 Use the arrow key to scroll to `OK` and press **Enter**.

14 Enter the required information at the following BMR process prompts:

- `Client name` (for a discovery boot, enter the client's name as it appears in the **Tasks** view from the prepare-to-discover operation)
- `NetBackup master server name`
- `NetBackup master server IP address`
- `NetBackup master server gateway IP address`

The restore begins.

Restoring a Linux client with media boot

Note: If NetBackup access management is used in your environment, you must provide the appropriate credentials when prompted so that NetBackup can restore the client files.

Use the following procedure for Linux clients.

To restore a Linux client with media boot

1. Prepare to restore the client using the SRT you created on the bootable media.

   See "Preparing a client for restore" on page 54.

2. Insert the bootable CD or bootable DVD into the CD-ROM drive.

   On some systems, you may have to modify the BIOS settings so that the system boots from the CD-ROM drive. Consult your hardware documentation for details.

3. Turn off the client, then turn it on.

4. Enter the required information at the following BMR process prompts:

   - `Client name` (for a discovery boot, enter the client's name as it appears in the **Tasks** view from the prepare-to-discover operation)
   - `Client IP address`
   - `Network mask`
   - `Default gateway`
   - `NetBackup master server name`
   - `NetBackup master server IP address`
   - `NetBackup master server gateway IP address`
   - `Additional gateway address to reach the NetBackup master server`

   The restore begins.

Restoring a Solaris client with media boot

Note: If NetBackup access management is used in your environment, you must provide the appropriate credentials when prompted so that NetBackup can restore the client files.

Use the following procedure for Solaris clients.

To restore a Solaris client with media boot

1. Prepare to restore the client using the SRT you created on the bootable media.

   See "Preparing a client for restore" on page 54.

2. Insert the bootable CD or bootable DVD into the CD-ROM drive.

3. Turn off the client, then turn on.

4 Terminate the boot process using the **Stop**+**A** key combination.

5 If the PROM monitor prompt displays <, use the `N` command to reach the `OK` prompt.

6 Enter the following command:

```
boot cdrom
```

The Solaris OS Installation prompts you for network identification.

7 Enter the network identification.

8 Enter the required information at the following BMR process prompts:

- `Client name` (for a discovery boot, enter the client's name as it appears in the **Tasks** view from the prepare-to-discover operation)
- `NetBackup master server name`
- `NetBackup master server IP address`
- `NetBackup master server gateway IP address`

After you enter the required information, the restore begins.

Restoring a Windows client with media boot

Note: If NetBackup access management is used in your environment, you must provide the appropriate credentials when prompted so that NetBackup can restore the client files.

To media boot a Windows client, do the following.

To restore a Windows client with media boot

1 Prepare to restore the client.

See "Preparing a client for restore" on page 54.

2 Create a bootable CD or bootable DVD from the SRT used during the Prepare to Restore.

3 Insert the bootable CD or bootable DVD into the CD-ROM drive.

On some systems, you may have to modify the BIOS settings so that the system boots from the CD-ROM drive. Consult your hardware documentation for details.

4 Turn off the client, then turn it on.

The following message appears:

```
press any key to boot from CD
```

5 The system boot and the restore begin with no further intervention required.

About restoring to a specific point in time

When NetBackup backs up a BMR client, it also backs up the currently saved configuration, and that configuration contains the information about the client on that specific date and time. So you can restore to any point in time for which you have a backup for a BMR client.

For a point in time restore, you must create a restore configuration and specify the point in time to which you want to restore.

About the point in time restore process

Normally, BMR restores from the most recent backup. In a point in time restore, BMR can restore the system to a state earlier than the last full backup.

To restore the system to a previous point in time, you select the point in time for the restore when you create a restore configuration.

A point in time restore is useful when a recent software change has rendered the system unusable. Bare Metal Restore can restore the system to a previous known working state.

Use the point in time restore feature in the following scenarios:

- A hardware change has destabilized the system. There may be cases in which the software that is associated with the hardware cannot be removed completely. Instead of removing all the associated drivers and software, point in time restore can recover the system to a known working state.
- A software addition has destabilized the system. Rather than uninstalling the software, which may not return the system to its state before the software was installed, point in time restore can recover the system.
- A virus attacked the system.
- Critical system or application files were deleted.

Creating a point in time restore configuration

The following procedure creates the restore configuration for a point in time restore for any client type. Then follow the standard restore procedures for the client.

To create a point in time restore configuration

1. In the NetBackup Administration Console, expand **Bare Metal Restore Management > Hosts > Bare Metal Restore Clients**.
2. In the **All Bare Metal Restore Clients** pane, right-click the saved configuration for the client (the configuration labeled current), then select **New** from the shortcut menu.
3. In the **New Configuration** dialog box, enter a name for the new configuration.
4. Click **Retrieve from NetBackup**.
5. Select the **Policy** and **End Date** for the restore.

   If the backup policy uses multiple data streams to back up the client, all of the data streams for each backup job are shown in the **End Date** drop-down list. Select the most recent stream of the backup job on the date to which you want to restore. Normally backup jobs occur on separate days and data streams within the same backup job are separated by seconds or minutes.
6. Click **OK**.

   The new configuration appears in the list of the client's configurations. The configuration is now ready for the prepare-to-restore operation.
7. Restore the client.

   See "About restoring BMR clients using network boot" on page 60.

   See "About restoring BMR clients using media boot" on page 66.

About restoring to dissimilar disks

You can restore a protected client even if the disk drives were replaced. You also can perform a dissimilar disk restore (DDR) if you need to change the volume layout or restore only some of the disks.

About the dissimilar disk restore process

In a standard restore, BMR uses the current client configuration to recreate the original system. Little or no intervention is required because the original system is moved onto the original disk configuration.

In a dissimilar disk restore, intervention is required because you have to map the volume configuration from the protected client to the new disks. (Disk refers to a physical disk and volume refers to a logical division of disk space on one or more physical disks.)

Mapping occurs as follows:

- Before the restore. You can create a configuration you can edit (an editable restore configuration) and initialize that configuration with the new disk layouts. Then map the original volume configuration to the new disks. After you finish mapping, you restore the client using the restore configuration.

  This method requires a record in BMR of the following:

  - Layouts of the new disks on the client, which is necessary, for example, when you perform a discovery operation.
  - Whether another protected client has the same disks.

- During the restore. You perform a standard restore and BMR detects that the disks are different. BMR enters DDR mode and creates an editable restore configuration so you can map the disks.

  You map disks as follows:

  - For UNIX and Linux clients, use the BMR disk mapping utility in the NetBackup Administration Console on the master server.
  - For Windows clients, you can map on the client or on the master server using the BMR disk mapping utility in the NetBackup Administration Console.

You should use dissimilar disk restore in the following circumstances:

- A physical disk is replaced.
- The size of one or more disks has decreased and cannot contain the same volume arrangement.
- The location of one or more disks changes.
- The number of disks has decreased and the required volume arrangement cannot be restored.
- You need to change the layout and volumes for the restored system.
- You want to restore only some of the disks in a system.

Warning: Changes in disk locations may prevent a clustered resource from going online after a restore. BMR does not attempt to adjust clustered resource attributes to account for a dissimilar disk restore.

Creating a restore configuration for DDR

Table 6-6 is an overview of the process to create an editable restore configuration and perform disk mapping before you begin the restore.

You do not have to create a DDR configuration before you begin the restore. You can begin a restore and perform disk mapping during the restore itself.

See "Restoring a client to dissimilar disks" on page 75.

Table 6-6 To create a restore configuration

Step	Task	Procedure
Step 1	Discover the configuration of the new disks.	See "Discovering a configuration" on page 173.
Step 2	Create an editable restore configuration by copying the current configuration.	See "Copying a configuration" on page 171.
Step 3	Open the **Change Configuration** dialog box for the restore configuration.	See "Modifying a configuration" on page 174.
Step 4	Initialize the restore configuration with the disk information from the discovered configuration and then map the original volume configuration to the new disks.	See "About Volumes properties" on page 188.
Step 5	After you finish mapping, perform the DDR restore procedure.	See "Restoring a client to dissimilar disks" on page 75.

Restoring a client to dissimilar disks

Table 6-7 is an overview of the process to restore to dissimilar disks. If you did not prepare a restore configuration in advance, BMR creates an editable restore configuration during this process.

Note the following for UNIX and Linux DDR:

- Shared disks in a cluster are marked restricted.
- Unused VxVM disks on Solaris clients are marked restricted and should remain restricted.

- You cannot map Linux LVM volume groups with the physical volumes that were created on top of multi devices with the same configuration. The physical volumes are mapped to either disks or partitions but not to a multi device.

Table 6-7 To perform a dissimilar disk restore

Step	Task	Procedure
Step 1	Prepare to restore the client.	If you prepared a restore configuration in advance, select that configuration during the prepare operation. See "Preparing a client for restore" on page 54.
Step 2	Begin the restore by booting the client using either network boot or media boot.	If you use a configuration where the protected system's volume configuration is already mapped to the new disks, the restore proceeds as a standard restore. No intervention is required. If BMR detects that the disks are different and are not already mapped, BMR enters DDR mode. See "About restoring clients" on page 51.

Table 6-7 To perform a dissimilar disk restore *(continued)*

Step	Task	Procedure
Step 3	Save the editable restore configuration.	Non-editable configuration only. If you use a configuration that cannot be edited, BMR creates an editable restore configuration. It copies the current configuration and prompts you to enter a name for it, as follows: `Current configuration name for restore is 'current'. Please enter the name for a new editable configuration:`
Step 4	Save the discovered configuration.	To obtain the layouts of the new disks, BMR discovers the hardware of the client. BMR prompts you for a name for the discovered configuration, as follows: `Please enter the name for a new discovered configuration:` BMR saves the discovered configuration. Later, you import the disk layouts from this discovered configuration into the restore configuration.

Table 6-7 To perform a dissimilar disk restore *(continued)*

Step	Task	Procedure
Step 5	Open the **Change Configuration** dialog box .	After the discovered configuration is saved, in the NetBackup Administration Console on the master server, open the **Change Configuration** dialog box for the restore configuration. See "Modifying a configuration" on page 174.
Step 6	Initialize the restore configuration.	Initialize the restore configuration with the new disk layout from the discovered configuration. And then map the original volume configuration to the new disks. See "About Volumes properties" on page 188.
Step 7	Prepare to restore and then restore the client, using the edited restore configuration.	See "Preparing a client for restore" on page 54. See "About restoring BMR clients using network boot" on page 60. See "About restoring BMR clients using media boot" on page 66.
Step 8	If the disk mapping in the restore configuration is incomplete, BMR enters DDR mode again so you can continue to map volumes to disks.	See "About Volumes properties" on page 188.

Restoring to a dissimilar Windows system

Microsoft Windows systems only.

Table 6-8 describes the process to restore to a dissimilar system.

If the target system disk(s) are different than the protected system disks, disk and volume mapping (as performed with a dissimilar disk restore) are required.

Table 6-8 Dissimilar system restore overview

Step	Task	Procedure
Step 1	Learn about dissimilar system restore.	See "About dissimilar system restore" on page 79.
Step 2	Discover the configuration of the target system.	See "About discovering the configuration of the new system" on page 80.
Step 3	Create a configuration to use for the restore.	See "Creating an editable DSR configuration" on page 80.
Step 4	Add NIC drivers and the MSD drivers to the restore configuration system.	See "About adding NIC and MSD drivers" on page 81.
Step 5	Change the network interfaces and network identities in the restore configuration.	See "About changing network interfaces" on page 82.
Step 6	Map disks in the restore configuration.	See "About mapping disks in the restore configuration" on page 82.
Step 7	Create boot media.	See "About creating boot media" on page 83.
Step 8	Restore the client.	See "About restoring the client" on page 83.
Step 9	Complete the DSR changes at the first logon to the restored system.	See "Logging on for the first time after system restore" on page 83.

About dissimilar system restore

Microsoft Windows systems only.

A dissimilar system restore (DSR) restores a protected Windows client to a new system that has a different hardware configuration.

Note: Changes in the hardware configuration may prevent clustered resources from going online after a restore. BMR does not attempt to adjust clustered resource attributes to account for a dissimilar system restore.

A DSR is useful in the following situations:

- You change the preferred vendor for a class of systems in your enterprise.
- You migrate an application from older hardware to the newer hardware.
- Your system experiences critical hardware failure and similar hardware is not available for replacement.
- Your disaster recovery provider does not have identical hardware to yours at the disaster recovery site.
- You stage and verify an application at a test site with different hardware from the production site. (You can migrate the application from test to production.)

Use DSR when any of the following conditions apply:

- The target system has a disk controller that the protected system does not have.
- The target system has a network card that the protected system does not have.
- The target system requires a different hardware abstraction layer (HAL) or kernel than the protected system.
- The target system has different TCP/IP settings than the protected system has. (Only TCP/IP properties are restored. Other networking properties, such as Internetwork Packet Exchange (IPX), are not restored and must be configured after the restore.)

About discovering the configuration of the new system

The first step in restoring to dissimilar hardware is to discover the hardware that is contained on the new system.

See "Discovering a configuration" on page 173.

Creating an editable DSR configuration

You must create a configuration to use for the restore of the protected client. The following table lists the step to creating the configuration.

Table 6-9 Process for creating an editable DSR configuration

Step	Action	Related topic
Step 1	Create the DSR configuration by copying an existing configuration of the protected client. For example, to restore client `protected` to system `target`, create a configuration named `dsr_to_target` by copying the current configuration of client `protected`.	See "Copying a configuration" on page 171.
Step 2	After you create the DSR configuration, open the **Change Configuration** dialog box to modify the configuration as described in the following sections.	See "Client configuration properties" on page 176.

About adding NIC and MSD drivers

The DSR configuration must include the NIC drivers and the MSD drivers that the target system requires.

The target system drivers were added to the packages pool when you performed one of the procedures to discover configurations.

See "Discovering a configuration" on page 173.

The drivers are available to add to the DSR configuration.

To add drivers, select them in the **Available drivers** window of the configuration's **Drivers** dialog box. Then add them to the **Drivers to be used during restore** window.

See "Devices and drivers properties" on page 178.

If you added the drivers to the packages pool using the following methods, the driver description includes the name of the target system:

- By saving the target system's configuration
- By extracting the drivers from the target system

The driver description helps identify which drivers are required for the target system. Also, remove any drivers from the DSR configuration that the protected system uses and the target system does not.

Note: Only TCP/IP properties are restored. Other networking properties, such as Internetwork Packet Exchange (IPX), are not restored and must be configured after the restore.

About changing network interfaces

You must change the network interfaces and network identities in the DSR configuration.

For the changes to work properly you must back up the target system in compliance with the procedures that are part of discovering a configuration.

See "Discovering a configuration" on page 173.

If you installed the client on the target system and backed it up in compliance with the procedures above, you can do the following:

- Import the NIC information from that configuration.
- Map the network identifiers (IP address, netmask, and domain name) from the protected client to the NICs in the target system.

If you did not save the target system's configuration, you must determine the MAC addresses of the NICs in the target system. Then add the network interface information manually to the DSR configuration.

More information is available on procedures to import and map interfaces or change them manually.

See "Network interfaces properties" on page 182.

About mapping disks in the restore configuration

A dissimilar system restore may also be a dissimilar disk restore. If the target system has different disks than the protected client, you must map the volume configuration from the original system to the new disks. (You map as in a dissimilar disk restore.) You can also shrink or extend the size of the system partition or volume. You do not have to map the vendor partition (if one exists) from the protected client to the target system's disks.

For the changes to work properly, you must back up the target system in compliance with the procedures that are part of discovering a configuration.

See "Discovering a configuration" on page 173.

If you installed the client on the target system and backed it up in compliance with the procedures above, you can do the following:

- Import the disk layouts from that configuration.

- Map disks before the restore.

Symantec recommends that you map disks before the restore, especially when the protected client's system partition cannot fit on the target system's system disk.

If you did not save the target system's configuration, you must do the DDR mapping during the restore.

More information is available about dissimilar disk restore.

See "About restoring to dissimilar disks" on page 73.

About creating boot media

If you use media to start the target system, create that media if it is not available already.

See "About boot media" on page 157.

About restoring the client

Prepare to restore the client and initiate the dissimilar system restore process using the DSR configuration.

See "About restoring BMR clients using network boot" on page 60.

See "About restoring BMR clients using media boot" on page 66.

Logging on for the first time after system restore

After the system is restored, a local administrator logon is required to complete the DSR changes. The `bmrcleanup` utility runs and displays a status box that describes the actions being performed.

While the status box is visible, Windows may display a number of New Hardware Found Wizards.

To logon for the first time after system restore

- Perform the following action, depending on which wizard or message screen appears:
  - In the **Digital Signature Not Found** panel, click **Yes** or **Continue**.
  - In the **Found New Hardware Wizard** panel, click **Cancel**.
  - In the **New drivers are installed, do you want to reboot?** panel, click **No**.

Note: Do not reboot the system until the `bmrcleanup` status box completes.

Note: Windows XP and Windows Server 2003 systems may require a product activation after a DSR.

About restoring NetBackup media servers

You can restore NetBackup media servers if they are protected as BMR clients (exception: you cannot restore a media server that is co-located with a NetBackup master server).

The following options exist for restoring NetBackup media servers:

- If you back up a media server to a different media server, restore the protected media server as you restore any protected client.
  See "About restoring BMR clients using network boot" on page 60.
  See "About restoring BMR clients using media boot" on page 66.
- A media server can back up its own data using SCSI-attached storage devices or SAN-attached storage devices. If this true for you, use BMR to restore the media server by first configuring NetBackup to use an alternate media server.

More information is available.

See "About configuring an alternate media server" on page 84.

See "Restoring the media server" on page 86.

About configuring an alternate media server

Two methods exist to configure an alternate media server in NetBackup.

You must do one of the following:

- Configure the automatic media server failover. This method redirects the restore only if the media server is not available. This method is most useful if the library that contains the media is connected both to the failed media server and the alternate media server. Normally, you configure automatic media server failover before the failure, which results in less time and effort during the restore.
- Override the original media server manually. This method forces restores to the alternate server, regardless of the state of the original media server.

  This method is most useful in the following situation:

  - You did not configure automatic media server failover before the failure.

- You want to perform a temporary media server reassignment to restore the original media server.

All backup and restore requests (not only BMR restores) are directed to the alternate media servers.

More information is available.

See "Overriding the original media server manually" on page 85.

See "Enabling automatic media server failover to an alternate server" on page 85.

More detailed information about how to configure NetBackup to use an alternate media server is available.

See the *NetBackup Administrator's Guide for UNIX and Linux, Volume I* or the *NetBackup Administrator's Guide for Windows, Volume I*.

Enabling automatic media server failover to an alternate server

Normally, automatic media server failover is configured before the original media server fails.

On UNIX and Linux systems, when you configure this option, it sets the `FAILOVER_RESTORE_MEDIA_SERVERS` parameter in the `bp.conf` file.

To enable automatic failover to an alternate server

1. In the NetBackup Administration Console, open the **Restore Failover** host properties for the master server.
2. Add an entry in the **Alternate Restore Failover Machines** list; name the media server and failover restore server(s).
3. Stop and restart the NetBackup Request Manager daemon or service on the master server.

Overriding the original media server manually

If necessary, before you physically override the media server, move the media to a library that is attached to the new media server. Then update the Enterprise Media Manager database to reflect the move.

After you perform the restore, reverse the NetBackup configuration changes by removing the alternate server entry from the **Media Host Override** list. The original server performs the NetBackup and restore requests again.

On UNIX and Linux systems, when you configure this option, it sets the `FORCE_RESTORE_MEDIA_SERVER` parameter in the `bp.conf` file.

To override the original server for restores manually

1. In the NetBackup Administration Console, open the **General Server** host properties for the master server.
2. Add an entry in the **Media Host Override** list; name the original backup server and the restore server.
3. Click **OK**.
4. Stop and restart the NetBackup REquest Manager daemon or service on the master server.

Restoring the media server

If you configured the alternate media server before the media server failed (which is most likely with the automatic failover method), the alternate media server is saved as a host in the original media server's BMR client configuration. Now you can perform a standard restore.

If you did not configure the NetBackup alternate media server before the failure, create and modify a restore configuration to use during the restore.

Table 6-10 Restore media server process

Step	Task	Procedure
Step 1	Create a restore configuration.	See "Copying a configuration" on page 171.
Step 2	Add the alternate media server as a host.	See "Modifying a configuration" on page 174. See "Hosts properties" on page 181.
Step 3	After you create and modify the restore configuration, perform a standard restore.	See "About restoring BMR clients using network boot" on page 60. See "About restoring BMR clients using media boot" on page 66.

About restoring BMR boot servers

You can restore BMR boot servers if you protect them as BMR clients. First, back them up. Then use a shared resource tree on another boot server that contains the resources to rebuild the protected boot server.

If a boot server is installed on the same system as the NetBackup master server, you cannot protect it as a BMR client. You can recover the NetBackup catalogs

(which include the BMR databases) on the NetBackup master server. However, you must reinstall the NetBackup and BMR software on the master server.

For more information, see the disaster recovery procedures in the *NetBackup Troubleshooting Guide*.

About external procedures

External procedures are the scripts that interact with the restore process during user exits. Using external procedures, you can minimize the interaction that is required for restores that are not automatic.

The following are the external procedure types:

- Client-specific for a specific client
- Operating system specific for all clients of that operating system type

Client-specific procedures take precedence over operating system procedures.

External procedures are started only if you do one of the following:

- Select **Run External Procedures** on the **Prepare to Restore Client or Prepare to Discover** dialog box.
- Specify external procedures by using the `bmrprep -runep` command.

External procedures operate in the restore environment (a limited operating system environment during the restore process). Many of the commands and capabilities that are available with a complete operating system are not available in the restore environment.

UNIX external procedures execute as root. Windows external procedures execute as administrator.

External procedures are stored in the BMR database on the NetBackup master server. Use the `bmrepadm` command on the master server to manage external procedures.

Note: Using external procedures requires a general knowledge of scripts.

External procedure points and names

BMR can run external procedures at the following user exit points during the restore process, in the following sequence:

`prediscover`	Before discovery of hardware is reported to the BMR server (UNIX clients only).

`preformat`	Before disks are formatted and partitioned. On Windows systems, the preformat takes place after the system drive is formatted but before any nonsystem drives are formatted.
`prerestore`	Before files begin to restore.
`postrestore`	After files are restored.
`first boot`	After the restore is complete and at the first boot of a restored client. On Windows systems, the first boot external procedure operates as the first user to log on after a client is restored.

An external procedure point name is used as part of the name of each external procedure script that you create. The naming convention for client-specific external procedures is different than for operating system-specific external procedures.

Note: Do not add a `.cmd` extension for the external procedures that are intended for Microsoft Windows systems. BMR adds the appropriate file name extension when it generates the scripts during the prepare-to-restore process.

Client-specific external procedure names	Client-specific external procedure names are in the following format: *`clientname_externalprocedure`* For example, the `sol123_prerestore` external procedure is started before files are restored on client `sol123`. (The procedure starts if Run External Procedures is specified during restoration.)

Operating system-specific external procedures names	Operating system-specific external procedure names are in the following format: `externalprocedure.ostype` The *ostype* is one of the following: ■ `aix` ■ `hp` HP-UX systems ■ `linux` Linux systems ■ `sol` Solaris systems ■ `win` Windows systems For example, the `preformat.linux` external procedure is started on Linux clients before drives are formatted. (The procedure starts if Run External Procedures is specified during restoration.)

About managing external procedures

Use the `bmrepadm` command to do the following:

- Add an external procedure so it is available during a restore.
- Delete an external procedure from the database.
- Extract an existing procedure from the database.
- List all the external procedures in the database.

For example, to add a prerestore external procedure for a client named sol123, use this command on the NetBackup master server with a BMR license:

```
bmrepadm -add sol123_prerestore
```

The `bmrepadm` command does not validate client names (that is, you can add an external procedure for a nonexistent client).

For another example, to add an external procedure auxiliary file named `ListStorageGroups.vbs`, use the following command:

```
bmrepadm -add -data ListStorageGroups.vbs
```

For more information about the `bmrepadm` command, see *NetBackup Commands*.

Specifying external procedures

You must specify during the prepare-to-restore operation that you want to run external procedures. The BMR master server then creates the appropriate external procedure scripts and uses them during the restore.

Note: External procedures should be in the BMR database before the prepare-to-restore or prepare-to-discover operation is started.

To specify external procedures

- Select **Run External Procedures** in a **Prepare To Discover** or **Prepare to Restore Client** dialog box.

  See "Discovering a configuration" on page 173.

  See "Preparing a client for restore" on page 54.

  Alternatively, use the `bmrprep` command `-runep` option to specify external procedures.

About external procedure data transfer

You can use the `bmrc` command to transfer files from the BMR master server to a client during a restore.

On UNIX systems, store data in the `/tmp` file system or in the file systems that are mounted under `/tmp`. All other file systems are read only during a restore.

On Windows systems, transferred files are stored in the current directory by default. The directory is `%SystemDrive%\` during restore. The directory is `%HOMEPATH%` during the first boot procedure. You can specify other path names or file names on the command line.

The following is an example of using the `bmrc` command to transfer a file from the master server to the client:

```
bmrc -operation pull -resource procedure -client clientName -source
file_on_server -destination /tmp/filename
```

When you start the `bmrc` command in an external procedure, specify the full path in the restore environment, as follows:

- On UNIX and Linux clients: `/usr/openv/NetBackup/bin`
- On Microsoft Windows clients: `%SystemDrive%\BMR\NBU\bin`
  At the first boot external procedure point, the path to the `bmrc` command is *`install_path`*`\NetBackup\bin` on Microsoft Windows clients.

For more information about the bmrc command, see *NetBackup Commands*.

About interaction with external procedures

UNIX and Linux systems

You can enter commands and interact with an external procedure during restore time. To do so, start the bmrShell function from within the external procedure script. The bmrShell function allows input from the default console keyboard and outputs to the console monitor.

You can also use redirection to send output to the screen from an external procedure by redirecting output to the special device. To do so, use /dev/console (as in echo "Hello World" >> /dev/console).

On UNIX and Linux systems, the bmrShell is not available during first boot.

Windows systems

You can enter commands and interact with an external procedure during restore time. To do so, start the Windows command interpreter cmd from within the external procedure script.

On Windows systems, the limited restore environment may not contain DLLs or the same version of DLLs that were used with the original client system. Use bmrc to transfer these DLLs during the restore to the C:\BMR\WINNT\SYSTEM32 directory. Alternatively, add the location of that DLL to the path environment variable.

External procedure logging examples

The following logs are created on the BMR master server during the restore process:

/usr/openv/netbackup/logs/bmrrst/*client_name*/log.*mmddyy* (UNIX)
install_path\NetBackup\logs\bmrrst*client_name*\log.*mmddyy* (Windows)

On UNIX and Linux systems, the BMR restore process writes external procedure begin and end messages to the logs. (On Windows systems, the BMR restore process does not perform begin and end logging.) You can use the bmrc command in your external procedure scripts to write messages to the logs also.

External procedures write messages when they start and finish. A message includes the date and time that the procedure began, the client name, and a description that includes the external procedure name. See the following examples:

```
2005/08/02 12:10:38.180 w2k200,sol157 INFO: Executing External
Procedure: sol123,sol123_prerestore.
2005/08/02 12:10:38.350 w2k200,sol157 INFO: Completed executing
External Procedure: sol123,sol123_prerestore.
```

You can use the bmrc command to write messages to the restore log. The following is an example of a bmrc command that writes a message during a restore of client sol123:

```
bmrc -operation create -resource message -client sol123 -msg "
message text to log"
```

Alternatively, you can pipe data to the bmrc command, as in the following example:

```
echo "Hello World" | bmrc -operation create -resource log -client sol123
```

The following is the log entry from the previous command:

```
Restoration log start time: 2005/03/28 10:59:27
Hello World.
Restoration log end time: 2005/03/28 10:59:27
```

When you start the bmrc command in an external procedure, specify the full path in the restore environment, as follows:

- On UNIX and Linux clients: /usr/openv/netbackup/bin
- On Microsoft Windows clients: %SystemDrive%\BMR\NBU\bin
  At the first boot external procedure point, the path to the bmrc command is *install_path*\NetBackup\bin on Microsoft Windows clients.

For more information about the bmrc command, see *NetBackup Commands*.

External procedure operational states

During the operation of an external procedure, the following operational states appear in the **Tasks** view:

Discovery External Procedure	An external procedure runs during the prediscovery phase.
First Boot External Procedure	An external procedure runs during the first boot phase.
Post-restore External Procedure	An external procedure runs during the postrestore phase.
Pre-format External Procedure	An external procedure runs during the preformat phase.
Pre-restore External Procedure	An external procedure runs during the prerestore phase.

About external procedure exit codes

Ensure that external procedures exit with a return code of 0. If an external procedure exits with a non-zero code, the restore pauses for input.

If it is acceptable for an external procedure to fail during the restore (that is, not vital to system functionality), ensure that you exit 0 from the external procedure.

About external procedure error handling

By default, external procedures halt the restore process and await user action if the procedure returns a non-zero return code.

For UNIX and Linux restores, the following menu appears:

```
What do you want to do next? Choices are:
a) Abort the restore.
r) Retry the external procedure again.
I) Ignore the error and continue the restore.
s) Escape to shell prompt, return here when done.
```

If you retry, a prompt asks if you want to transfer the external procedure again from the BMR server before you run it. The prompt lets you edit the external procedure on the master server before you run it again.

Note: When a UNIX first boot external procedure is started with no terminal defined and the procedure returns non-zero, the Bare Metal Restore process ends.

For Windows restores, a dialog box appears with the following choices:

- **Cancel** halts the restore.
- **Try Again** starts the external procedure again.
- **Continue** ignores the error and continues with the restore.

If you try again, a prompts asks if you want to transfer the external procedure again from the BMR server before you run it. The prompt lets you edit the external procedure on the master server before you run it again.

About external procedure environment variables

BMR sets and exports certain environment variables during the restore process. Some are general environment variables; others are specific to BMR.

UNIX and Linux environment variables

The following environment variables are exported on all UNIX and Linux systems:

Table 6-11 UNIX and Linux environment variables

Variable	Description
$BMRC	Path name to the bmrc executable file (/usr/openv/NetBackup/bin/bmrc)
$bootServerAddress	Boot server IP address
$clAddress	The IP address of the client
$clAddressHex	Client IP address that is converted to hex
$client_firstboot	Name of client-specific, first boot external procedure
$client_postrestore	Name of client-specific, post-restore external procedure
$client_prediscover	Name of client-specific discover external procedure
$client_preformat	Name of client-specific preformat external procedure
$client_prerestore	Name of client-specific prerestore external procedure
$clName	The name of the client.
$clOs	BMR abbreviated OS specification
$configName	The name of the configuration
$default_firstboot	Name of OS default first boot external procedure
$default_postrestore	Name of OS default postrestore external procedure
$default_prediscover	Name of OS default prediscover external procedure
$default_preformat	Name of OS default preformat external procedure
$default_prerestore	Name of OS default prerestore external procedure
$defaultGateway	The name of the default gateway

Table 6-11 UNIX and Linux environment variables *(continued)*

Variable	Description
$extProcName	Current external procedure name
$importNonRootVgs	Import nonsystem volume and disk groups
$logging	Log restore; yes=yes, no=no
$newConfig	Name of the configuration to discover
$onEpError	Restore behavior on External Procedure Error: 0=cancel 1=prompt 2=ignore
$runEp	Start external procedures if found 0=no, 1=yes
$runMode	Mode of BMR process discover or restore
$serverAddress	NetBackup server IP address
$serverGateway	Gateway to the NetBackup server
$serverName	NetBackup server name

AIX environment variables

$BMR_BOSINST_DATA $MNT
$RC_CONFIG $ROUTES

The following exported operating system environment variables are set at restore:

$BIDATA $HOME
$LIBPATH $NIM_HOSTNAME
$NIM_HOSTS $NIM_NAME
$NSORDER $ODMDIR
$PATH $PWD
$SHOWLED $SPOT
$SYSCFG_PHASE

HP-UX environment variables

The following exported operating system environment variables are set at restore:

```
$DEFAULT_RELEASE_DIR          $EDITOR
$ENV                          $ERRNO
$FCEDIT                       $HISTFILE
$HOME                         $IFS
$INST_CLIENT_DIR              $INST_CUR_PRIMARY_PATH
$INST_IS_BOOTP_SYSTEM         $INST_LOG_FILE
$INST_NOT_TEST_MODE           $LINENO
$MAILCHECK                    $OPTARG
$OPTIND                       $PATH
$PPID                         $PS1
$PS2                          $PS3
$PS4                          $PWD
$RANDOM                       $SECONDS
$SHELL                        $SOURCE
$SOURCE_LIF_FILE              $SOURCE_NET_DIR
$SOURCE_TYPE                  $TMOUT
```

Solaris environment variables

The following exported operating system environment variables are set at restore:

```
$IFS                          $MAILCHECK
$OPTIND                       $PATH
$PS1                          $PS2
$PWD                          $TZ
$_DVFS_RECONFIG
```

Windows environment variables

CMD is used to start the Windows command-line interpreter during restore.

The following exported operating system environment variables are available during the restore:

```
%ALLUSERSPROFILE%             %APPDATA%
%CommonProgramFiles%          %COMPUTERNAME%
%ComSpec%                     %HOMEDRIVE%
```

About storage area network support

Bare Metal Restore can restore a system that is attached to a Storage Area Network (SAN). On Windows, AIX, Linux, and Solaris systems, if the host bus adapter (HBA) drivers are available, BMR automatically restores the SAN-attached volumes. On HP-UX systems, BMR only restores the volumes that are not on the SAN.

See "Restoring Solaris SAN-attached volumes if they are left unmapped" on page 97.

See "About SANs and dissimilar system restores on Windows clients" on page 97.

Restoring Solaris SAN-attached volumes if they are left unmapped

The following information applies only to Solaris clients.

After a Solaris system is recovered using the dissimilar disk restore feature, you may need to perform the following procedure for SAN-attached volumes that were left unmapped (marked not to restore).

To restore Solaris SAN-attached volumes if they are left unmapped

1. Determine the differences between the current and previous `vfstab` files:

   ```
   % diff /etc/vfstab /etc/vfstab.old.bmr.dmr
   ```

2. Review the differences.
3. Copy the entries about the SAN devices from the `/etc/vfstab.old.bmr.dmr` file. Add them to the `/etc/vfstab` file or uncomment the corresponding lines that are commented out when `vfstab` was merged.
4. Mount the file systems that are on the SAN.
5. Manually restore the SAN file systems using the NetBackup Backup, Archive, and Restore interface.

About SANs and dissimilar system restores on Windows clients

The following information applies only to Windows clients.

If you perform a dissimilar system restore on Windows and you want to restore to a SAN disk, you must do the following:

- Add the HBA drivers to the restore configuration. The HBA drivers can be added the same way as any other mass storage device driver.
- Reconfigure your SAN so that the HBA in the target system sees the same devices as the HBA that existed in the source system.

More information is available on adding drivers.

See "About adding NIC and MSD drivers" on page 81.

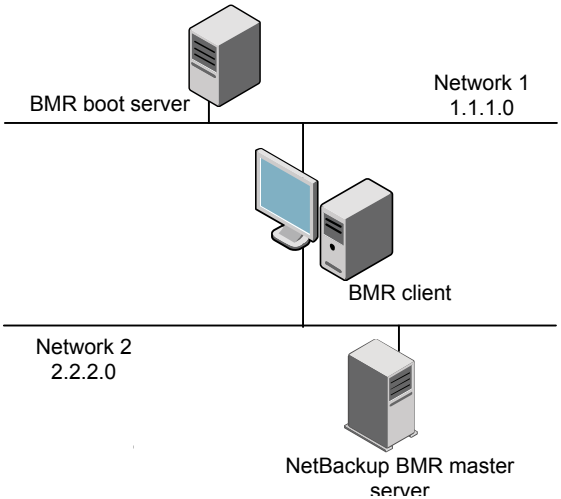
About multiple network interface support

BMR recovery occurs in two major stages: boot stage and restore files stage. The boot stage uses a single network interface to talk to the BMR boot server. Once the restore environment is loaded from the boot server, BMR configures and activates all network interfaces for the restore files stage.

Note: Systems with multiple network interfaces are also known as multihomed systems. BMR fully support multihomed clients.

Figure 6-3 illustrates a configuration that can occur with multihomed clients. For this configuration, specify the network interface for Network 1 when you network boot the client.

Figure 6-3 Simple multihomed example



About client configuration using gateways

BMR clients can use gateways to communicate with BMR and NetBackup servers during a restore operation.

Table 6-12 describes gateway attributes that are used during a restore.

Table 6-12 Network gateways

Gateway	Description
Default Gateway	Defines the default network gateway for the client during the restore.
Master Server Gateway	Defines the gateway from the client to the NetBackup master server.
Media Server Gateway	Defines the gateway from the client to the NetBackup media server used to restore the files.

You may not have to specify all gateways. If the client can communicate with all hosts through the default gateway, you only have to specify the default gateway.

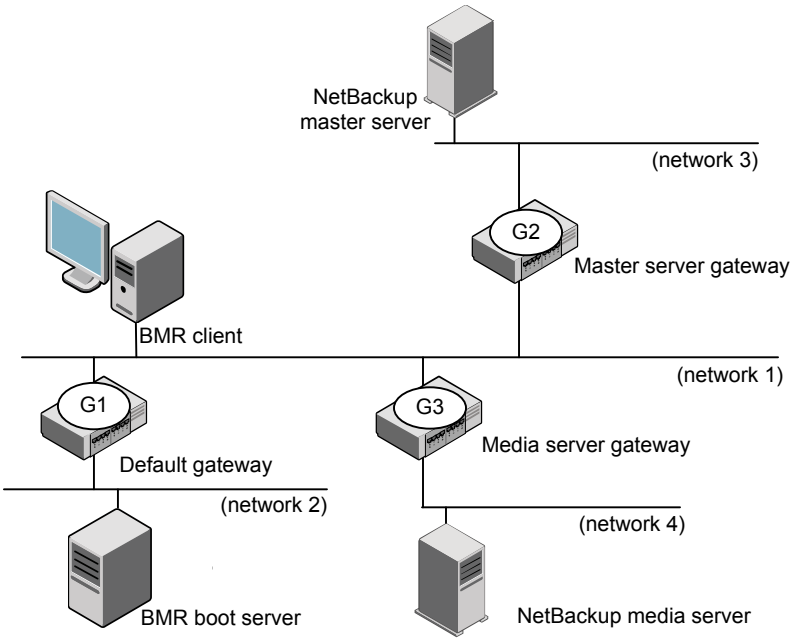
For network boots, specify the following:

- The gateways for the NetBackup master and media servers in the **Hosts** dialog box of the restore configuration
- The default gateway in the **Network Routes** dialog box

For media boots, you are prompted for these values when you create the boot media or during the restore.

Figure 6-4 shows how gateways can be used during a BMR client restore.

Figure 6-4 Gateway example



The client in this diagram cannot communicate with all of the servers it needs to by using only the default gateway. For such a configuration, you should specify the default gateway as G1, the master server gateway as G2, and the media server gateway as G3.

Port usage during restores

During restores, clients communicate with BMR boot servers through specific services and ports. If the boot server is behind a firewall, communication between the client server and boot server must be allowed through these ports.

Table 6-13 lists the ports and services that are used during restores.

Table 6-13 Port usage during restores

Service	Port	UNIX	Linux	Windows
`bootp/DHCP`	67, 68	X	X	X
`ping`			X	
`lockd`	Unreserved	X	X	

Table 6-13 Port usage during restores *(continued)*

Service	Port	UNIX	Linux	Windows
`mountd`	Unreserved	X	X	
`nfsd`	2049	X	X	
`portmapper`	111	X	X	
`rpcbind`		X (for `bootparam` on Solaris only)		
`statd`	Unreserved	X	X	
`tftp`	69	X	X	X
`vnetd`	13724	X	X	X
`bpcd`	13782	X	X	X
Windows File Sharing	445			X

Chapter 7

Managing shared resource trees

This chapter includes the following topics:

About shared resource trees

A shared resource tree (SRT) is a collection of the following:

- Operating system files

- NetBackup client software
- Programs that format drives, create partitions, rebuild file systems, and restore the original files using the NetBackup client software

An SRT also provides the resources that are needed to boot the client system and begin the restore process.

The software in an SRT is not installed permanently on the protected system. Its purpose is to bring the protected system to a state from which the original files can be restored.

Note the following:

- For UNIX and Linux systems: Each client type and operating system version requires its own SRT. For example, Solaris 9 requires a Solaris 9 SRT, AIX 5.3 requires an AIX 5.3 SRT, and so on.
- For Windows systems: A single SRT can restore all Windows versions.

For UNIX and Linux systems, you create SRTs on boot servers of the same operating system. The boot server must run the same version or a later version of the operating system that is installed in the SRT. For example, a Solaris 9 SRT must reside on a Solaris 9 or later boot server. For Windows systems, any version of Windows can host the SRT.

For more information about supported operating systems for clients, SRTs, and boot servers, see the *NetBackup Release Notes*.

During a restore, a client accesses the SRT from a boot server over a network, or on a CD or DVD. Although SRTs reside on boot servers, you can copy an SRT to CD media or DVD media, boot the client from that media, then access the SRT on that media.

Depending on the operating system for which an SRT is created, the SRT requires 100 MB to 600 MB of disk space.

For more information about disk space requirements, see the *NetBackup Release Notes*.

About the space requirements for SRTs

This section lists the approximate space requirements of the specific SRTs with respect to various platforms and setups.

Table 7-1 lists the approximate space requirements of SRTs.

Table 7-1 Space requirements of SRTs

Operating system	NetBackup version	SRT size without VxVM(Approximate)	SRT size with VxVM(Approximate)	SRT size without SFW(Approximate)	SRT size for legacy / legacy with SFW(Approximate)
Windows 2000 32-bit	7.5	Not applicable	Not applicable	163 MB	680 MB / 800 MB
Windows 2000 64-bit	7.5	Not applicable	Not applicable	191 MB	780 MB / 923 MB
Windows 2008 32-bit	7.5	Not applicable	Not applicable	163 MB	1150 MB / 1350 MB
Windows 2008 64-bit	7.5	Not applicable	Not applicable	191 MB	1200 MB / 1350 MB
Windows 2008 R2	7.5	Not applicable	Not applicable	191 MB	1310 MB / 1450 MB
RHEL 5	7.5	400 MB	Not applicable	Not applicable	Not applicable
RHEL 6	7.5	420 MB	Not applicable	Not applicable	Not applicable
SLES10	7.5	375 MB	Not applicable	Not applicable	Not applicable
SLES11	7.5	375 MB	Not applicable	Not applicable	Not applicable
Solaris 64-bit	7.5	500 MB	1 GB	Not applicable	Not applicable
Solaris Sparc	7.5	500 MB	1 GB	Not applicable	Not applicable
AIX 7.1	7.5	2.1 GB	2.2 GB	Not applicable	Not applicable
AIX 6.1 TL6 SP1	7.5	2.5 GB	2.6 GB	Not applicable	Not applicable
AIX 5.3 TL12	7.5	2 GB	2.1 GB	Not applicable	Not applicable
HPUX 11.11	7.1	750 MB	800 MB	Not applicable	Not applicable
HPUX 11.31	7.5	2.93 GB	3.9 GB	Not applicable	Not applicable

About creating a shared resource tree

A shared resource tree must be created on a local file system of the boot server. BMR sets permissions for the SRT directory to allow read access to all and read and write access to the root or Administrator user.

When you create an SRT, you install the operating system software and NetBackup client software into the SRT. You also can install other software when you create the SRT or at any time thereafter.

To create an SRT, you need the installation software or images for the following items:

- Operating system (UNIX and Linux only).
- For Linux SRTs, the Bare Metal Restore third-party products CD. This CD contains the open source products that may not be included in the vendor Linux distribution.
- Optional: Other applications or packages (such as Veritas Volume Manager or Veritas File System).
- Optional: Patches, maintenance levels, Maintenance Packs, service packs, fileset, or the drivers that the operating system requires or other software that is installed in the SRT. You must install into the SRT any operating system patches that the NetBackup client software requires. If they are not installed, NetBackup does not function correctly in the temporary restore environment, and the restore may fail.

  For more information about package or patch dependencies, see the *NetBackup Release Notes*.

If you need more than one SRT of the same operating system, create an SRT with only the operating system and NetBackup client software. (For example, you want to restore the clients that have different versions of Veritas Volume Manager or different drivers.) Then make as many copies as you need and add the different versions of the other software to the copies. If you copy an existing SRT, it is usually faster than if you create an SRT.

During SRT creation, you are prompted for the path to the installation program or software if you do one of the following:

- Place the installation program in a removable media drive of the boot server. Then provide the path to that removable media drive.
- Copy the contents of the installation program to a local directory. Then provide the path to that local directory.

- Copy the installation program contents to a remote directory, available to the boot server through NFS or network share. Then provide the path to that remote directory or share location.

The amount of time that is needed to create an SRT is between 5 minutes and 60 minutes. It depends on the speed of the system, the operating system of the SRT being created, and other software being installed.

See "Creating an SRT for UNIX or Linux" on page 107.

See "Creating an SRT for Windows" on page 124.

Creating an SRT for UNIX or Linux

Use the `bmrsrtadm` command to create a new SRT.

More information is available about how to copy an SRT to a bootable CD or DVD (create boot media).

See "Creating boot media for UNIX and Linux" on page 160.

To create an SRT for UNIX or Linux

1 On the boot server where you want to create the SRT, change to the following directory:

```
/usr/openv/netbackup/bin
```

2 Enter the following command:

```
./bmrsrtadm
```

3 When you are prompted, select the option to create a new SRT.

Caution: The `bmrsrtadm` command on AIX and HP-UX prompts you to enter the desired architecture (32/64) while you create BMR SRT.

If you want to install NetBackup client of the versions older than 7.0 into SRT, this OS architecture type should to be selected as 32-bit. For NetBackup 7.0, select 64-bit as OS architecture type.

While you install NetBackup client into SRT, `bmrsrtadm` gives the appropriate error message if there is any incompatibility between SRT OS architecture type and NetBackup client version.

4 To continue to create the specific SRT type, see the following:

- See " Creating an AIX SRT" on page 108.
- See "Creating an HP-UX SRT" on page 111.
- See "Creating a Solaris SRT" on page 116.
- See "Creating a Linux SRT" on page 119.

Creating an AIX SRT

When you create an AIX SRT, you are guided through the installation process, as follows:

- The operating system software
- NetBackup client software

To create an AIX SRT

1. On the boot server where you want to create the SRT, change to the following directory:

   ```
   /usr/openv/netbackup/bin
   ```

2. Enter the following command:

   ```
   ./bmrsrtadm
   ```

3 When you are prompted, select the option to create a new SRT.

Caution: The `bmrsrtadm` command on AIX and HP-UX prompts you to enter the desired architecture (32/64) while create BMR SRT.

If you want to install NetBackup client of the versions older than 7.0 into SRT, this OS architecture type should to be selected as 32-bit. For NetBackup 7.0, select 64-bit as OS architecture type.

While you install NetBackup client into SRT, `bmrsrtadm` gives the appropriate error message if there is any incompatibility between SRT OS architecture type and NetBackup client version.

---

4 Complete the command prompts as indicated in following table.

`Enter the name of the SRT to create`	The name of the SRT also is used for the directory that contains it. Only alphanumeric characters and underscore (_) characters are allowed.
`Enter the description of the new SRT`	A description of the SRT.
`Enter desired OS level of AIX`	Enter the levels you can create based on the operating system version of the boot server.
`Enter desired Architecture(32/64)`	Enter whether 32-bit or 64-bit AIX operating system needs to be installed into SRT. **Note:** This SRT operating system architecture type is not related to the client operating system architecture type. Instead, it is related to NetBackup client software going to be installed into SRT. If you want to install NetBackup client of the versions older than 7.0 into SRT, this OS architecture type should to be selected as 32-bit. For NetBackup 7.0, select 64-bit as OS architecture type. During the NetBackup client installation into SRT step, `bmrsrtadm` gives the appropriate error message if there is any incompatibility between SRT OS architecture type and NetBackup client version.
`Enter the directory in which to place the new SRT`	The path to the directory in which to create the SRT. The root of the SRT (called the SRT path) is the path name to the SRT location, which includes the SRT name. The default is either /export/srt or the directory where an SRT was last created successfully. The directory must already exist.

`Source of AIX install images`	Enter the name of the device where the operating system installation program is inserted or enter the path to the installation image. After you enter the device name or host:/path, the operating system is installed into the SRT.
`Enter the source of the NetBackup install images.` `Specify a device name or an NFS path (host:/path form), or a local directory`	Enter the device name where the NetBackup client software installation program is inserted or enter the path to the installation image. After you enter the device name or path, the NetBackup client installation procedure installs the client software into the SRT.
`Do you want to continue? [y,n] (y)`	Enter **y**.
`Do you want to install the NetBackup client software for this client? [y,n] (y)`	Enter **y**.
`Enter the name of the NetBackup server:`	Enter any non-blank value. The server name is replaced at restore time with the correct values for the BMR client being restored.
`Would you like to use` *`servername`* `as the configured name of the NetBackup client? [y,n] (y)`	Accept the default or enter any non-blank value. The client name is replaced at restore time with the correct values for the BMR client being restored.

After you install the AIX and NetBackup software, the `bmrsrtadm` command provides options to install other software in the SRT. You can either add other software now or quit (you can add software later). During step **NetBackup client installation into SRT** you might get an error message if the operating system architecture type and NetBackupclient version are incompatible.

More information is available about how to add other software.

See "About adding software to a shared resource tree" on page 125.

Creating an HP-UX SRT

When you create an HP-UX SRT, you are guided through the installation process, as follows:

- Ignite software
  If the SRT is to be used to restore PA-RISC2-based clients, use Ignite-UX 5.3*x* or later to create the SRT.
- Operating system software
- NetBackup client software

To create an HP-UX SRT

1. On the boot server where you want to create the SRT, change to the following directory:

   ```
   /usr/openv/netbackup/bin
   ```

2. Enter the following command:

   ```
   ./bmrsrtadm
   ```

3. When you are prompted, select the option to create a new SRT.

   Caution: The `bmrsrtadm` command on AIX and HP-UX prompts you to enter the desired architecture (32/64) while you create BMR SRT.

   If you want to install NetBackup client of the versions older than 7.0 into SRT, this OS architecture type should to be selected as 32-bit. For NetBackup 7.0, select 64-bit as OS architecture type.

   While you install NetBackup client into SRT, `bmrsrtadm` gives the appropriate error message if there is any incompatibility between SRT OS architecture type and NetBackup client version.

   ---

4. Complete the command prompts as indicated in following table.

`Enter the name of the SRT to create`	The name of the SRT also is used for the directory that contains it. Only alphanumeric characters and the underscore (_) character are allowed.
`Enter the description of the new SRT`	A description of the SRT.
`SRT OS level`	The levels you can create based on the operating system version of the boot server.

`Enter desired Architecture(32/64)`	Enter whether 32-bit or 64-bit AIX operating system needs to be installed into SRT. **Note:** This SRT operating system architecture type is not related to the client operating system architecture type. Instead, it is related to NetBackup client software going to be installed into SRT. In case you want to install NetBackup client of the versions older than 7.0 into SRT, this OS architecture type should to be selected as 32 bit. For NetBackup 7.0, select 64-bit as OS architecture type. During the NetBackup client installation into SRT step, `bmrsrtadm` gives the appropriate error message if there is any incompatibility between SRT OS architecture type and NetBackup client version.
`Enter the directory in which to place the new SRT`	The path to the directory in which to create the SRT. The root of the SRT (called the SRT path) is the path name to the SRT location, which includes the SRT name. The default is either /export/srt or the directory where an SRT was last created successfully. The directory must exist.

`Location (device or directory path) of the Ignite install media.`	BMR searches for the following directory (*x.x* is either 11.00 or 11.11): ■ Ignite-UX/FILE-SRV-*x.x*/opt/ignite/data/Rel_B.*x.x*/ (BOSdatapath) If the BOSdatapath directory is found, BMR expects the Ignite installation image to be in one of the following directories. (Note that -PA indicates Ignite version B41.) ■ Ignite-UX/BOOT-KERNEL/opt/ignite/data ■ Ignite-UX/BOOT-KERNEL/opt/ignite/boot ■ Ignite-UX/BOOT-KERNEL-PA/opt/ignite/data ■ Ignite-UX/BOOT-KERNEL-PA/opt/ignite/boot If the BOSdatapath directory is not found, BMR looks for a file named INSTCMDS from the tar file supplied in one the following directories: (Note that -PA indicates Ignite version B41.) ■ Ignite-UX/BOOT-KERNEL/opt/ignite/data ■ Ignite-UX/BOOT-KERNEL-PA/opt/ignite/data If the file is not found, BMR cannot install Ignite.
`Enter the location (device or directory path) of the HP-UX x.x install media`	The variable *x.x* is the SRT operating system version.

`The following patches are required for this SRT: patch_list`
`They can be found on an HP support plus media, or they can be downloaded from HP Web site.`
`Location (device or path) of the media that contains patch_list:`
	If your version of Ignite requires a patch, you are prompted to provide the path to the specific patch that the version requires.

`Location (device or path) of the Symantec NetBackup install media`	Enter the name of the device where the NetBackup client software installation media is inserted or enter the path to the installation image. After you enter the device name or path, the NetBackup client installation procedure installs the client software into the SRT. The following appears when the NetBackup client software installation process begins: Symantec installation script Copyright 1993 - 2007 Symantec Corporation, All Rights Reserved. Installing NetBackup Client Software **Note:** To install NetBackup server software, insert the appropriate NetBackup server CD.
`Do you want to continue? [y,n] (y) y`	Enter `y`.
`Do you want to install the NetBackup client software for this client? [y,n] (y)`	Enter `y`.
`Enter the name of the NetBackup server:`	Enter any non-blank value. The server name is replaced at restore time with the correct values for the BMR client being restored.
`Would you like to use servername as the configured name of the NetBackup client? [y,n] (y)`	Accept the default or enter any nonblank value. The client name is replaced at restore time with the correct values for the BMR client being restored.

After you install the HP-UX and NetBackup software, the `bmrsrtadm` command provides options to install other software in the SRT. You can either add other software now or quit (you can add software later).

More information is available about how to add other software.

See "About adding software to a shared resource tree" on page 125.

Creating a Solaris SRT

When you create a Solaris SRT, you are guided through installing the operating system software.

BMR can create a new SRT from the following:

- The Solaris installation program
- The installation program that copied to a local directory or a remote directory
- The Solaris software that is installed in an existing SRT. Furthermore:

For CD media, use the Software 1 of 2 CD.

If you create a Solaris 9 SRT by using a network shared CD, both slice 0, and slice 1 must be shared.

You may want to consult the following additional information:

- See "About installing patches, packages, and Solaris SRTs" on page 129.

To create a Solaris SRT

1. On the boot server where you want to create the SRT, change to the following directory:

   ```
   /usr/openv/netbackup/bin
   ```

2. Enter the following command:

   ```
   ./bmrsrtadm
   ```

3 When you are prompted, select the option to create a new SRT.

Caution: The `bmrsrtadm` command on AIX and HP-UX prompts you to enter the desired architecture (32/64) while you create BMR SRT.

If you want to install NetBackup client of the versions older than 7.0 into SRT, this OS architecture type should to be selected as 32-bit. For NetBackup 7.0, select 64-bit as OS architecture type.

While you install NetBackup client into SRT, `bmrsrtadm` gives the appropriate error message if there is any incompatibility between SRT OS architecture type and NetBackup client version.

4 Complete the command prompts as indicated in following table.

`Enter the name of the SRT to create`	The name of the SRT also is used for the directory that contains it. Only alphanumeric characters and the underscore (_) character are allowed.
`Enter the description of the new SRT`	A description of the SRT.
`Enter desired level of Solaris/SunOS`	Enter the levels you can create based on the operating system version of the boot server.
`Enter the directory in which to place the new SRT`	The path to the directory in which to create the SRT. The root of the SRT (called the SRT path) is the path name to the SRT location, which includes the SRT name. The default is either /export/srt or the directory where an SRT was last created successfully. The directory must exist.
`Enter a [hostname:/]pathname containing a suitable Solaris` *`x.x`* `Boot CDROM or SRT image`	Enter one of the following: the name of the device where the installation program is inserted, the path to the installation image, or the path to an existing Solaris SRT. After you enter the device name or path, the operating system is installed into the SRT.
`Enter a [hostname:]/ pathname containing NetBackup client software`	Enter the name of the device in which the NetBackup software installation media is inserted or enter the path to the installation program (named `install`). After you enter the device name or path, the NetBackup installation procedure installs the client software into the SRT.

	The following appears when the NetBackup client software installation process begins: Symantec installation script Copyright 2006 Software Corporation, All rights reserved. Installing NetBackup Client Software **Note:** To install NetBackup server software, insert the appropriate NetBackup server CD.
`Do you want to continue? [y,n] (y) y`	Enter `y`.
`Do you want to install the NetBackup client software for this client? [y,n] (y)`	Enter `y`.
`Enter the name of the NetBackup server:`	Enter any nonblank value. The server name is replaced at restore time with the correct values for the BMR client being restored.
`Would you like to use servername as the configured name of the NetBackup client? [y,n] (y)`	Accept the default or enter any nonblank value. The client name is replaced at restore time with the correct values for the BMR client being restored.

After you install the Solaris and NetBackup software, the `bmrsrtadm` command provides options to install other software in the SRT. You can either add other software now or quit (you can always add software later).

More information is available about how to add other software.

See "About adding software to a shared resource tree" on page 125.

Creating a Linux SRT

The first time you create an SRT on a Linux boot server, you are guided through installing the following software:

- The operating system software.
- BMR third-party products, the open source products that may not be included in the vendor Linux distribution. To download a CD image at no charge, see the following:

http://seer.support.veritas.com/docs/275782.htm

- NetBackup client software.

During this process, the `bmrsrtadm` command also copies files from the operating system installation program and BMR third-party installation program to the following directory:

```
/usr/openv/netbackup/baremetal/server/data/media
```

Each time thereafter that you create an SRT on that boot server, `bmrsrtadm` uses those installation files. You do not have to enter the path to the installation program or images. If you want to be prompted for installation program or image location again, remove the `media` directory before running `bmrsrtadm`.

The `bmrsrtadm` command on Linux also lets you specify the path to a file system image file. (You also can specify a device path, a local directory path, or a network directory path). For example, the BMR third-party products CD is distributed as an ISO file system image. You can download the image and use it as the source image or write it to CD media.

To create a Linux SRT

1. On the boot server where you want to create the SRT, change to the following directory:

   ```
   /usr/openv/netbackup/bin
   ```

2. Enter the following command:

   ```
   ./bmrsrtadm
   ```

3 When you are prompted, select the option to create a new SRT.

Caution: The `bmrsrtadm` command on AIX and HP-UX prompts you to enter the desired architecture (32/64) while you create BMR SRT.

If you want to install NetBackup client of the versions older than 7.0 into SRT, this OS architecture type should to be selected as 32-bit. For NetBackup 7.0, select 64-bit as OS architecture type.

While you install NetBackup client into SRT, `bmrsrtadm` gives the appropriate error message if there is any incompatibility between SRT OS architecture type and NetBackup client version.

4 Complete the command prompts as indicated in following table.

`Enter the name of the SRT to create`	The name of the SRT also is used for the directory that contains it. Only alphanumeric characters and the underscore (_) character are allowed.
`Enter the description of the new SRT`	A description of the SRT.
`Enter the directory in which to place the new SRT`	The path to the directory in which to create the SRT. The root of the SRT (called the SRT path) is the pathname to the SRT location, which includes the SRT name. The default is either /export/srt or the directory where an SRT was last created successfully. The directory must exist.

`The following media is required:`
`Linux distribution - disk` *x* `of` *x*
`Please load the media now.`
`Load media from:`
	The Linux distribution (Red Hat or SUSE) and the required disk.
	The `bmrsrtadm` command prompts you for several of the Linux installation discs.
	Some systems try to mount the media that is loaded in the CD drive automatically (such as the Red Hat `magicdev` process). When you are prompted for media on those systems, do the following: load the media into the drive, close the drive tray, and wait for the drive light to stop flashing before pressing Enter.

`The following media is required:`
`BMR third-party products CD (3PPCD)`
`Please load the media now.`
`Load media from:`
	Enter the name of the device in which the BMR third-party products CD is inserted or enter the path to the installation image.
	This CD contains open source the components that BMR uses on Linux systems.

`The following media is required:`
`NetBackup x.x Client`
`Please load the media now.`
`Load media from:`
	Enter the name of the device in which the NetBackup client software installation media is inserted or enter the path to the installation image.
	After you enter the device name or path, the NetBackup client installation procedure installs the client software into the SRT.
	The following appears when the NetBackup client software installation process begins:
	Symantec installation script
	Copyright 1993 - 2007 Symantec Corporation, All Rights Reserved.
	Installing NetBackup Client Software
	Note: To install NetBackup server software, insert the appropriate NetBackup server CD.

`Do you want to continue? [y,n] (y) y`	Enter `y`.
`Do you want to install the NetBackup client software for this client? [y,n] (y)`	Enter `y`.

`OS Level Options`
`1. IBMzSeriesLinux2.4.21`
`2. RedHat2.4`
`q. To quit from this script`
	Always choose Red Hat 2.4, even when you create an SUSE Linux SRT.

`Enter the name of the NetBackup server:`	Enter any nonblank value. The server name is replaced at restore time with the correct values for the BMR client being restored.
`Would you like to use servername as the configured name of the NetBackup client? [y,n] (y)`	Accept the default or enter any nonblank value. The client name is replaced at restore time with the correct values for the BMR client being restored.

After you install the Linux and NetBackup software, the `bmrsrtadm` command provides options to install other software in the SRT. You can either add other software now or quit (you can always add software later).

More information is available about how to add other software.

See "About adding software to a shared resource tree" on page 125.

Creating an SRT for Windows

Windows SRTs no longer require the user to supply a version of Windows. The SRTs use a special version of Windows that is shipped with the boot server.

To create an SRT for Windows

1 From the **Start** menu on the Windows BMR boot server that is to host the SRT, select **Programs > Symantec NetBackup > Bare Metal Restore Boot Server Assistant**.

The Bare Metal Restore Boot Server Assistant appears.

2 Click **Shared Resource Tree Administration Wizard**.

The Shared Resource Tree Administration Wizard appears.

Note: You can use an SRT containing the NetBackup client of 7.0 or higher versions to restore the back-level NetBackup clients.

---

3 Select the option to create a shared resource tree. Then follow the prompts to create a shared resource tree. You must provide the following information:

Name	The name of the SRT is also used for the directory that contains it. Only alphanumeric characters and the underscore (_) character are allowed.
Description	Enter the description of the SRT. For example: Windows 2008 SRT
Location for the SRT	When you configure the 32-bit or 64-bit SRT for the first time, you need to specify the source location of SRD. For 32-bit SRT, specify the source location of `srd.wim`, which is as follows: *<DVD root>*`\Addons\x86\BMRBS` For 64-bit SRT, specify the source location of `srd_x64.wim`, which is as follows: *<DVD root>*`\Addons\x64\BMRBS` *<DVD root>* is the root folder on the NetBackup Windows installation DVD.
Path to the NetBackup client software image	Enter the path of the BMR client software image.

About adding software to a shared resource tree

Install additional software into an existing SRT only if it is required during a restore. Additional software may include an operating system patch or fileset that

NetBackup client software requires. The software in an SRT is not installed on the restored system. It only brings the protected system to a state from which the original files can be restored. Therefore, you do not need to install the following: patches, maintenance levels, Maintenance Packs, service packs, fileset, or drivers into an SRT that are in a protected system.

Clustering software does not need to be installed into an SRT. After the local file systems are restored, the client rejoins the cluster.

More information is available on the following tasks:

- See "Adding software to a UNIX or Linux SRT" on page 126.
- See "Adding software to a Windows SRT" on page 130.

Adding software to a UNIX or Linux SRT

The `bmrsrtadm` command provides options to install additional software in an existing UNIX or Linux SRT.

The following options are available, although not all options are supported on all systems:

- Symantec NetBackup Maintenance Pack
- Veritas Volume Manager and Veritas File System
- Symantec Security Service
- Other software
  The name of the option depends on the operating system.

Note: Use only the specific options from this list to add products to an SRT.

If you did not add required NetBackup software when you created the SRT, a prompt appears to add it when you select the modify option.

After you add the NetBackup software when you create an SRT, the `bmrsrtadm` command provides options to install other software in the SRT.

To add software to a UNIX or Linux SRT

1. On the BMR boot server where the SRT resides, change to the following directory:

   ```
   /usr/openv/netbackup/bin
   ```

2. Enter the following command:

   ```
   ./bmrsrtadm
   ```

3. When you are prompted, select the option to modify an existing shared resource tree.
4. Enter the name of the SRT to modify.
5. Select an installation option.

   The `bmrsrtadm` command guides you through software installation. Usually, you have to enter the path to the installation program or image for the software.

   To continue, see the following information about the software you install:

   - See "About adding NetBackup Maintenance Packs" on page 127.
   - See "About adding Veritas Volume Manager and Veritas File System" on page 127.
   - See "About adding Symantec Security Services" on page 129.
   - See "About adding other software" on page 129.

About adding NetBackup Maintenance Packs

If a NetBackup maintenance or feature pack is installed on the clients the SRT protects, install that Maintenance Pack or feature pack in the SRT.

When you install a Maintenance Pack or feature pack, you are prompted for the location of the installation program or image:

```
Location (device or path) of the Symantec NetBackup Maintenance Pack
media
```

About adding Veritas Volume Manager and Veritas File System

The following information does not apply to Linux systems.

If Veritas Volume Manager (VxVM) and Veritas File System (VxFS) are installed on the systems that the SRT protects, install them in the SRT. Then BMR can use them to partition disks and rebuild file systems.

The VxVM and VxFS versions in the SRT must exactly match that of the client being restored. If the versions do not match, the restored client software is unable to access the file systems and volumes.

If protected clients have different versions of VxVM or VxFS, create a separate SRT for each of those versions. However, SRTs that include VxFS and VxVM can be used to restore the clients that do not have VxFS or VxVM installed. If you need more than one SRT of the same operating system, create an SRT with only the operating system and NetBackup client software. (For example, if you want to restore the clients that have different versions of VxVM or different drivers.) Then make as many copies as you need and add the different versions of the other software to the copies. To copy an existing SRT usually is faster than to create an SRT.

Identify any prerequisites that VxVM and VxFS require, such as operating system patches. Install them in the appropriate order before you install VxVM and VxFS.

Warning: On Solaris systems, verify that any patches support the `patchadd -C` flag. Only install patches that support the `patchadd -C` flag into the SRT. Most patches for VxFS and VxVM do not support the `patchadd -C` flag. Test results show that the clients that use patched versions of VxFS and VxVM can perform a restore successfully. They perform restores successfully even when they use an SRT that contains unpatched versions.

The **Install Veritas Volume Manager and Veritas File System** option in the `bmrsrtadm` command prompts you to:

```
Install Veritas License Software (prerequisite to below)
Install Veritas Volume Manager
Install Veritas File System
```

You do not have to untar and uncompress the packages before you install them in an SRT. When you are prompted for the path to each component, enter a path to the extracted packages. Or enter a path to the root directory of the installation program (the directory that contains the *file_system* and *volume_manager* directories).

For more information about operating system dependencies for VxVM and VxFS, see the *NetBackup Release Notes*.

About adding Symantec Security Services

In Bare Metal Restore 7.5, separate installation of Symantec Security Services in SRT is not required. Symantec Security Services gets installed into SRT along with NetBackup client installation. For the SRTs containing an older version of NetBackup client, Symantec Security should be installed separately into SRT. If you use NetBackup Access Management to administer access to your NetBackup environment, install the Symantec Security Services (VxSS) software for NetBackup client older version.

For more information about Access Management components and how to use Access Management, see the *NetBackup Security Guide*.

About adding other software

Use only the specific Symantec options to add Symantec products to an SRT.

The following menu options for other software depend on the operating system of the SRT:

AIX	Maintenance levels (MLs) or additional fileset
HP-UX	No other software is required; therefore, you cannot add software
Linux	Additional drivers
Solaris	Additional packages or patches

When you install other software, you are prompted for the following: the location of the installation program, image, package, patch, fileset, rpm, and so on (depending on operating system).

See "About installing patches, packages, and Solaris SRTs" on page 129.

See "Installing device drivers into Linux SRTs" on page 130.

About installing patches, packages, and Solaris SRTs

Always use the `bmrsrtadm` command to install patches and packages into Solaris SRTs. The `bmrsrtadm` command prevents any damage from the packages that do not support the `pkgadd -R` flag.

Patches that are installed into the miniroot that do not support the `patchadd -C` flag can damage BMR boot servers as well as JumpStart servers. Therefore, do not install the patches into an SRT that do not support the `patchadd -C` flag.

Installing device drivers into Linux SRTs

To add or update device drivers in a Linux SRT, use the following procedure.

To install device drivers into Linux SRTs

1 Choose **Install additional drivers**.

The following appears:

```
The following options are available to install or update kernel
drivers in the boot image:
1. Install a Red Hat driver update disk (.img file) into the boot
image.
2.Install a driver module (.o file) into the boot image.
3. None of the above, leave unchanged.
Enter your selection [3] :
```

2 Some hardware vendors provide drivers in a floppy image file. Choose option 1 to install these drivers (both the kernel driver module and any related hardware identification information that is contained in the image).

3 Choose option 2 to update an existing kernel driver module. Do not use this option to add new driver modules. It loads the driver module only and not the hardware identification information that is required to associate a new driver with the corresponding hardware.

Adding software to a Windows SRT

You can install the following into an existing Windows SRT:

- Windows service pack (Legacy SRTs only)
- NetBackup client software
- Veritas Storage Foundation for Windows
- NetBackup Security Services

To add software to a Windows SRT

1 On the **Start** menu on the Windows BMR boot server that hosts the SRT, click **Programs > Symantec NetBackup > Bare Metal Restore Boot Server Assistant**.

2 In the **Bare Metal Restore Boot Server Assistant**, click **Shared Resource Tree Administration Wizard**.

3 In the Shared Resource Tree Administration Wizard, click **Next** on the **Welcome** panel.

4 Select the option to update an SRT.

5 Select one of the following resources to add to the shared resource tree:

- Add a Windows service pack to an SRT.
- Add or update NetBackup client software images in an SRT. An SRT must contain a NetBackup client image that is the same version as the system(s) to be protected.
- Add Veritas Storage Foundation for Windows to an SRT.
- Add Symantec Security Services to an SRT.
  This option is specific to legacy-based SRTs of versions older than NetBackup 7.0.
  For NetBackup 7.0, separate installation of Symantec Security Services for SRT is not required. Symantec Security Services are automatically installed in SRT along with NetBackup client software installation.
  For the SRTs with the NetBackup client software of versions older than 7.0, Symantec Security Services software should be separately installed. This additional installation is required if you use NetBackup Access Management to administer your NetBackup environment.

6 Follow the prompts to add software to the shared resource tree.

  The Shared Resource Tree Wizard help provides additional information.

Enabling or disabling SRT exclusive use

The following information applies only to UNIX and Linux clients.

If you save custom files with the client configuration, you can copy those custom files into the SRT. They then are used in the temporary operating system environment on the client during the restore. To do so, enable the SRT for exclusive use by the client. Other clients cannot use that SRT until you disable it from exclusive use, which removes the custom files from the SRT.

Enable exclusive use before you do any of the following:

- Run a prepare-to-restore operation.
- Run a prepare-to-discover operation.
- Create a bootable CD or DVD (if you create a bootable CD or DVD that contains an SRT that has custom files).

Note: If you enable an SRT for exclusive use before custom files are saved for that client, the prepare-to-restore or prepare-to-discover process fails.

You may want to consult the following additional information:

See "About saving custom files on UNIX or Linux" on page 42.

To enable or disable SRT exclusive use

1. On the boot server where the SRT resides, change to the following directory:

   `/opt/openv/netbackup/bin`

2. Enter the following command:

   `./bmrsrtadm`

3. When you are prompted, select the option to modify an existing shared resource tree.
4. When you are prompted, enter the name of the SRT to modify.
5. When you are prompted, select the option to change exclusive use of the SRT.
6. When you are prompted, do either of the following:
   - To enable exclusive use, enter a client name.
   - To disable exclusive use, press **Enter** without entering anything.

About importing a shared resource tree

This section provides information on how to import a shared resource tree.

Importing an SRT on UNIX and Linux

This topic provides the procedure to import a shared resource tree on UNIX and Linux.

On UNIX and Linux boot servers, use the `bmrsrtadm` command to import an SRT.

To import an SRT on UNIX and Linux

1. Enter the following command:

   `./bmrsrtadm`

2. Select the option to import an existing shared resource tree.
3. Enter the required information, as follows:
   - The name for the new SRT
   - The path on the boot server where the existing SRT is located

Importing an SRT on Windows

This topic provides the procedure to import a shared resource tree on Windows.

Note: In NetBackup 7.0 and later versions, Windows Boot Servers do not support import of SRTs of versions 6.X and 6.5.X.

Windows 7.1 Windows Boot Servers do not support import of old Legacy DOS-based SRT.

On Windows boot servers, use the Shared Resource Tree Administration Wizard to import an SRT.

To import an SRT on Windows

1. On the **Start** menu on the boot server where you want to create the SRT, click **Programs > Symantec NetBackup > Bare Metal Restore Boot Server Assistant**.
2. Click **Shared Resource Tree Administration Wizard**.
3. In the **Shared Resource Tree Administration** wizard, select the option to import an SRT and then follow the prompts.

   Enter or select the following options:

   - The name for the new SRT
   - The directory on the boot server where the existing SRT is located

About copying a shared resource tree

You can create a new SRT by copying another SRT.

The new SRT is created on the boot server where you run the `bmrsrtadm` command (UNIX and Linux) or Shared Resource Tree Administration Wizard (Windows). The existing SRT may reside on either a local or a remote boot server.

NFS services are required to copy an SRT that resides on a remote boot server. The remote boot server must have NFS server services enabled.

An SRT that is in the process of being modified cannot be copied. Usually, it takes several minutes to copy an SRT. However, it can take longer depending on the size of the source SRT and the network speed if you copy to a different boot server.

See "Copying an SRT on UNIX and Linux" on page 134.

See "Copying an SRT on Windows" on page 134.

Copying an SRT on UNIX and Linux

On UNIX and Linux boot servers, use the `bmrsrtadm` command to copy an SRT.

To copy an SRT on UNIX and Linux

1. Change to the following directory on the boot server where you want to create the SRT:

   ```
   /usr/openv/netbackup/bin
   ```

2. Enter the following command:

   ```
   ./bmrsrtadm
   ```

3. When you are prompted, select the option to copy an existing shared resource tree.
4. When you are prompted, enter the required information, as follows:
   - The name of an existing SRT to copy
   - The name for the new SRT
   - The path on the boot server in which to create the SRT
   - The description of the SRT
   - (Linux only). The path to the device in which the BMR third-party options CD is inserted or an installation image of the BMR third-party options CD (Only if the SRT is copied to a Linux boot server where an SRT has not been created.)

Copying an SRT on Windows

On Windows boot servers, use the Shared Resource Tree Administration Wizard to copy an SRT.

Caution: In NetBackup 7.0 and later versions, Windows Boot Servers do not support copy of SRTs of versions 6.X and 6.5.X.

To copy an SRT on Windows

1. On the **Start** menu on the boot server where you want to create the SRT, click **Programs > Symantec NetBackup > Bare Metal Restore Boot Server Assistant**.
2. In the Bare Metal Restore Boot Server Assistant, click **Shared Resource Tree Administration Wizard**.
3. In the Shared Resource Tree Administration Wizard, select the option to copy an SRT and then follow the prompts. You must enter or select the following:
   - The name of an existing SRT to copy
   - The name for the new SRT
   - A description for the new SRT
   - The path on the boot server in which to create the SRT

Repairing a damaged shared resource tree

The following information applies only to UNIX and Linux boot servers.

If BMR places an SRT into a **DAMAGED** state, it may be possible to repair it to return it to a **READY** state. If an SRT is marked **DAMAGED** because a previous `bmrsrtadm` command is interrupted, recovery is likely. If you are unsure why an SRT was marked **DAMAGED**, delete it and create a new one from scratch.

SRT states appear in the **Shared Resource Trees** view of the NetBackup Administration Console.

To repair a damaged share resource tree

1. Change to the following directory on the boot server on which the SRT resides:

   ```
   /usr/openv/netbackup/bin
   ```

2. Run the following command:

   ```
   ./bmrsrtadm
   ```

3. Enter the number of the option to modify an existing shared resource tree.

4 When you are asked for the name of an SRT, enter the name of the damaged SRT.

5 When you are asked if you want to continue, enter **y**.

The `bmrsrtadm` program attempts to repair the SRT. The program guides you through installation of any missing SRT components.

If repair is successful, the `bmrsrtadm` modify menu appears. When you quit the program, the SRT is in a **READY** state.

Breaking a stale shared resource tree lock

The following information applies only to UNIX and Linux boot servers.

An SRT in the `LOCKED_READ` or `LOCKED_WRITE` state is busy and most operations are not allowed. To manage a locked SRT, you should wait for the process using the SRT to finish and release the lock before you proceed. (The one exception is that you can allocate an SRT in a `LOCKED_READ` state to a restore task.)

In rare cases, an SRT may be left with a stale lock. For example, if a boot server crashes or is rebooted in the middle of an SRT operation, the SRT may be left locked. If you are sure that an SRT lock is stale, you can break the lock.

Do not attempt to break an SRT lock unless you are positive it is stale. If you break the lock of an SRT while it is in use, it may become corrupted.

SRT states are displayed in the Shared Resource Trees view of the NetBackup Administration Console.

To break a stale SRT lock

1 Change to the following directory on the boot server on which the SRT resides:

```
/usr/openv/netbackup/bin
```

2 Run the following command:

```
./bmrsrtadm
```

3 When you are asked for a select, provide the number of the option to modify the Shared Resource. The following appears:

```
Enter the name of an existing SRT :
```

4 When you are asked for the name of an existing SRT, enter the name of the locked SRT and press **Enter**.

Warning: If you break the lock of an SRT while it is in use, it may become corrupted.

---

5 When you are asked if you want to break the lock, enter **n** to break the lock.

6 When you are asked if you are sure that you want to break the lock, enter **y** to break the lock.

The stale lock is broken.

The `bmrsrtadm` command modify menu appears.

When you quit the program, the SRT is in a **READY** state.

About deleting a shared resource tree

You can delete an SRT by using the `bmrsrtadm` command (UNIX and Linux boot servers) or Shared Resource Tree Administration Wizard (Windows boot servers).

An SRT that is allocated to a restore task or being modified cannot be deleted.

Deleting an SRT on UNIX and Linux

On UNIX and Linux boot servers, use the `bmrsrtadm` command to delete an SRT.

To delete an SRT on UNIX and Linux

1 Change to the following directory on the boot server where the SRT resides:

```
/usr/openv/netbackup/bin
```

2 Run the following command:

```
./bmrsrtadm
```

3 When you are prompted, select the option to delete an existing shared resource tree.

4 When you are prompted, type the name of the SRT and press **Enter**.

5 When you are asked if you want to delete the SRT, enter **y** to delete the SRT.

If the SRT is locked, this operation fails.

See "Breaking a stale shared resource tree lock" on page 136.

Deleting an SRT on Windows

On Windows boot servers, use the Shared Resource Tree Administration Wizard to delete an SRT.

To delete an SRT on Windows

1. On the **Start** menu on the Windows BMR boot server that hosts the SRT, click **Programs > Symantec NetBackup > Bare Metal Restore Boot Server Assistant**.
2. In the **Bare Metal Restore Boot Server Assistant**, click **Shared Resource Tree Administration Wizard**.
3. In the Shared Resource Tree Administration Wizard, select the option to delete an SRT. Then follow the prompts.

Shared Resource Tree Administration Wizard

This wizard applies only to Windows systems.

Use the Shared Resource Tree Wizard to do the following:

- Create an SRT
- Change an SRT description
- Import an SRT
- Copy an SRT
- Delete an SRT
- Create a bootable CD or DVD image
- Add a Windows service pack to an SRT
- Add or update NBU client software images to an SRT
- Add Veritas Storage Foundation for Windows to an SRT
- Add Veritas Security Services to an SRT

Create or modify a Shared Resource Tree panel

Select from among the following shared resource tree tasks:

- **Create a new Shared Resource Tree**
  Imports an operating system image into the SRT. To create BMR SRT on HP IA 11.31 platform with Veritas Storage Foundation packages (VxVM, VxFS), the following HP IA OS patch is required: PHCO_40961
- **Edit Shared Resource Tree**
- **Add or Update Packages to a Shared Resource Tree**
  Use this option to add or update the following:

- Windows service pack
- NetBackup client software
- Veritas Storage Foundation for Windows
- Symantec Security Services

- **Copy or Import a Shared Resource Tree**
- **Delete a Shared Resource Tree**
- **Create a bootable CD/DVD from a Share Resource Tree**
  You must first run the prepare-to-restore operation on the client for which you want to prepare the bootable CD.

Select the type of SRT to create panel

Either of the following types of Windows shared resource trees are supported:

- Fast Restore SRTs
- Legacy OS-based SRTs
  See "Create a legacy SRT panel" on page 139.

Create a legacy SRT panel

To create a legacy SRT, enter the following:

- A name for the SRT. This name is also used for the directory in which the SRT is created. Only alphanumeric characters and the underscore (_) character are allowed.
- A description of the SRT.
- A path name or browse to select the installation files (`autorun.inf` or `setup.exe`) for Windows.
- The license key for Windows.
- A path name or browse to select the location for the SRT.

Create a Fast Restore SRT panel

To create a Fast Restore shared resource tree, enter the following:

- A name for the SRT. This name is also used for the directory in which the SRT is created. Only alphanumeric characters and the underscore (_) character are allowed.
- A description of the SRT.

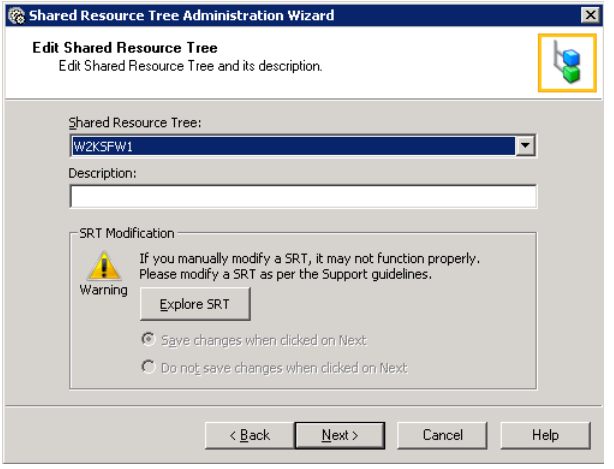
- A path name or browse to select the location for the SRT.

Edit an SRT panel

This panel lets you edit SRT parameters.

Figure 7-1 shows the **Edit Shared Resource Tree** panel in the Shared Resource Tree Administration Wizard.

Figure 7-1 Edit a Shared Resource Tree



Select the SRT to modify its parameters:

- Modify the SRT description.
- Modify the contents in the SRT by clicking **Explore SRT**.
  In certain scenarios, you may need to modify the SRT contents. For example, add a new `.exe` to the SRT as part of applying a new release update to the existing BMR version. In such scenarios, you first need to mount the SRT and then modify its contents.
  The **Explore SRT**option automatically mounts the selected SRT and shows it in the file explorer view where you can add a new `.exe`.
  If you manually modify an SRT, it may not function properly. In this case, you need to follow the guidelines that Symantec Support provides with the release update content.

After modifying the SRT, click either of the following:

- Click **Save changes when clicked on Next**.
- Click **Do not save changes when clicked on Next**.

If you select this option and click **Next**, the modifications to the SRT description or content is not saved.

Click **Next** to complete the SRT modification procedure.

Add a package to an existing SRT panel

Select the resource to add to the shared resource tree:

- Add a Windows service pack to an SRT.
- Update the NetBackup client software image in an SRT. An SRT must contain a NetBackup client image that is the same version as the system or systems to be protected.
- Add Veritas Storage Foundation for Windows to an SRT.
- Add Symantec Security Services to an SRT.

Add a Service Pack to legacy SRT panel

This option is specific to Legacy OS-based SRT and is not applicable to Fast Restore SRT.

The options for adding a Windows service pack to an SRT are as follows:

- Select the legacy shared resource tree to which you want to add a service pack.
- Select the service pack to add; all service packs available for the selected version of Windows are listed.
- Enter the path to or browse to select the service pack executable (`.exe`) image.

If you create a legacy SRT with a Microsoft Installation CD that includes a service pack, the wizard recognizes the service pack, and creates a record of it.

If you add a later service pack to an SRT that already has a service pack installed, the later one replaces the earlier one.

Add a NetBackup client image to the SRT panel

The options for adding a NetBackup client image to the shared resource tree are as follows:

- Select the shared resource tree to which to add the client image. If you want to create an SRT, the name of the SRT you want to create appears in the field.
- Enter the path name to the NetBackup client installation image (`NetBackup Client.msi`) or browse to select the image.

An SRT must contain a NetBackup client image that is the same version as the system(s) to be protected.

If the SRT already contains a NetBackup client image, it is replaced.

An SRT without a NetBackup client is in the **Defined** state. **Ready** state indicates a NetBackup client image is installed.

Add a Veritas SFW package to an SRT panel

Using this new panel, you can add maintenance packs or hot fixes that are associated with the installed version of SFW (Veritas Storage Foundation for Windows) to a legacy SRT.

Note: Using NetBackup Bare Metal Restore, you can protect clients that have SFW 5.0 and later versions installed.

The options for adding an SFW package to a legacy SRT are as follows:

- Select the legacy OS-based shared resource tree to which to add the SFW image.

  Note: PC-DOS is no longer required to run a Legacy Restore. In BMR 7.0.1 and later versions, the Legacy Restore SRT boots from a WinPE boot image.

- Apply SFW image to the selected SRT.
- Apply associated SFW Maintenance Pack to the SRT.
  Select this option to directly go the **Add a Veritas SFW Maintenance Pack Image to an SRT** panel.
- Apply associated SFW Hot Fix to the SRT.
  Select this option to directly go the **Add a Veritas SFW Hot Fix Image to an SRT** panel.

Table 7-2 lists the SFW versions that the SRT should have installed to restore clients with specific operating systems and SFW versions.

Table 7-2 SRT contents to restore SFW clients

Operating System	SFW version on the client	Minimum base SFW version in the SRT	Maintenance pack Required in the SRT	Hot Fix required in the SRT	MSXML 6.0 required
Windows 2003 (32 or 64-bit)	SFW 5.0, SFW 5.0 RP1, SFW 5.0 RP2	SFW 5.0	RP2	None	None
Windows 2003 (32 or 64-bit)	SFW 5.1, SFW 5.1AP1, SFW SP1, SFW SP2	SFW 5.1	AP1	Hotfix_5_1_01004_407_1974940b https://sort.symantec.com/patch/detail/3354/0/cGF0Y2gvc2VhcmNobWF0cml4LzIxLzIvMQ	Yes http://www.microsoft.com/downloads/en/details.aspx?FamilyId=993c0bcf-3bcf-4009-be21-27e85e1857b1&displaylang=en
Windows 2008 (32 or 64-bit)	SFW 5.1, SFW 5.1AP1	SFW 5.1	AP1	Hotfix_5_1_01004_407_1974940b https://sort.symantec.com/patch/detail/3354/0/cGF0Y2gvc2VhcmNobWF0cml4LzIxLzIvMQ	None
Windows 2008 (32 or 64-bit)	SFW 5.1 SP1	SFW 5.1	SP1	Hotfix_5_1_10012_584_1946291 https://sort.symantec.com/patch/detail/3491/0/cGF0Y2gvc2VhcmNobWF0cml4LzIxLzIvMQ	None
Windows 2008 (32 or 64-bit)	SFW 5.1 SP2	SFW 5.1	SP2	None	None
Windows 2008 R2 (32 or 64-bit)	SFW 5.1 SP1	SFW 5.1	SP1	Hotfix_5_1_10012_584_1946291 https://sort.symantec.com/patch/detail/3491/0/cGF0Y2gvc2VhcmNobWF0cml4LzIxLzIvMQ	None
Windows 2008 R2 (32 or 64-bit)	SFW 5.1 SP1 AP1	SFW 5.1	SP1	Hotfix_5_1_10012_584_1946291 https://sort.symantec.com/patch/detail/3491/0/cGF0Y2gvc2VhcmNobWF0cml4LzIxLzIvMQ	None

Table 7-2 SRT contents to restore SFW clients *(continued)*

Operating System	SFW version on the client	Minimum base SFW version in the SRT	Maintenance pack Required in the SRT	Hot Fix required in the SRT	MSXML 6.0 required
Windows 2008 R2 (32 or 64-bit)	SFW 5.1 SP2	SFW 5.1	SP2	None	None

Add a Veritas SFW image to the SRT panel

Using NetBackup Bare Metal Restore, you can protect clients that have SFW (Veritas Storage Foundation for Windows) 5.0 and later versions installed.

The options for adding an SFW image to a legacy SRT are as follows:

- Select the legacy OS-based shared resource tree to which to add the SFW image.
- Select the version of SFW.
- Enter the path to the root of the SFW installation CD or browse to select the folder.

Note: The SRT and the restoring client should contain the same base SFW version. For example: If you want to restore a 5.1 SP1 client, the SRT should contain 5.1 SP1 or later SP version.

You cannot use SRT with SFW 5.1 to restore an SFW 5.0 client. This is because volume and disk group creation parameters may change across major releases and there may be license key conflicts.

To know the compatibility between the SFW versions of BMR clients and SRT, refer to the SRT contents to restore SFW clients table.

See "Add a Veritas SFW package to an SRT panel" on page 142.

See "Examples screen shots for SFW package installation into SRT" on page 149.

During a restore, BMR installs SFW only if it was on the protected system. Therefore, you can use one SRT to protect clients with and without SFW.

If you add a later SFW package to an SRT that already has one, the later version replaces the earlier one.

Add an SFW Maintenance Pack to an SRT panel

Using NetBackup Bare Metal Restore, you can protect clients that have SFW 5.0 and later versions installed with all available Maintenance Packs.

To know the compatibility between the SFW versions of BMR clients and SRT, refer to the SRT contents to restore SFW clients table.

See "Add a Veritas SFW package to an SRT panel" on page 142.

See "Examples screen shots for SFW package installation into SRT" on page 149.

The options for adding an SFW Maintenance Pack to a legacy SRT are as follows:

- The selected SRT is displayed.
- Select the appropriate Service Pack for the existing SFW version.
  All Service Packs that are associated with the existing SFW version are available in the drop-down list for selection.
- Enter the path to the SFW Maintenance Pack installation image or browse to select the image.

Add an SFW Hot Fix to an SRT panel

Using NetBackup Bare Metal Restore, you can protect clients that have SFW 5.0 and later versions installed with all available Maintenance Packs and Hot Fixes.

To know the compatibility between the SFW versions of BMR clients and SRT, refer to the SRT contents to restore SFW clients table.

See "Add a Veritas SFW package to an SRT panel" on page 142.

See "Examples screen shots for SFW package installation into SRT" on page 149.

The options for adding an SFW Hot Fix to a legacy SRT are as follows:

- The selected SRT is displayed.
- Select the appropriate Maintenance Pack for the existing SFW version.
  All Hot Fixes that are associated with the existing SFW MP version are available in the drop-down list for selection.
- Enter the path to the SFW Hot Fix installation image or browse to select the image.

Add a Windows Hot Fix to an SRT panel

This panel is displayed if the selected legacy SRT has the following configuration:

- Windows 2003

- SFW 5.1

To know the compatibility between the SFW versions of BMR clients and SRT, refer to the SRT contents to restore SFW clients table.

See "Add a Veritas SFW package to an SRT panel" on page 142.

See "Examples screen shots for SFW package installation into SRT" on page 149.

Note: In case of Windows 2003, if you install SFW 5.1 AP1 Hot Fix, you need to also install MSXML 6.0 self-extractable `.exe`. You can download this Windows Hot Fix from the following location:

http://www.microsoft.com/downloads/en/details.aspx?FamilyId=993c0bcf-3bcf-4009-be21-27e85e1857b1&displaylang=en

For Windows 2008 and later versions, MSXML `.exe` is included in the SFW Hot Fix that you install into the SRT.

The options for adding a Windows Hot Fix to a legacy SRT are as follows:

- The selected SRT is displayed.
- Select the appropriate Service Hot Fix for Windows 2003, for example Microsoft XML Core Services 6.0.
- Enter the path to the SFW Hot Fix installation image or browse to select the image.

Add NetBackup Security Services to an SRT panel

Symantec Security Services (VxSS) is used by NetBackup for the Access Management type of security.

The options for adding VxSS to an SRT are as follows:

- Select the shared resource tree to which to add the VxSS image
- Select the version of VxSS
- Enter the path to the VxSS setup file (in `.exe` format) or browse to select the image.

Selecting the Copy SRT or Import SRT option panel

You can either create a new SRT or create an SRT based on any of the existing SRT.

On the **Copy or Import SRT** panel, you can select either of the following options:

- Select the **Copy a Shared Resource Tree** option to copy an SRT that resides on another boot server.
- Select the **Import a Shared Resource Tree** option to import an SRT that resides on another boot server.

Import an SRT panel

To import an SRT, do the following:

- Select the directory on the boot server where the existing SRT is located, which you want to import.
- Enter the name for the new SRT.

Copy an SRT panel

To copy an SRT from another boot server to your boot server, do the following:

- Select the SRT to copy.
- Enter a name for the SRT. The SRT name should not contain more than eight alphanumeric characters.
- Enter a description for the new SRT.
- Enter a description of the SRT.
- Enter a path to or browse to select the location to create the new the SRT.

Delete an SRT panel

Select the SRT to delete, then click **OK** in the confirmation dialog box.

Create a Fast Restore CD image or DVD image panel

The sequence of panels for creating bootable CD/DVD images from Fast Restore SRTs is as follows:

- Select the shared resource tree.
  See "Select an SRT panel" on page 148.
- Specify the location of ISO and client verification.
  See "Specify a location for the ISO image panel" on page 148.

The process ends with the **Copy Progress** panel and the **Completing the Shared Resource Tree** panel.

Select an SRT panel

Select the shared resource tree that you want to turn into a bootable CD or DVD image to be used for the restore. For legacy SRTs, you must run a prepare-to-restore operation on a client using the selected SRT.

Specify a location for the ISO image panel

Enter the path or browse to select the directory in which the ISO image is to be stored. The wizard does not create a CD or a DVD; it creates an image that you must burn onto a CD or a DVD.

If any clients are listed on this page, they are automatically restored when booting this image.

Create a bootable CD image for a legacy SRT panel

You can create a bootable CD image for a legacy SRT.

The following is the sequence of panels:

- **Select a shared resource tree**
  See "Select a shared resource tree panel" on page 148.
- **Location of ISO image**
  See "Location of ISO image panel" on page 148.

The process ends with the **Copy Progress** panel and the **Completing the Shared Resource Tree** panel.

Select a shared resource tree panel

Select the shared resource tree that you want to turn into a bootable CD or DVD image to be used for the restore.

Use the same SRT used during the prepare-to-restore operation.

You must run a prepare-to-restore operation on a client using the SRT you choose in this panel.

Location of ISO image panel

Enter the path or browse to select the directory in which the ISO image is to be stored.

The wizard does not create a CD. It creates an image that you must burn onto a CD.

Completing the Shared Resource Tree configuration panel

Click **Finish** to complete the process.

Examples screen shots for SFW package installation into SRT

This section provides a series of screen shots that help you understand the compatibility between the SFW package versions of the BMR clients and the SRTs.

This section contains the example screen shots for installations of SFW 5.0 and SFW 5.1 versions into SRT.

To know about the compatibility between all SFW versions of BMR clients and SRT, refer to the SRT contents to restore SFW clients table.

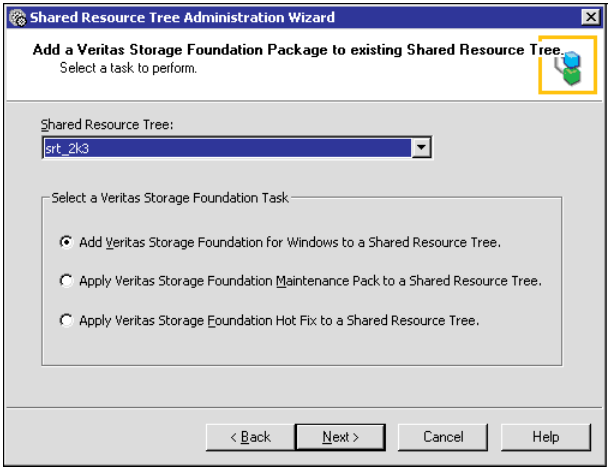
See "Add a Veritas SFW package to an SRT panel" on page 142.

- SFW 5.0
  See "Example screen shots for SFW 5.0 installation into SRT" on page 149.
- SFW 5.1
  See "Example screen shots for SFW 5.1 installation into SRT" on page 152.

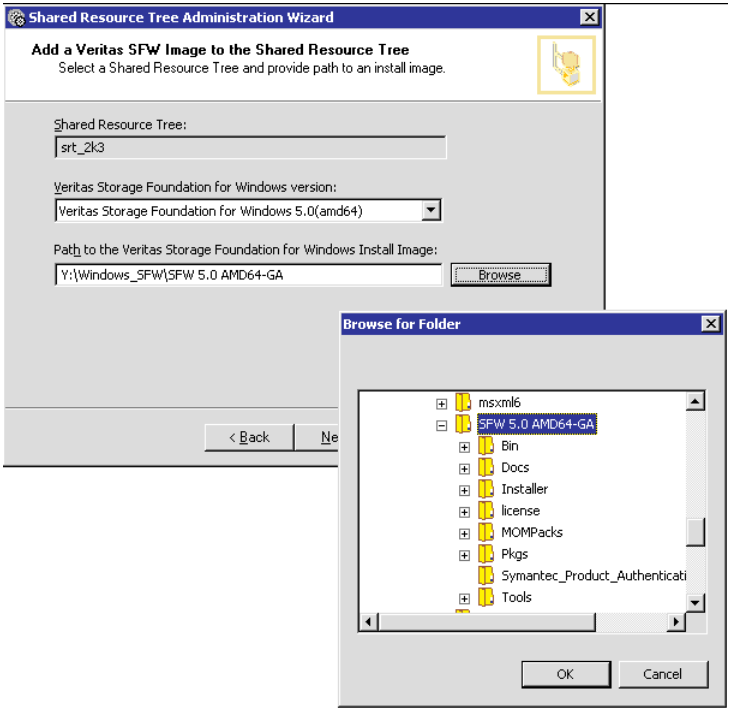
Example screen shots for SFW 5.0 installation into SRT

Refer to this section while installing SFW 5.0 packages into the selected SRT.

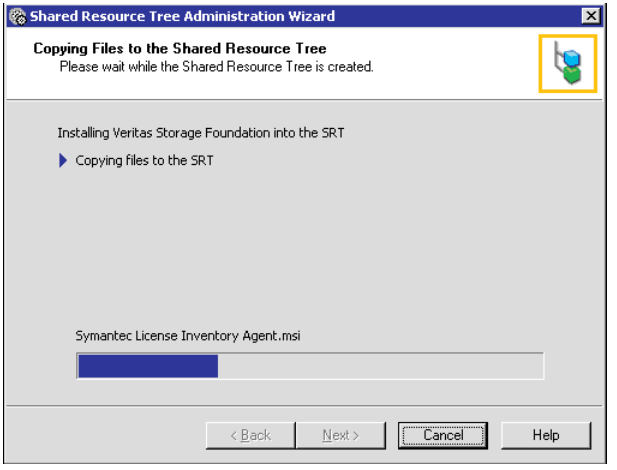
Select the SRT into which you want to install SFW 5.0 image.



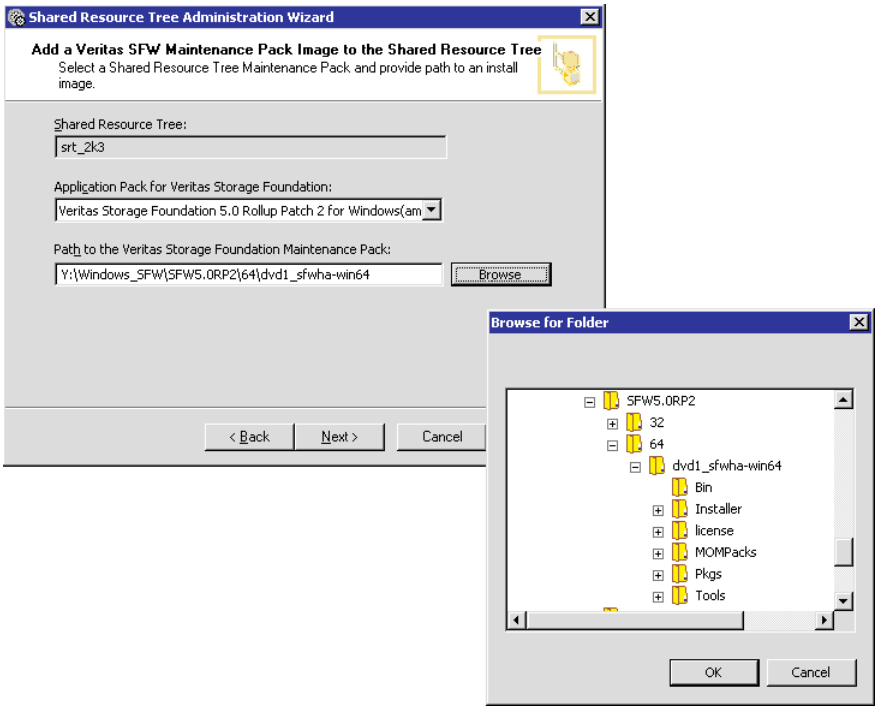
Select the SFW 5.0 image.



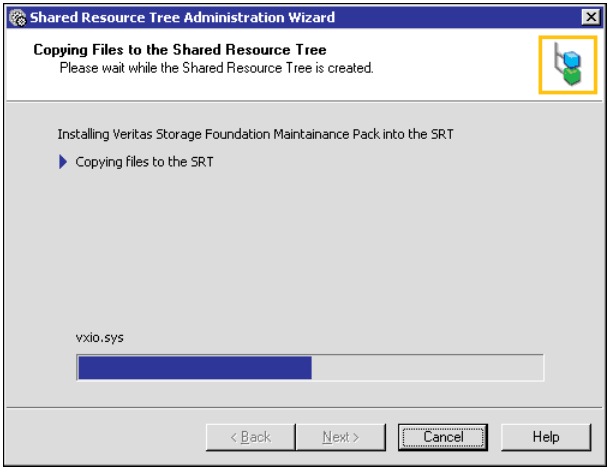
Start SFW 5.0 installation.



Select the required SFW 5.0 Application Pack and Maintenance Pack.



Start the SFW 5.0 RP2 installation.

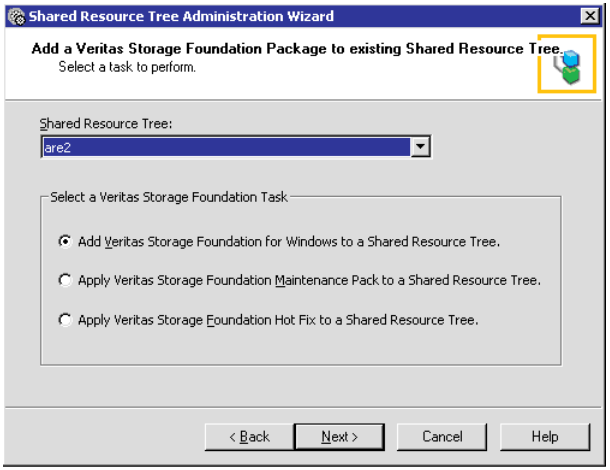


This completes the SFW 5.0 installation into the selected SRT.

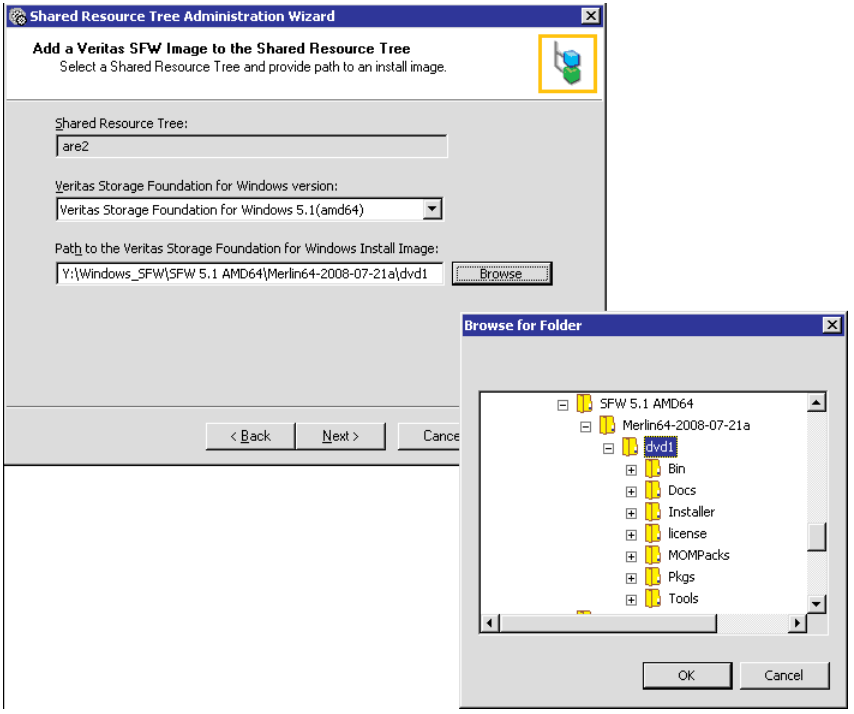
Example screen shots for SFW 5.1 installation into SRT

Refer to this section while installing SFW 5.1 packages into the selected SRT.

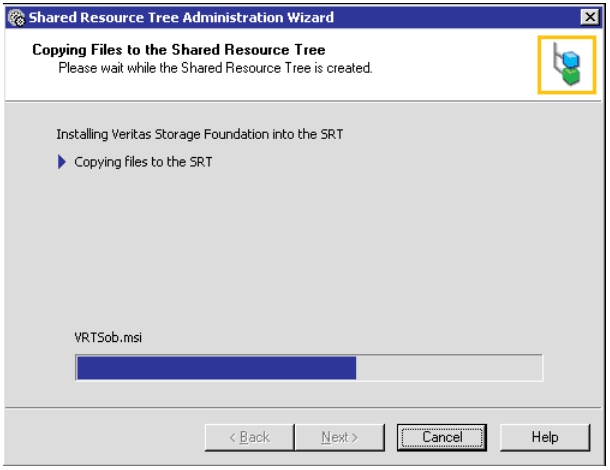
Select the SRT into which you want to install SFW 5.1 image.



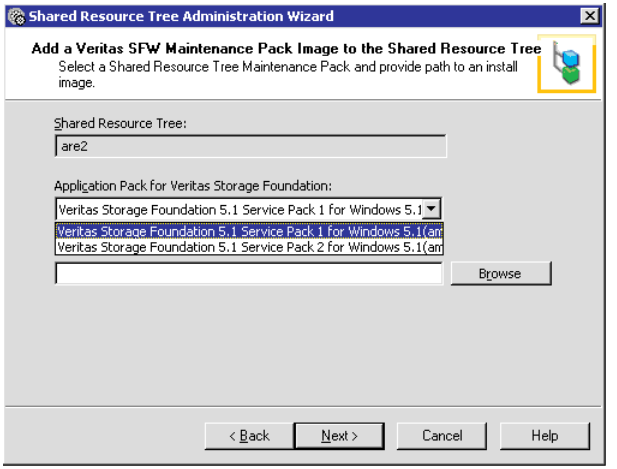
Select the SFW 5.1 image.



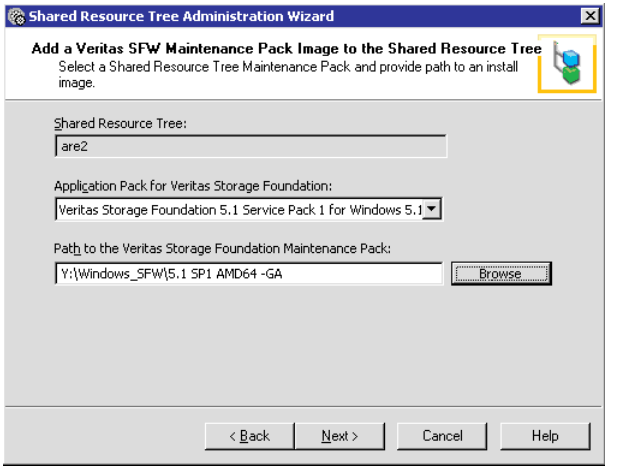
Start the SFW 5.1 installation.



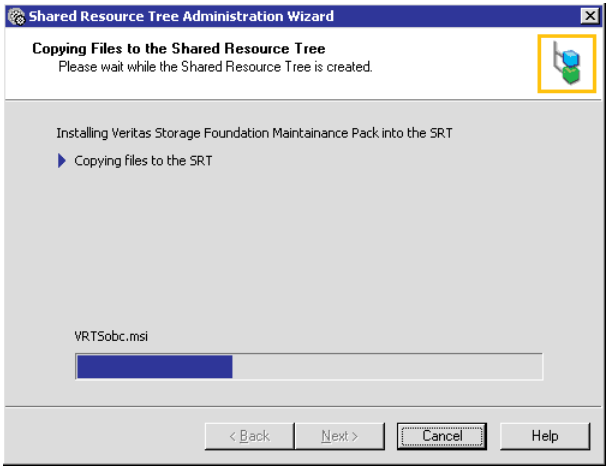
Select the required SFW 5.1 Application Pack.



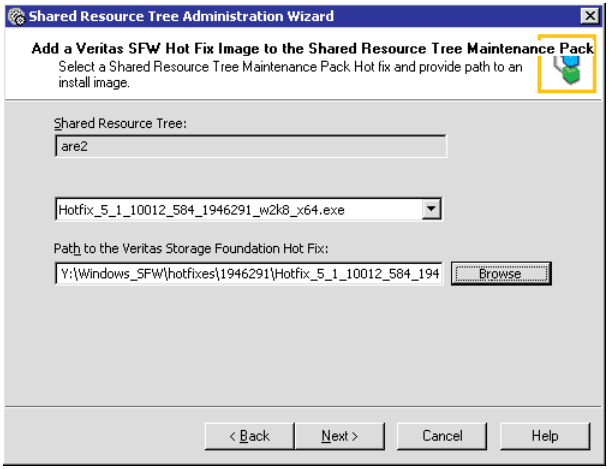
Select the SFW 5.1 SP1 Maintenance Pack.



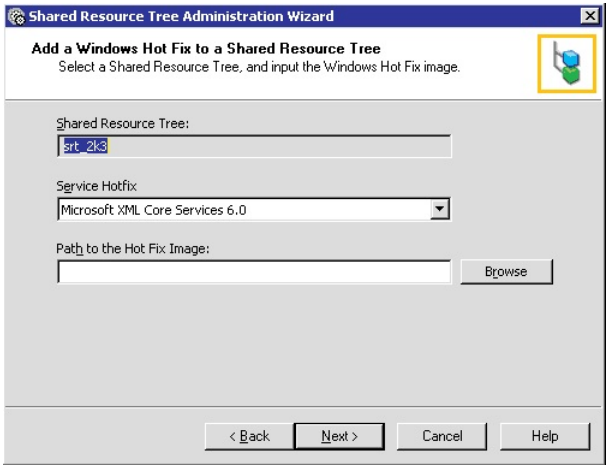
Start the SFW 5.1 SP1 MP installation.



Select the required SFW 5.1 Hot Fix.



Select the required Windows Hot Fix.



This completes the SFW 5.1 installation into the selected SRT.

Chapter 8

Managing boot media

This chapter includes the following topics:

About boot media

Boot media is used to boot a client and provide the shared resource tree or the resources to mount a shared resource tree. The boot media contains a small runtime environment that includes a kernel, a RAM file system, libraries, and programs. The client system firmware boots the kernel from the media. CD boot media also contains a shared resource tree.

If you use media to boot the client system, you must use BMR to prepare the appropriate boot media. You can prepare boot media at any time before the restore. However, a prerequisite is that the shared resource tree for the protected system must exist.

Boot media is created from the resources that are stored in an SRT. The boot media must be compatible with the commands and libraries in the SRT and the client.

A legacy boot floppy uses a version of DOS to start networking services and to copy the files that are needed for a restore environment. The SRT on the boot server sends these files to the client being restored. Boot floppies can be fully customized (automated) for a specific BMR client or they can be generic and prompt for information at restore time. At initial creation time, customized floppies may be archived on the master server for quicker re-creation later.

About the supported boot media on Windows for BMR 7.0.1 and later versions

The BMR restore process begins by network booting the client from a BMR boot server or from BMR prepared boot media (CD or DVD).

You can restore a client using Fast Restore SRTs or Legacy OS-based SRTs. Versions older than BMR 7.0.1 also supported floppy as a boot media if you selected the Legacy OS-based Restore option, on Windows platform.

Note: The Legacy OS-based Restore of Windows Server 2008 SP2 systems can be done with a Legacy OS-based SRT that is at Windows Server 2008 SP1 level. The `Prepare To Restore` command allows this special scenario.

Note: In BMR 7.0.1 and later versions, floppy-based restore is not supported on Windows platform.

In BMR 7.0.1 and later versions, you can boot BMR clients only with the following options on Windows platform:

- Network boot
- CD/DVD Media boot

Note: In BMR 7.0.1 and later versions, because of the elimination of PC-DOS, you do not need to create Boot Floppy. Therefore the **Legacy Boot Floppy Wizard** link on the **Boot Server Assistant** screen is removed.

About writing a CD or DVD

The size of the media boot image that BMR produces depends on several factors. The structure of the installation program can change from one release to another and from one type of media (CD) to another (DVD). Therefore, sizes of the final images that are produced may be different under seemingly identical conditions.

The size of the media boot image that BMR produces depends on the following:

- The optional software packages on the SRT
- The operating system version
- The install media type used (where applicable) during media boot image creation.

In all cases, if the final media boot image that BMR produces fits on a CD, burn the image to a CD or a DVD. However, if the final image cannot fit on a CD, you must burn a DVD.

CD/DVD media must be bootable by the system for which you create it. To determine the correct way to create a bootable CD/DVD for the specific system, see the instructions that are provided with your CD/DVD writing software.

In addition, consider the following:

- The CD/DVD image that is created for AIX, Linux, and Solaris uses ISO-9660 format. HP-UX uses a binary format that is different from ISO.
- BMR does not contain CD/DVD writing software.

  Burn the CD/DVD image onto a disk using CD/DVD writing software that supports the following:

  - ISO-format images for AIX, Linux, and Solaris
  - Binary images for HP-UX

  The procedures for writing CDs/DVDs vary between applications; refer to the documentation for procedures.
- The CD/DVD writing software may require that ISO-format or binary CD/DVD image files end in a .iso extension. If necessary, you can add a .iso extension to the CD/DVD image before you write it.
- If the BMR boot server does not have CD/DVD writing hardware and software, transfer the CD/DVD image to a system that does. Ensure that the CD/DVD image file transmits as a binary file and transfers without errors; corrupted CD/DVD image files produce unpredictable results.
- For the CD/DVD media that includes an SRT, the name of the SRT appears as the content of the root directory on the CD/DVD.
- Label the CD/DVD for easy identification.

  Include the following information.

  - The client name (Windows clients)
  - The NetBackup version that is used
  - The operating system of the SRT that is installed
  - Any extra software installed
- BMR does not use the CD/DVD image file after it is created. Therefore, you can move, rename, or delete the image file after you write the CD/DVD.

Creating boot media for UNIX and Linux

On UNIX and Linux systems, use the `bmrsrtadm` command to create a bootable CD/DVD image that contains an SRT. After you create the CD/DVD image, you must use CD/DVD writing software to burn the image onto a CD/DVD.

This process copies an existing SRT to the CD/DVD media; therefore, an SRT that supports the client must exist.

The following is the required information:

- The name of the SRT you want to use.
- The name to use for the SRT on the CD/DVD.
- The path to a directory that has enough free space to store the CD/DVD image.

To create boot media for UNIX and Linux

1. On Solaris systems only, use the following command to verify that the `vold` process is not running on the boot server where the SRT resides:

   ```
   # ps -ef | grep vold
   ```

   If it is running, do the following:

   - To eject any CD/DVD that may be loaded, run the following command

     ```
     # eject
     ```

   - To stop the `vold` process, run the following command

     ```
     # /etc/init.d/volmgt stop
     ```

2. On the boot server on which the SRT resides, change to the following directory:

   ```
   /usr/openv/netbackup/bin
   ```

3. Run the following command:

   ```
   ./bmrsrtadm
   ```

4 When you are prompted, select the option to create a new CD/DVD image based shared resource tree.

5 Continue by referring to the information about the operating system.

See "About boot media for AIX" on page 161.

See "About boot media for HP-UX" on page 161.

See "About boot media for Linux" on page 162.

See "About boot media for Solaris" on page 162.

About boot media for AIX

You must have the AIX installation program that created the SRT that you want to use to create the boot media. (You must have it even if you created the SRT from a network copy of the media.) You must enter the device name that contains the installation program.

The directory for the CD/DVD image should not be a direct prefix of the directory that contains the SRT you intend to use.

For example, you can use the following for SRT `/export/srt/aix433esm`:

- Do not specify `/`, `/export`, or `/export/srt` for the location.
- You can specify `/export/srt/mb` because it is not a direct prefix of the SRT path.

About boot media for HP-UX

HP-UX uses a binary format that is different from ISO. The CD/DVD image file is a binary image of the CD/DVD and does not contain an extension. However, you can add an `.iso` extension to the CD/DVD image if your CD/DVD writing software requires it.

The CD/DVD recording programs that are known to work for HP-UX images are as follows:

- Sony CD/DVD Extreme. Add an `.iso` extension to the image file name and use the **Global Image** or **Other Image** option from the **File** menu options.
- Nero. Add an `.iso` extension to the image file name, and use the **Burn Image to Disk** option.

Note: The Roxio Easy CD/DVD Creator recording program does not work for HP-UX images.

About boot media for Linux

For Linux, the `bmrsrtadm` command creates a bootable ISO image file by using the name of the SRT with an `.iso` extension. Any standard CD/DVD writing software can be used to write media from this file.

About boot media for Solaris

You must have the Solaris installation media (Software 1 of 2) that created the SRT you copy to the CD/DVD. You must enter the device name that contains the installation media.

After you enter the information about the SRT, the following information appears:

- If Veritas Volume Manager (VxVM) is installed on the BMR boot server, the following appears:

```
What do you want to use for temporary space?
Select one of the following options:
    1. Use a disk group.
    2. Use a raw partition.
Enter your selection (1-2) [1] :
```

  Enter `1` or `2`. Then enter the name of the disk group or the device file for the raw partition. If you use a raw partition for temporary storage, you are prompted to continue.

- If Veritas Volume Manager (VxVM) is not installed on the BMR boot server, the following appears:

```
Enter the name of a partition of size 103040 or more blocks
```

  Enter the name of the device file for the raw partition. Then respond to the next prompt if you want to continue.

After the CD/DVD image is created, restart the `vold` process (`/etc/init.d/volmgt start`) if you stopped it before running `bmrsrtadm`.

Creating boot media for a Windows client

Windows systems may create a bootable ISO image which can be burned to either a CD or DVD.

To create boot media for a Windows client

1. On the Windows BMR boot server, select **Programs > Symantec NetBackup > Bare Metal Restore Boot Server Assistant** from the Windows **Start** menu.

   The **Bare Metal Restore Boot Server Assistant** screen appears.

2. Click **Shared Resource Tree Administration Wizard**.
3. Select the option for **Create a Bootable CD/DVD** from a Shared Resource Tree.
4. Follow the prompts to create the boot media.

Chapter 9

Managing Windows drivers packages

This chapter includes the following topics:

About Windows drivers packages

Windows packages are network interface card (NIC) drivers and mass storage device (MSD) drivers. Packages are stored in the BMR database on the NetBackup master server. The packages pool is comprised of the packages that are stored in the database. The packages pool is the common pool of packages that can be added to restore configurations.

Packages may be required when you restore to a different system, in which case you add them to the restore configuration. If the **Packages** window does not contain a driver that is required for a dissimilar system restore, add it to Bare Metal Restore. Do not add it to the restore configuration if a driver is on the Windows installation media that created the SRT.

If a package required for a dissimilar system restore already appears in the **Packages** window, add it to the restore configuration.

See "Client configuration properties" on page 176.

See "Devices and drivers properties" on page 178.

Adding a Windows driver package

Add a package, as follows:

- Use the Driver Package Wizard on any Windows boot server to add a network interface card (NIC) driver or mass storage device (MSD) driver.
- Alternatively, install NetBackup client software on the target system and perform a full BMR backup. The drivers are saved in that client's configuration and available for use during a dissimilar system restore.

Before you can add a package, you must have the installation files for the package. Obtain them from the vendor's Web site, the installation program that is provided with the NIC device or MSD device, or another BMR Windows client in your environment.

Note: You can add only NIC and MSD drivers. All other types of drivers (audio, video, modem, and so on) must be installed on the system after the restore is complete.

See "Finding the correct driver if Windows is already installed" on page 166.

To add a driver package by using the Driver Package Wizard

1. On the **Start** menu on any Windows boot server, click **Programs > Symantec NetBackup > Bare Metal Restore Boot Server Assistant**.
2. In the Bare Metal Restore Boot Server Assistant, click **Driver Package Wizard**.
3. In the Driver Package Wizard, step through the prompts as follows to add the software package:
   - Path to the installation files for the package
   - Description of the package
   - Version of Windows that the package can be used with
   - The specific driver from the package installation files (installation files may include more than one driver)

Finding the correct driver if Windows is already installed

A driver information file (`.inf` or `txtsetup.oem`) may contain information about more than one driver. Therefore, when you add a mass storage device (MSD) or network interface card (NIC) driver, you may have to select from more than one option.

The devices should be documented in the materials that come with the computer. If not, contact the manufacturer for the driver option.

Alternatively, use the following procedure to determine the correct name for the driver if Windows is installed.

To find the correct driver if Windows is already installed

1. On the computer that contains the mass storage device adapter, open the Windows device manager.
2. Expand the category for the adapter (for example, network adapters).
3. Note the device name that appears here. The option name in the `.inf` file should be the same or similar to this one.

Deleting a Windows driver package

The following procedure deletes a driver package.

Warning: Do not delete any drivers that are required for a restore.

To delete a Windows driver package

1. In the NetBackup Administration Console on the NetBackup master server, click **Bare Metal Restore Management > Resources > Packages**.
2. In the details pane, right-click the driver you want to delete.
3. Select **Delete** on the shortcut menu.
4. In the confirmation panel, click **Yes**.

   The selected package is deleted.

Chapter 10

Managing clients and configurations

This chapter includes the following topics:

About clients and configurations

Logically, a BMR client is a collection of configurations. A configuration is a collection of information about the system to be used as a template to rebuild a protected system.

It includes the following:

- Number of disk drives
- Volume information
- File system information
- Number and type of network adapters

- Network properties
- Drivers
- Other system software components.

Most BMR operations are performed on configurations.

When a BMR protected client is backed up, the configuration of the client is saved and named current. Every time a client is backed up, the new saved configuration replaces the previously saved configuration.

The saved, current configuration is read-only. Use the current configuration to restore the original protected system to its state at the most recent backup (a standard or a self restore).

To restore to a different point in time, to different disks, or to a different system, create a restore configuration by copying a current configuration. Then modify the restore configuration.

About ZFS storage pool support

Zettabyte File System (ZFS) is a combined file system and logical volume manager, which is part of Solaris operating system. ZFS is available on both SPARC and x86-based systems.

Support for ZFS is added in Solaris 10 6/06 (“U2”). When you install Solaris 11 ZFS is also installed and set as the default file system.

Starting with NetBackup 7.5, Bare Metal Restore can protect Solaris 10 Update 8 and later clients that are attached to ZFS storage pools. The ZFS support in NetBackup 7.5 ensures that the Solaris clients with ZFS storage pools are protected.

BMR 7.5 supports backup and restore of Solaris 10 Update 8 and later clients with the following configurations:

- ZFS Root Pool and Data Pools
- ZFS storage pools on slice
- ZFS file system with zones
- ZFS with SAN boot
- ZFS storage pools along with VxVM and SVM disk groups

Note: All above features are supported on Solaris SPARC and Solaris x86_64 architectures.

BMR 7.5 does not support Solaris clients with the following configurations:

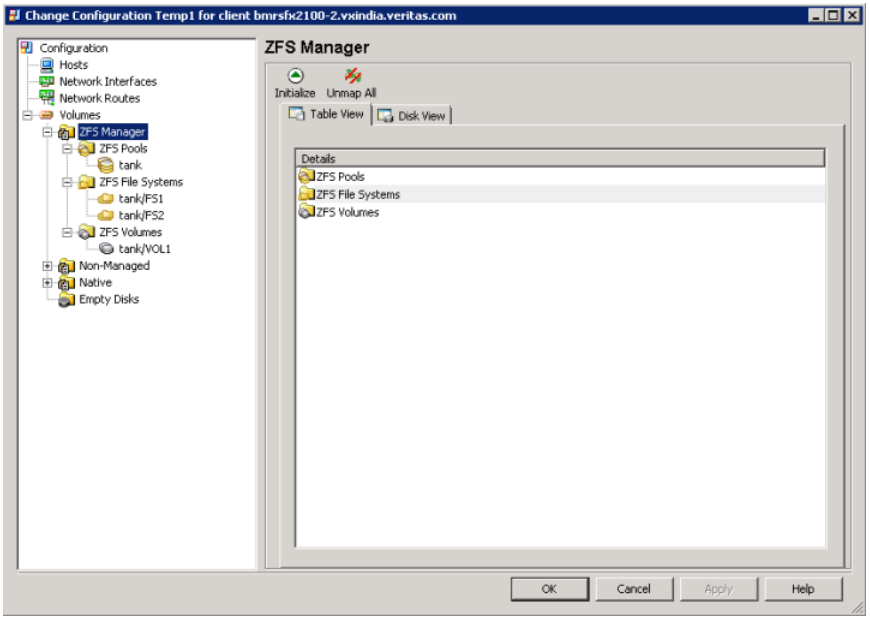
- UFS to ZFS migration
- Different file system on ZFS volumes

To view the ZFS Manager elements and its parameters, do the following:

- In the NetBackup Administration Console, click Bare Metal Restore Management > Hosts > Bare Metal Restore Clients. Open the Change Configuration dialog box for the client for which you want to view all associated volumes.

Figure 10-1 shows the ZFS Manager GUI screen.

Figure 10-1 ZFS Manager UI



Copying a configuration

Copy a configuration so that you can do the following:

- Restore a client to a state that was saved in a backup before the last backup.
  See "About restoring to a specific point in time" on page 72.
- Restore a client in which the disks have changed.
  See "About restoring to dissimilar disks" on page 73.
- Restore a Windows client to a different system.
  See "Restoring to a dissimilar Windows system" on page 78.

- Restore a client to the same hardware but with different network properties.

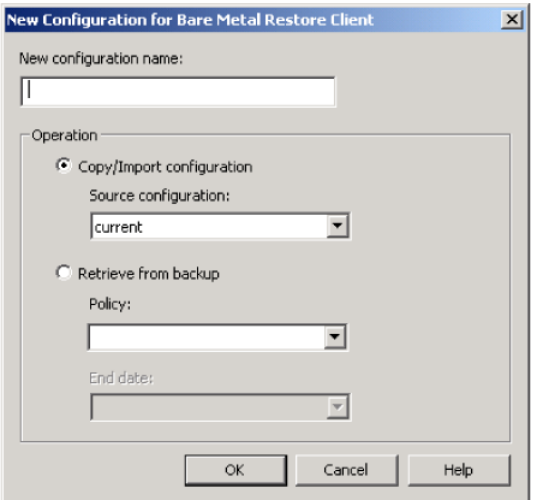
A copied configuration that is used for a restore is called a restore configuration.

After you create the restore configuration, modify it so it matches the target hardware properties.

Note: You do not have to modify the point in time restore configuration.

To copy a configuration

1. In the NetBackup Administration Console, click **Bare Metal Restore Management > Hosts > Bare Metal Restore Clients**.
2. In the **All Bare Metal Restore Clients** tree pane, expand the view of the client that contains the configuration you want to copy.
3. Right-click the configuration you want to copy.
4. On the shortcut menu, select **New**.



5. On the **New Configuration for Bare Metal Restore Client** dialog box, complete the fields.
6. Click **OK**.
7. If necessary, modify the configuration.

   See "Modifying a configuration" on page 174.

Discovering a configuration

You can discover the configuration of a new system; the system does not have to be a NetBackup client. A discovered configuration contains the hardware and the software information of a host.

When you discover a configuration, BMR adds it to the discovered configurations pool. The elements of the configuration (such as disk layout) can then be used when you perform operations such as dissimilar disk restore.

When the discovery operation ends, the following occurs on the client, and the configuration appears in the **Discovered Configurations** view:

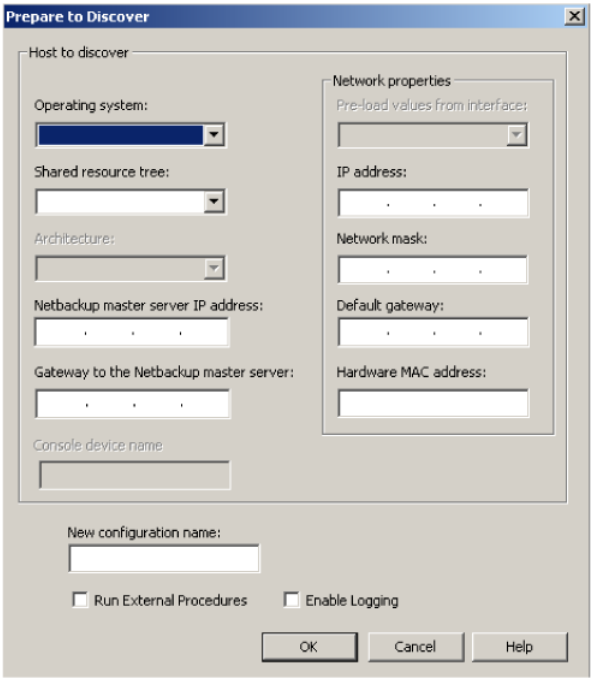
- AIX clients display B55 on the LED display.
- HP-UX, Linux, and Solaris clients display the following message:

  ```
  The Bare Metal Restore hardware discovery boot has concluded.
  ```

- Windows clients display a popup box stating that the discovery is finished and that you can click **OK** to reboot the system.

To discover a configuration

1 In the **Bare Metal Restore Management** node, click **Actions > Prepare to Discover**.



2 In the **Prepare to Discover** dialog box, complete the fields and enter data as necessary.

If you select a client in the **Hosts > Bare Metal Restore Clients** view, the values for that client are included in the dialog box.

If a client is the target of a dissimilar disk restore (DDR) and VxVM manages the protected client's disks, specify an SRT with VxVM installed.

3 Click **OK**.

4 Boot the client to start the hardware discovery operation.

If you use media boot, when BMR prompts for the client name, enter it as it appears in the **Tasks** view from the prepare-to-discover operation.

Modifying a configuration

Modify a configuration so you can do the following:

- Restore a client to a state that was saved in a backup before the last backup.
  See "About restoring to a specific point in time" on page 72.
- Restore a client in which the disks have changed.
  See "About restoring to dissimilar disks" on page 73.
- Restore a Windows client to a different system.
  See "Restoring to a dissimilar Windows system" on page 78.
- Restore a client to the same hardware but different network properties.

You cannot modify the configuration named current; you must create a configuration you can edit.

See "Copying a configuration" on page 171.

To modify a configuration

1. In the NetBackup Administration Console, click **Bare Metal Restore Management > Hosts > Bare Metal Restore > Clients**.
2. In the **All Bare Metal Restore Clients** pane, expand the view of the client that contains the configuration you want to modify.
3. Right-click the configuration you want to modify.
4. On the shortcut menu, select **Change**.
5. In the **Change Configuration** dialog box, modify properties as needed.

   See "Client configuration properties" on page 176.

Deleting a configuration

You cannot delete a current configuration.

To delete a configuration

1. In the NetBackup Administration Console, click **Bare Metal Restore Management > Hosts > Bare Metal Restore Clients**.
2. In the **All Bare Metal Restore Clients** pane, expand the view of the client that contains the configuration you want to delete.
3. Right-click the configuration you want to delete.
4. On the shortcut menu, select **Delete**.
5. In the confirmation dialog box, click **Yes**.

Deleting a client

When you delete a client, it removes only the client and its configuration from the BMR database. It does not remove the NetBackup software on the client, nor remove it from NetBackup, nor delete the backups of the client.

You can delete a client but not remove it from the NetBackup policy that backs it up. If you do, the client is reregistered with BMR the next time it is backed up and appears in the Bare Metal Restore Clients view. (The NetBackup policy that backs it up is the policy that collects BMR information.)

To delete a client

1. In the NetBackup Administration Console, click **Bare Metal Restore Management > Hosts > Bare Metal Restore Clients**.
2. Right-click the client you want to delete.
3. On the shortcut menu, select **Delete**.
4. In the confirmation dialog box, click **Yes**.

Client configuration properties

Use the **Change Configuration** dialog box to map the attributes of the client configuration on the protected system to the restore configuration. Map the configurations to enable point-in-time restore, dissimilar disk restore, or dissimilar system restore.

The **Change Configuration** dialog box contains multiple property sheets.

See "Configuration Summary properties" on page 177.

See "Devices and drivers properties" on page 178.

See "Hosts properties" on page 181.

See "Network interfaces properties" on page 182.

See "Network routes properties" on page 186.

See "About Volumes properties" on page 188.

Configuration changes are saved differently depending on which of the following NetBackup administration interfaces you use:

- In the Windows-based Administration Console, changes occur when you click **OK** or **Apply**.
- In the Java-based Administration Console, changes occur when you make them.

Configuration Summary properties

Use **Configuration Summary** property sheet of the **Change Configuration** dialog box to do the following:

- View a summary of the configuration.
- Change a license key for software on the protected system that requires a license key.
- Determine the components of the restore configuration so you can select a shared resource tree that has the appropriate software for the restore.

Figure 10-2 Configuration Summary

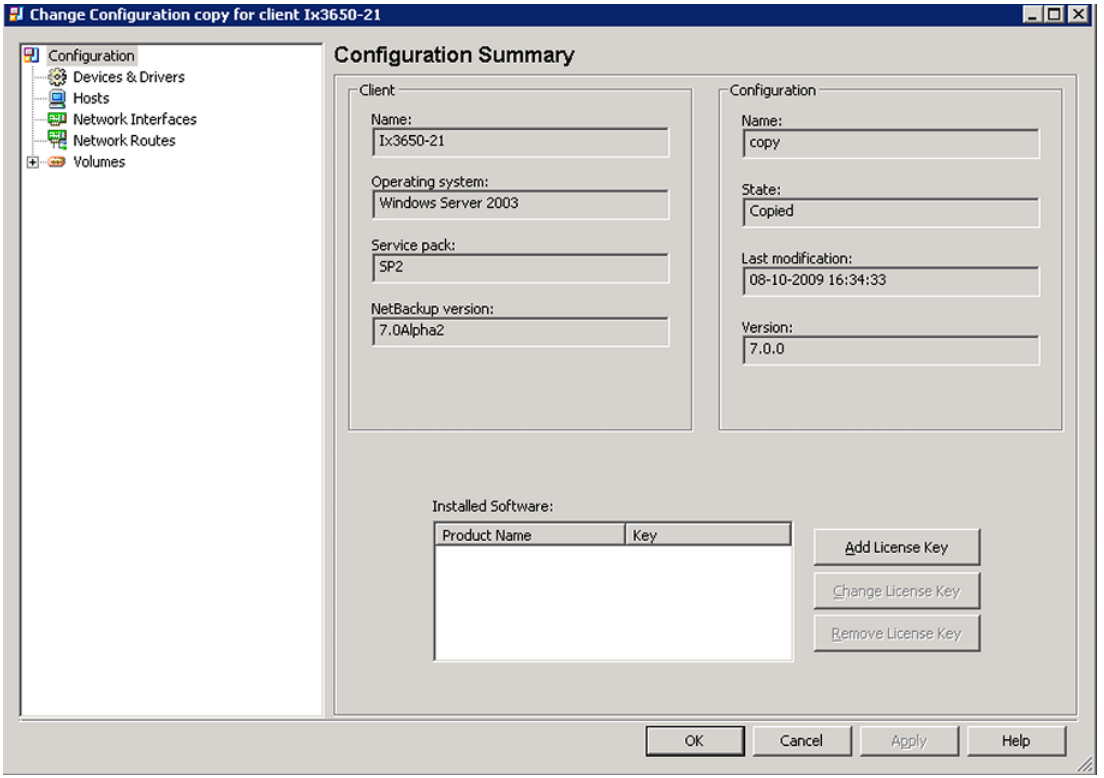


Table 10-1 describes the actions you can initiate regarding license keys.

Table 10-1 License key actions

Action	Description
Add License Key	
Change License Key	
Remove License Key	Deletes the selected license key.

Table 10-2 describes the client fields that are displayed in the dialog box.

Table 10-2 Client items

Field	Description
Name	The name of the client.
Operating system	The operating system of the client.
Service pack	(Windows clients only.) The service pack version on the client.
Architecture	(UNIX and Linux clients only.) The architecture of the client.
NetBackup version	The NetBackup software version on the client.
Veritas Volume Manager version	The version of Veritas Volume Manager or Veritas Storage Foundation for Windows (if any).

Table 10-3 describes the configuration fields that are displayed in the dialog box.

Table 10-3 Configuration fields

Field	Description
Name	The name of the configuration.
State	The state of the configuration. Saved indicates a configuration that cannot be edited. Copied indicates that the configuration can be edited.
Last modification	The date and time the configuration was last modified.
Version	The version of the configuration.

Devices and drivers properties

The **Devices & Drivers** property sheet applies only to Microsoft Windows clients.

Use the **Devices & Drivers** property sheet of the **Change Configuration** dialog box to perform the following actions:

- Initialize the devices in this configuration from a new hardware discovered configuration or from another client's configuration.
- Automatically select the correct mass storage device (MSD) drivers and network interface card (NIC) drivers for the listed devices.
- Manually add MSD and NIC drivers to the configuration.

You can also specify whether to use only BMR discovered drivers.

Figure 10-3 Devices & Drivers dialog box

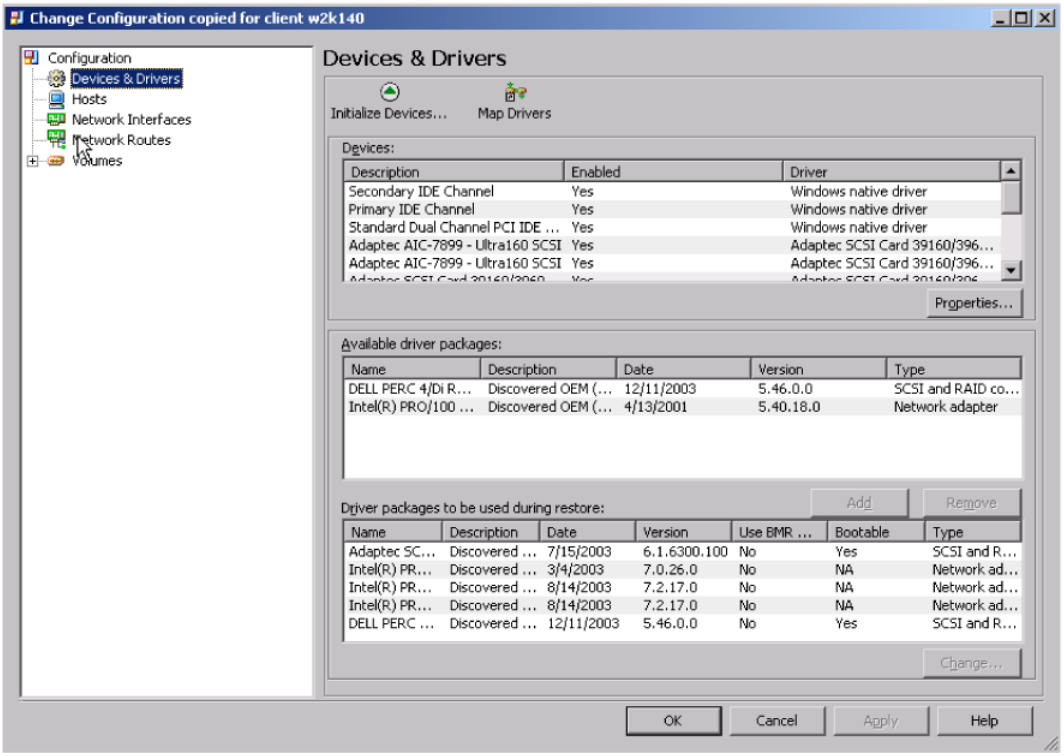


Table 10-4 describes the options available and the actions they initiate.

Table 10-4 Device and driver options

Option	Action
Initialize Devices...	Prompts you for another configuration from which to import the devices. You may select a discovered configuration or one from another client. The initialize operation updates the Drivers packages to be used during restore window to include the necessary drivers for this hardware.
Map Drivers	Automatically matches drivers to devices without drivers. If drivers are added to BMR after the last initialize operation, repeat this action. Sometimes, it may be useful to override the driver that is selected automatically by using the **Add** option to select a specific driver manually. Devices without a driver are identified in the **Devices** window by **No matching driver** in the **Enabled** column. These devices are not available during the restore.
Add	Moves the selected driver from the **Available driver packages** window to the **Driver packages to be used during restore** window.
Remove	Moves the selected driver from **Driver packages to be used during restore** window to the **Available driver packages** window.
Change	Lets you change the following attributes of the selected driver: ■ The **Use BMR discovered drivers instead of Windows supplied drivers** checkbox controls whether the selected driver is used if Windows already has a built-in driver. ■ For MSD drivers, the Bootable driver to be used during text mode portion of the installation checkbox only applies to a legacy DOS restore. It determines if the driver is used during the installation phase of the restore. It has no effect for a Fast Windows Restore.

Using discovered Windows drivers during a restore

When BMR saves third-party drivers from a protected system, the driver signing is lost. (Third-party drivers are those that are not part of the Windows distribution.) During the BMR restore, the installation process installs the standard drivers into the temporary repair environment because the drivers from the protected system are unsigned.

You can edit the configuration so that the discovered drivers are installed rather than the standard Windows drivers.

To use discovered Windows drivers during a restore

1. In the **Devices & Drivers** property sheet, select the desired driver from the list of drivers in the bottom window, and click **Change**.
2. Select the **Use BMR discovered drivers instead of Windows supplied drivers** checkbox.
3. Click **OK**.

Hosts properties

Use the **Hosts** property sheet of the **Change Configuration** dialog box to add, remove, or change the attributes of any host that has a role in the restore process.

You can change attributes so you can restore on a network with a different configuration, such as at a disaster recovery site.

Figure 10-4 Hosts property sheet

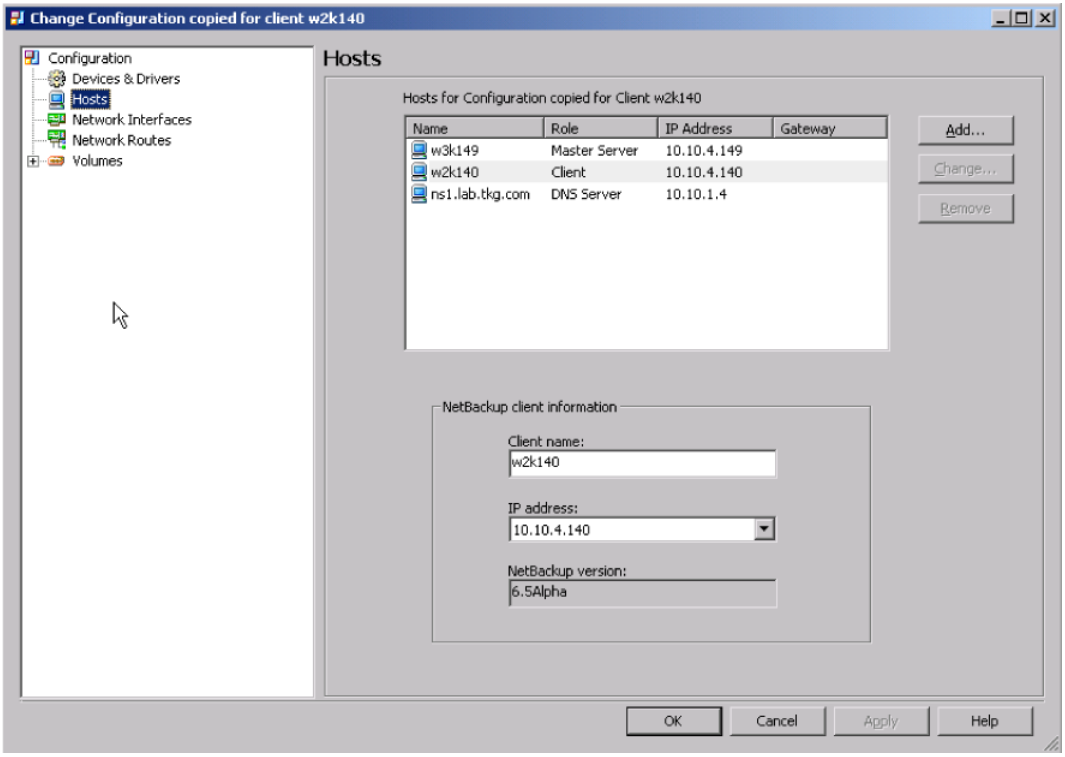


Table 10-5 describes the actions you can initiate from the property sheet.

Table 10-5 Hosts mapping actions

Action	Description
Add	
Change	
Remove	Removes the selected host. If you don't want to remove the host, click **Cancel** to exit the **Change Configuration** dialog box without applying the changes.

Table 10-6 describes the **Client Information** fields in the **Hosts** property sheet.

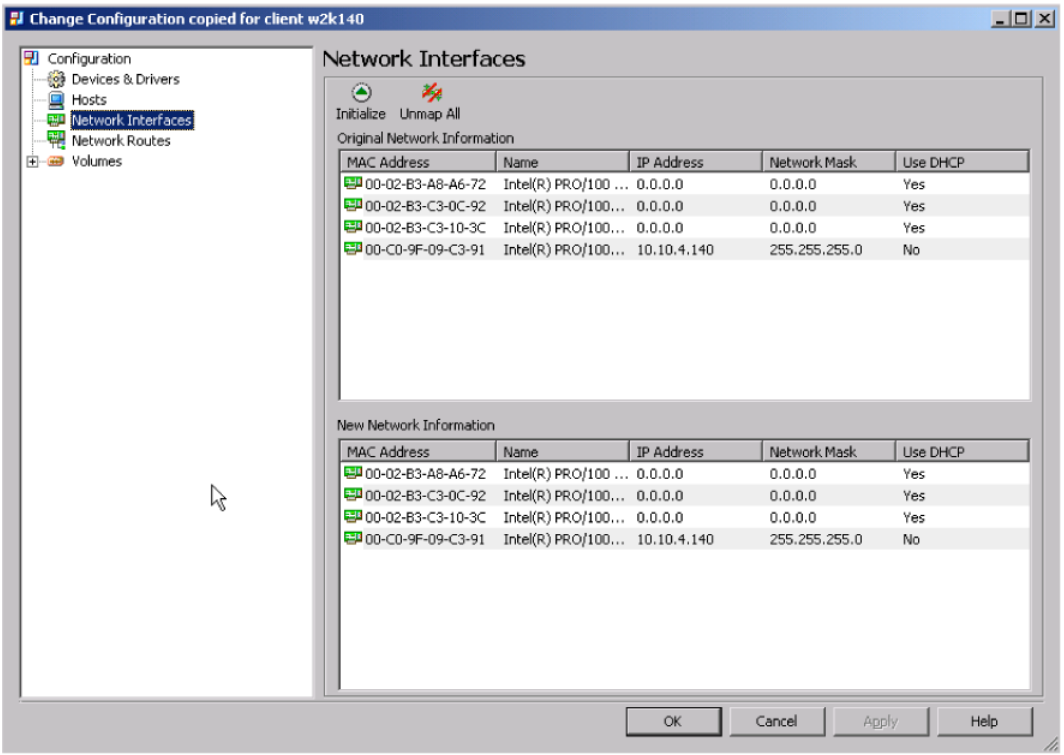
Table 10-6 NetBackup Client Information fields in Hosts dialog box

Field	Description
Client Name	The name by which NetBackup knows the client. The specified client name must match the client name in the NetBackup policy that backs up the client.
IP address	The IP address of the client. All IP addresses defined in the network interfaces are in the drop-down list.
NetBackup version	The NetBackup software version on the client.

Network interfaces properties

Use the **Network Interfaces** property sheet of the **Change Configuration** dialog box to add or remove interfaces or change the network identity that is associated with an interface.

Figure 10-5 Network interfaces property sheet



The **Original Network Information** is read-only. The **New Network Information** shows the values that are used for the restore. If the configuration was not edited, the top panes and bottom panes show the same information.

Table 10-7 describes the actions you can initiate from the dialog box.

Table 10-7 Network interface mapping actions

Action	Description
Initialize	Opens a dialog box from which you can select a configuration to import. Only the hardware information from the configuration is imported, not the network identity. The interfaces from the imported configuration replace the interfaces in the **New Network Information** window.

Table 10-7 Network interface mapping actions *(continued)*

Action	Description
Unmap All	Unmaps all mapped interfaces in the **New Network Information** window and changes all interfaces in the **Original Network Information** window to Unmapped. The unmapping removes the name, IP addresses, network masks, gateways, and DHCP and bootable attributes. MAC addresses are not removed.
Map	
Unmap	Right-click an interface in the **New Network Information** window and select **Unmap** from the shortcut menu. The unmapping of an interface removes the name, IP addresses, network masks, and DHCP and bootable attributes. MAC addresses are not removed.
Change	

Importing and mapping interfaces

If you restore to a dissimilar system and you save the target system's configuration by backing up the target system, you can do the following:

- Import the network interface card (NIC) information from the target system into the restore configuration.
- Then map the network identify from the NICs in the original configuration to the NICs in the restore configuration.

To import and map interfaces

1. Click **Initialize**.
2. In the **Import configuration** dialog box, select the client configuration to import.
3. Click **OK**.

   The network hardware information is imported into the **New Network Information** window and replaces the interfaces that were in the window. The network identity (IPs, routes, and so on) is not imported.
4. Right-click an interface in the **Original Network Information** window and select **Map** from the shortcut menu.

5 In the **Map or Change Interface** dialog box, select an interface from the **Map to Interface** drop-down list.

6 Click **OK**.

The IP address, netmask, and fully qualified domain name are applied to that interface on the restored system.

Changing interfaces manually

If you restore to a dissimilar system and do not save the target system's configuration, you can manually change interface properties for a restore.

You must first determine the MAC addresses of the NICs in the target system.

To change an interface manually

1 Right-click an interface in the **New Network Information** window and select **Change** from the shortcut menu.

2 In the **Map or change interface** dialog box, select **Use DHCP** (if using DHCP). Because this action is an interface change, the dialog box includes the **Hardware MAC Address** field.

Go to step 5.

3 Select a row of attributes in the **Attributes for Network Interface** window and click **Change**.

4 In the **Add Network Identity** dialog box, enter the IP address, netmask, and fully qualified domain name from the interface on the protected system.

Then click **OK**.

5 Enter the hardware MAC address of the NIC in the target system.

6 Click **OK**.

The MAC address and network identity are changed. The name of the interface is not changed, but it does not affect the restore.

Specifying the UNIX and Linux boot interface

UNIX and Linux clients must use a single network interface to boot from and to restore through. The **Bootable** column in the **Network Interfaces** dialog box shows the interface that is configured as the boot interface. If your restore configuration includes more than one network interface, you can specify which one to use for the restore.

Table 10-8 helps you to determine the correct interface.

Table 10-8 Bootable network interfaces

Platform or hardware type	Bootable network interface(s)
AIX	Integrated Ethernet, Ethernet card, or Token Ring Note the following about the network interfaces on AIX: ■ Only chrp hardware is supported. ■ Booting the RS/6000 from a network adapter requires support in the system firmware.
HP-UX	Integrated Ethernet only
Linux	Any Ethernet device
Solaris	Any Ethernet device

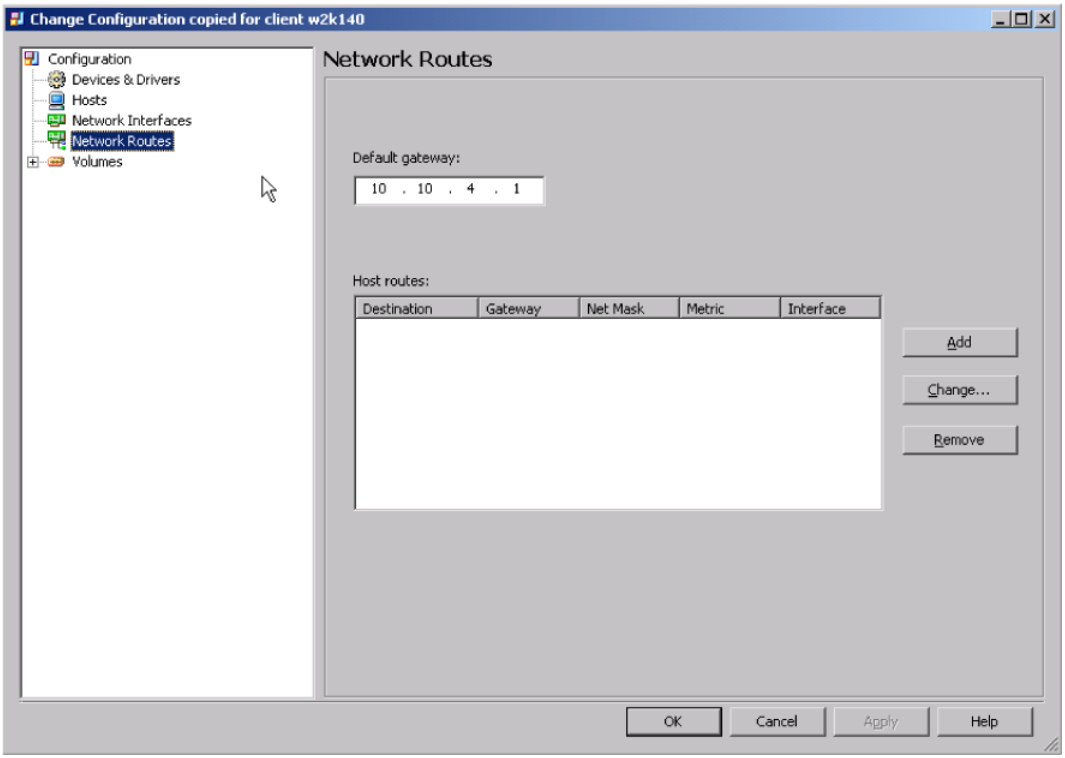
To specify the UNIX and Linux boot interface

1. In the **New Network Information** window of the **Network Interfaces** property sheet, right-click the interface that you want to use as the boot interface.
2. Select **Change** from the shortcut menu.
3. In the **Map or Change Interface** dialog box, click **Bootable**.
4. Click **OK**.

Network routes properties

Use the **Network Routes** property sheet of the **Change Configuration** dialog box to add a network route to use during the restore.

Figure 10-6 Network routes property sheet



You may need to add a route if an existing route in the configuration is not sufficient to reach the NetBackup or BMR servers. This situation can occur during disaster recovery at a different location when you move servers from one subnet to another. It also can occur when any routers that intervene are changed.

For example, client 10.10.5.12 and NetBackup master server 10.10.6.23 have a router (10.10.5.254) between them because they are on different subnets. When you prepare to restore, the restore process configures the route to the NetBackup master server as 10.10.5.254, and the restore is successful. However, if the IP address of the router between them changes, the client may not be able to reach the master server. The client cannot reach the server because the configuration does not include the correct route to it. Therefore, you must add a network route to the master server before you perform the prepare-to-restore operation.

BMR attempts to reach hosts in the following order:

- Host routes (specified on the **Hosts** property sheet)
- Network routes that are specified on this property sheet

- The default route that is specified on this property sheet

Table 10-9 describes the fields and options in the property sheet.

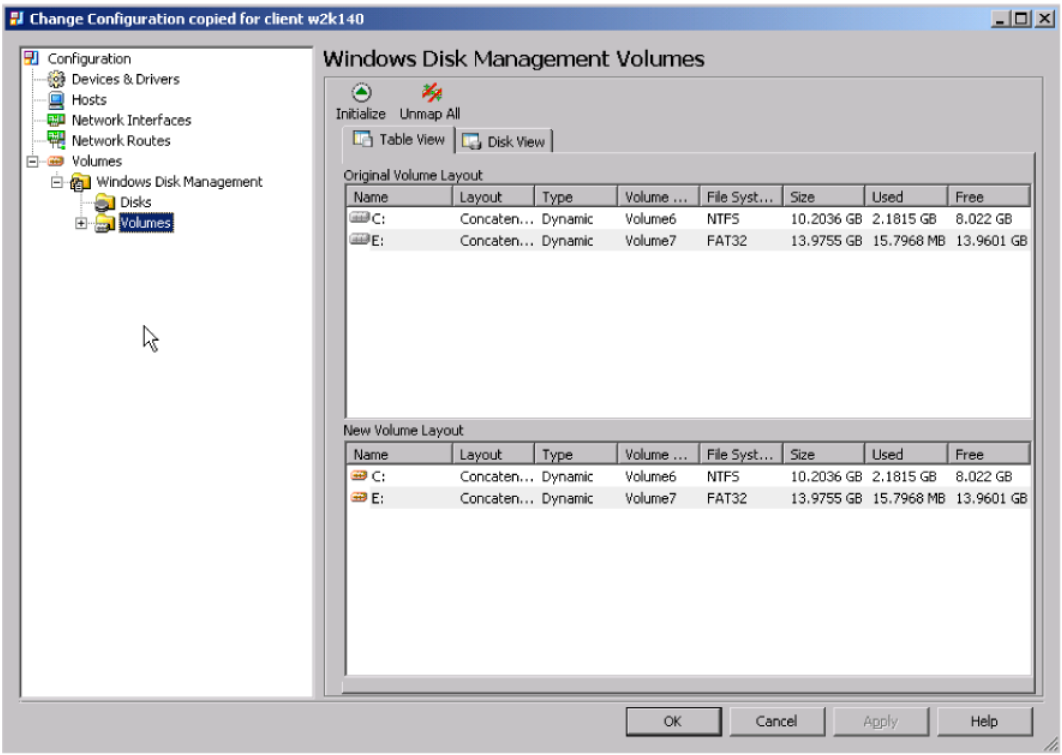
Table 10-9 Network routes mapping fields

Action	Description
Default gateway	The gateway to use if no other route reaches a host.
Add	
Change	
Remove	Removes the selected route.

About Volumes properties

Use the **Volumes** property sheet of the **Change Configuration** dialog box to map the volume configuration from the protected client to the new disks of the restore configuration.

Figure 10-7 Volumes property sheet



You can perform the following operations for mapping volumes and for changing configurations:

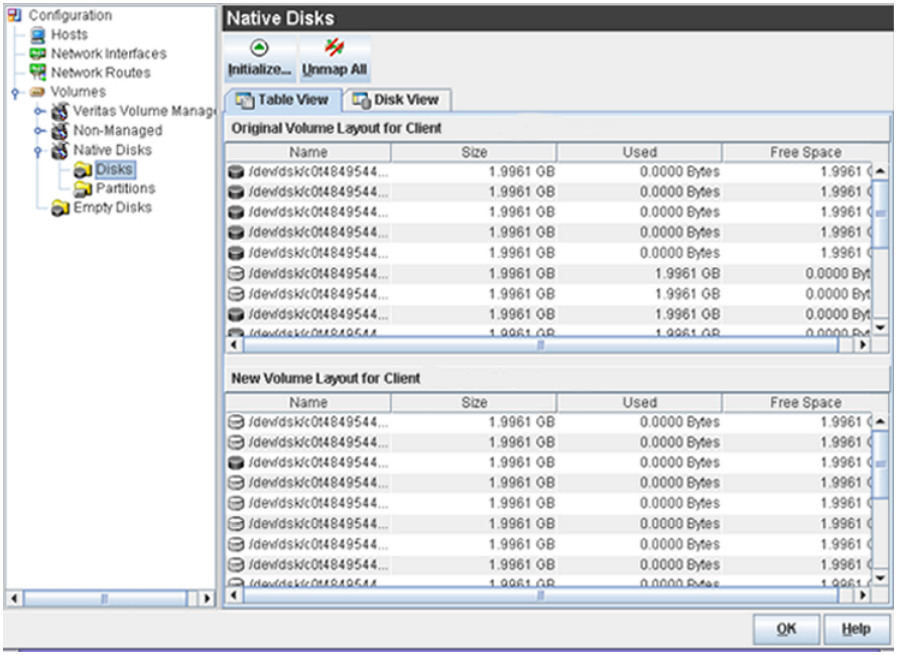
- Change the disks that make up a disk group.
- Control the file systems that are restored.
- Control the logical volumes that are created.
- Change the attributes of either a file system, a logical volume, or a disk.
- Restrict a disk to prevent it from being used as a target for mapping.
- Make a discovered disk available for mapping (remove restriction).

Given enough space on the target disk, you can map all the logical volumes and their file systems. Or you can map specific logical volumes and file systems. You do not have to restore all your logical volumes and file systems.

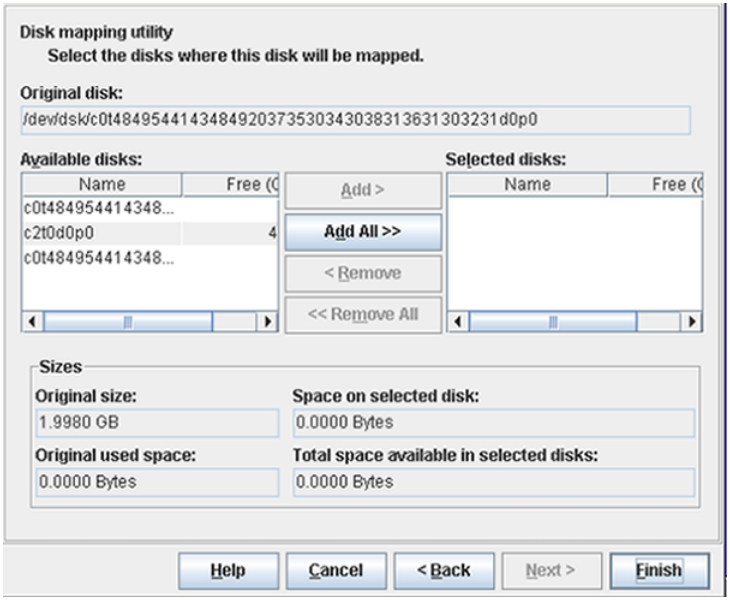
Primary partitions and simple volumes require only one disk. Striped, mirror, and RAID-5 volumes require multiple disks.

About Native Disk Objects

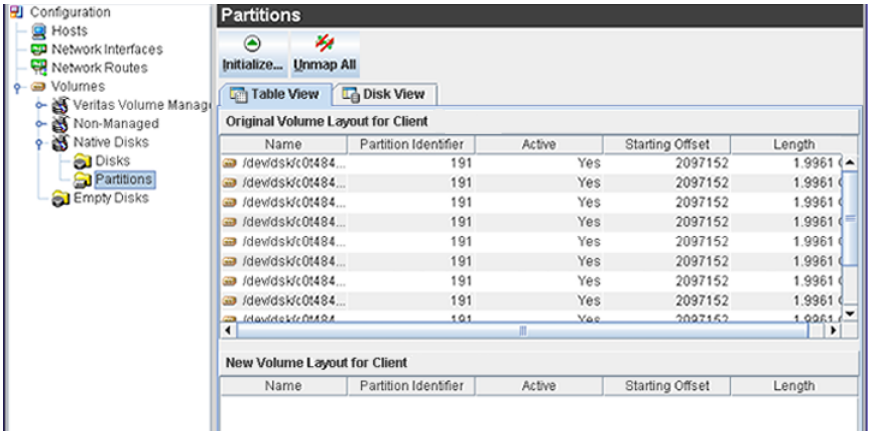
A new **Native Disk** node appears under the **Volumes** node in the **Change Configuration** dialog box. The following example shows information about the Native disks that are available with the total size, used space, and free space.



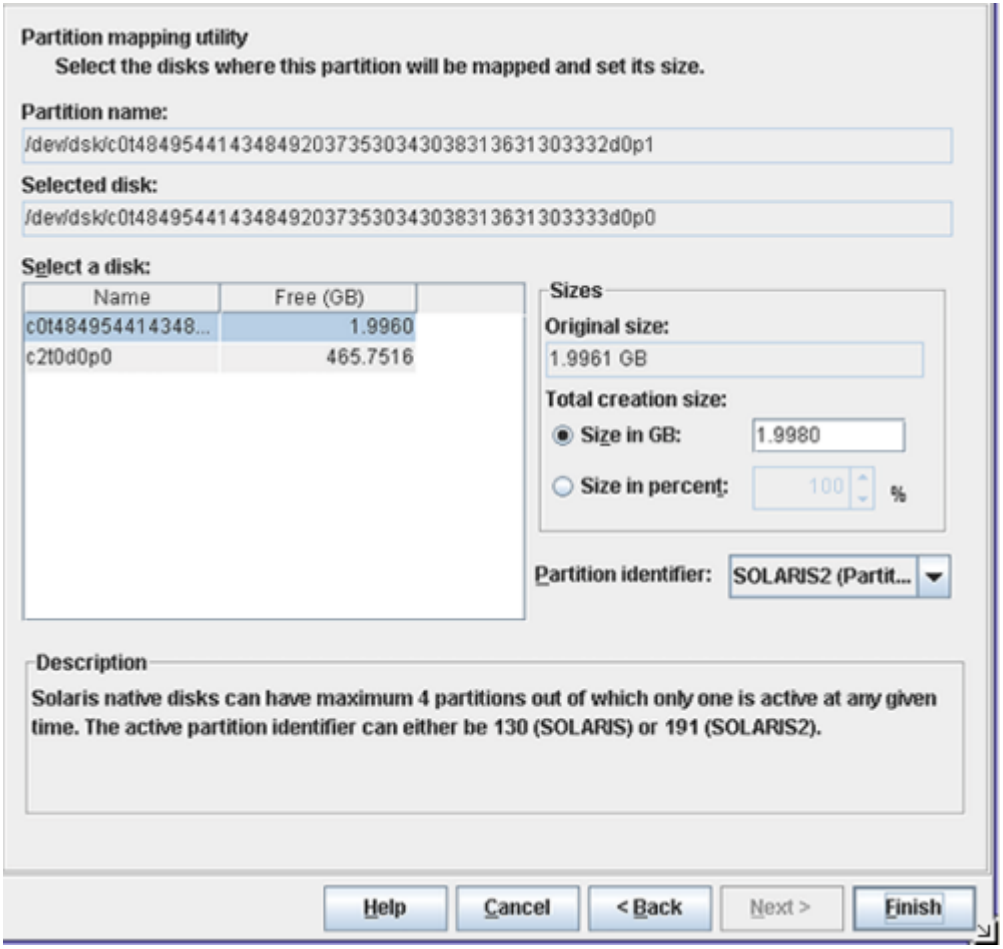
You can map the Solaris Native disk resource by using the disk mapping wizard. To map a disk using the mapping wizard, right-click a volume in the list and click **map**. The following is an example of Disk Mapping Wizard.



A **Partition** node appears under the **Native Disks** node. The following example shows the information regarding the partition name, partition state, partition length (size).



You can map the partition by using the mapping wizard. Right-click the Volume to launch the mapping wizard. You can map the source partition to destination disk and specify the percentage space of the destination disk to use for creating the partition.



About mapping and unmapping volumes

Wizards guide you through the mapping process; the appropriate wizard appears depending on what you select to map.

The mapping is saved between sessions, so you can stop mapping and then resume later. (If you map during a dissimilar disk restore process and you click **OK** to close the **Change Configuration** dialog box, the DDR restore process continues.)

If an element is mapped or unmapped, all the elements that are contained in it are mapped or unmapped.

The main options are as follows:

Initialize	Opens a dialog box where you can select a configuration to import into the **New Volume Layout** window. Only the disk information from the configuration is imported. Use this option to initialize the configuration with the layout of the new disks so you can begin mapping
Unmap All	Removes all mapped elements in the **New Volume Layout** and changes all elements in the **Original Volume Layout** window to **Unmapped**

Note: The mapping wizards do not let you reduce the size of a volume or partition to less than the required space to restore files.

The following notes apply to UNIX and Linux DDR:

- Shared disks in a cluster are marked restricted.
- Unused VxVM disks on Solaris clients are marked restricted.
- You cannot map Linux LVM volume groups with the physical volumes that are created on top of multi devices with the same configuration. The physical volumes are mapped to either disks or partitions but not a multi device.

The following notes apply to Windows DDR:

- The system drive is always mapped and cannot be moved; however, you can resize it if you map disks before the restore.
- Original disks and their volumes that were clustered cannot be mapped.
- The discovered disks that have the same disk signature as an original disk that was clustered cannot be mapped.

Table 10-10 describes possible volume mapping actions.

Table 10-10 Volume mapping actions

Action	Description
Initialize	Opens a dialog box from which you can select a configuration to import into the **New Volume Layout** window. Only the disk information from the configuration is imported.
Fast Map	Evaluates the original configuration and maps source disks to disks in the target configuration that have the necessary attributes.
Unmap All	Removes all mapped elements in the target configuration and changes all elements in the original configuration to **Unmapped**.

Table 10-10 Volume mapping actions *(continued)*

Action	Description
Map	Right-click an element in the **Table View of the Original Volume Layout** window and select **Map** from the shortcut menu. The mapping wizard starts for the selected element (except main element Disk Group, Disks, Volumes, Volume Sets, and so on).
Map Volume	Right-click a volume in the **Disk View of the Original Volume Layout** window and select **Map Volume** from the shortcut menu. The mapping wizard starts for the selected element.
Map Volume Group	Right-click a volume group in the **Disk View of the Original Volume Layout** window and select **Map Volume Group** from the shortcut menu. The mapping wizard starts for the selected element.
Map Disk	Right-click a disk in the **Disk View of the Original Volume Layout** window and select **Map Disk** from the shortcut menu. The mapping wizard starts for the selected element.
Map Disk Group	Right-click a disk group in the **Disk View of the Original Volume Layout** window and select **Map Disk Group** from the shortcut menu. The mapping wizard starts for the selected element.
Restrict	(Veritas Cluster Server only.) Right-click an element in the **Original Volume Layout** window and select **Restrict** from the shortcut menu.
Remove Restriction	Veritas Cluster Server only. Right-click an element in the **New Volume Layout** window and select **Restrict** from the shortcut menu to map the disk.

Mapping volumes

Use the following procedures to map volumes from the protected client to the restore configuration.

To initiate mapping for individual elements

1. In the **Table View** or **Disk View**, right-click the element in the **Original Volume Layout** window.
2. Choose the appropriate map option on the shortcut menu (the map options are context-sensitive).

   The Mapping Wizard starts with one of the following contexts, as appropriate:

Map	The Mapping Wizard starts for the selected element (except main element disk groups, disks, volumes, volume groups, and so on).
Map Volume	The Volume Mapping Wizard appears.
Map Volume Group	The Volume Group Mapping Wizard appears.
Map Disk	If the element is a disk in a disk group or a volume group, the disk group or volume group wizard appears. Then the volume mapping wizard for each volume appears (the required properties are set). The Disk Mapping Wizard appears if the element is as follows: ■ A disk that is not in a disk group ■ Not part of a volume group (AIX) ■ None of its volumes span other disks (mirrors, stripes). Then all the volumes and the file systems are populated into the target disk. The mapped state are set for both source elements and target elements (disks, volumes, and file systems)
Map Disk Group	The Disk Group Mapping Wizard appears.

To unmap an element

1. In the **Table** View or **Disk** View, right-click the element you want to unmap in the **New Volume Layout** window.
2. Click the unmap option on the shortcut menu. The unmap options are context-sensitive and include **Unmap**, **Unmap Disk**, **Unmap Volume**, and others.

   The element is unmapped, and the values of used and free space change accordingly.

To change the system volume size on Windows

1. In the **Table** View or **Disk** View, right-click the volume in the **New Volume Layout** window.
2. Click **Change Size** on the shortcut menu.
3. In the **Windows System Volume Size Change** dialog box, change the size of the volume.
4. Change the size of the volume.

To restrict a disk or remove restriction

1. In the **Table** View or **Disk** View, right-click the disk in the **New Volume Layout** window.
2. Click either **Restrict** or **Remove Restriction** on the shortcut menu to specify the following:
   - **Restrict** prevents a disk to be used as a target for mapping. Also, it is not formatted, and the volume groups or volumes on it are not created or restored.
   - **Remove Restriction** removes the restriction so the disk can be used as a target. If the disk is mapped, it is formatted and its volumes and volume groups are created and restored.

To promote a disk to dynamic on Windows

1. In the **Table** View or **Disk** View, right-click the disk in the **New Volume Layout** window.
2. Click **Promote to Dynamic** on the shortcut menu.

To add or remove a Windows system mirror

1. If the disk is a basic disk, promote it to a dynamic disk
2. In the **Table** View or **Disk** View, right-click the element in the **New Volume Layout** window.
3. Click either **Add Mirror** or **Remove Mirror** on the shortcut menu.
4. If you add a mirror, in the **Windows Add Mirror to System Volume** dialog box, select the disk to use for the mirror.
5. If you add a mirror, select the disk to use for the mirror.

Volumes views

The tree view (the left pane) shows the elements that are part of the disk layout. The elements in the tree change depending on the operating system of the client and the volume managers that are enabled. The tree view filters the details pane on the right. Select an element to display its attributes in the right pane and to filter other elements so they do not appear in the details pane.

The following indicators show an element's state throughout the mapping process:

Unmapped	The element is not mapped into the new configuration.
Mapped	The element is mapped into the new configuration.

Restricted	The disk is or was shared or manually restricted and cannot be used.

The details pane on the right contains the following views:

- The **Table View** shows the elements in an ordered list.
- The **Disk View** shows how every disk is organized. A colored bar indicates the type of storage layout. For extended partitions, the primary partition color appears in the top color bar and the extended color in a bottom bar. For soft partitions, the top bar shows the underlying volume or slice on which the soft partition was created.
- The **Pool View** shows how every file system and volume of ZFS pool is organized.

  Note: The pool view is added in NetBackup 7.5 to support ZFS-managed storage pools.

- The **Original Volume Layout** (the top window) shows the volume layout and the source elements (disks, disk groups, or volumes) in the original system. The amount of space that is used and the size of the disk appears. To view the properties for an element, right-click the element and select **Properties** on the shortcut menu.
- The **New Volume Layout** (the bottom window) shows the volume layout and elements for the target system. If you initialize the configuration with the layout from a discovered configuration, map elements from the **Original Volume Layout** to the **New Volume Layout**.

The following is the hierarchy for volume information:

- A disk group, volume group, or disk set contains disks.
- A disk contains volumes and partitions.
- A volume or a partition contains file systems.

All volume managers may not use all of these logical concepts. For example, a Solaris slice does not belong to a disk group and has only a file system.

The following tables show the various elements in the tree view and what appears in the **Table View** tab and **Disk View** tab.

Table 10-11 lists details about the selected Windows elements.

Table 10-11 Windows elements

Node	Appears in Table View	Appears in Disk View
Windows Disk Management	Disk and volumes	Not applicable.
Disks	All disks in the system.	All disks in the system.
Volumes	All the volumes that are defined in the system, both managed or unmanaged.	Disks that contain volumes, regardless of which volume manager created them.
One specific volume	Disks that the volume spans.	Disks that the volume spans.

Table 10-12 lists details about the selected Veritas Volume Manager elements.

Table 10-12 Veritas Volume Manager and Storage Foundation for Windows elements

Selected element	Appears in Table View	Appears in Disk View
Veritas Volume Manager	Disk groups, volume sets, and volumes.	Not applicable.
Disk groups	Disk groups in the configuration.	Disks that are part of any disk group.
A specific disk group	Disks that are part of that disk group.	Disks that are part of that disk group.
Volumes	All the volumes that Volume Manager manages.	Disks that contain Volume Manager volumes (ordered by disk group)
A specific volume	Disks that contain that volume.	Disks that contain that volume.

Table 10-13 lists details about the ZFS Manager elements.

Note: In NetBackup 7.5, BMR can also restore Solaris 10 clients that have ZFS storage pool attached.

Table 10-13 ZFS Manager elements

Selected Element	Appears in Table View	Appears in Pool View	Appears in Disk View
ZFS Manager	Not applicable	Not applicable	Not applicable
ZFS pools	Not applicable	Details of File systems and Volumes on each ZFS Pool	Details of disks associated with each ZFS Pool
ZFS file systems	Not applicable	Pool space consumption details of each selected ZFS File system	Not applicable
ZFS volumes	Not applicable	Pool space consumption details for each selected ZFS volume	Not applicable

Table 10-14 lists details about the selected Solaris Volume Manager elements.

Table 10-14 Solaris Volume Manager elements

Selected Element	Appears in Table View	Appears in Disk View
Solaris Volume Manager	Disk sets and volumes.	Not applicable.
Disk sets	All named (nonlocal) sets.	Disks that are part of a named (nonlocal) set (ordered by disk set).
A specific disk set	Disks that are part of that disk set.	Disks that are part of that disk set.
Volumes	All SVM volumes.	Disks that have SVM volumes.
A specific volume	Disks that include that volume.	Disks that include that volume.

Table 10-15 lists details about the selected non-managed Solaris elements.

Table 10-15 Non-managed Solaris elements

Selected element	Appears in Table View	Appears in Disk View
Non-managed	Disks and partitions.	Not applicable.
Disks	All disks that VxVM does not manage and all disks that are not in an SVM disk set.	All disks that VxVM does not manage and all disks that are not in an SVM disk set.

Table 10-15 Non-managed Solaris elements *(continued)*

Selected element	Appears in Table View	Appears in Disk View
Slices	All slices that are not managed and not used as SVM metadevices.	All disks that contain nonmanaged slices.

Table 10-16 lists details about the selected empty disks elements.

Table 10-16 Empty disks elements

Selected element	Appears in Table View	Appears in Disk View
Empty disks	Disks that are not used.	Disks that are not used.

Table 10-17 lists details about the AIX and HP-UX logical volume manager elements.

Table 10-17 AIX and HP-UX logical volume manager elements

Selected Element	Appears in Table View	Appears in Disk View
Logical volume manager	Volume groups and volumes.	Not applicable.
Volume groups	Volume groups in the configuration.	Disks that are part of any volume group (ordered by volume group).
A specific volume group	Disks that are part of that volume group.	Disks that are part of that volume group.
Volumes	All the volumes that the LVM manages.	Disks that have LVM volumes.
A specific volume	Disks that contain that volume.	Disks that contain that volume.

Chapter 11

Managing BMR boot servers

This chapter includes the following topics:

About boot servers

Boot servers provide the environment that is required to rebuild a protected client, including resources such as shared resource trees (SRT). Boot servers also provide the resources that are used to boot the client system when it performs a network boot before restore.

Boot server software is installed from the NetBackup installation media.

Boot server requirements

More information is available about the SRT requirements that are related to boot servers.

See "About shared resource trees" on page 103.

Table 11-1 Boot server requirements

Type of server	Requirements
General boot server	You must have a boot server for each type of client that you want to protect. For example, a Solaris client requires a Solaris boot server, a Windows client requires a Windows boot server, and so on. For UNIX, Linux, and legacy Windows restores, a boot server at a particular operating system version can only host SRTs of the same operating system version or lower. For example, a Solaris 9 boot server can host Solaris 8 and Solaris 9 SRTs, but not Solaris 10 SRTs. For UNIX, Linux, and legacy Windows restores, a client at a particular operating system version requires an SRT of the same operating system version.
AIX boot server	AIX boot servers do not have any special requirements. An AIX boot server can reside on the same subnet as the subnet of the client, or on a different subnet. However, AIX boot servers at a specific operating system version can only host SRTs of the same or earlier operating system version. For example, a 5.3.0.10 boot server can only host 5.1.x.x, 5.2.x.x, 5.3.0.0, and 5.3.0.10 SRTs, but not 5.3.0.20 SRTs. Likewise, a 5.2.x.x boot server cannot host 5.3.x.x SRTs.
HP-UX boot server	Each network segment with HP-UX clients must have an HP-UX boot server that can support the clients. On an HP-UX boot server, the Ignite version of an SRT must match the Ignite version that is installed on the boot server.
Linux boot server	Each network segment that has Linux clients must have a Linux boot server.

Table 11-1 Boot server requirements *(continued)*

Type of server	Requirements
Solaris boot server	Each network segment with Solaris clients must have a Solaris BMR boot server that can support the clients. However, you can use the following to minimize the effect of this requirement: ■ When necessary, you can install BMR boot server software on a Solaris computer in the network segment. Then create an SRT after the client has failed and needs to be restored. ■ The Solaris BMR boot server can be defined on a Solaris computer that has a physical IP presence on multiple networks. That is, you can use a single Solaris BMR boot server with multiple network interfaces for Solaris BMR clients on each network segment. ■ Configure a relay boot server to allow Solaris computers on remote subnets to boot from a BMR boot server using a network gateway. Contact your support representative for a Tech Note that describes the procedure. ■ The BMR boot server for Solaris10_x64 requires the following software installed: ■ TFTP Server ■ DHCP server ■ NFS Server ■ **SRTs** for carrying out a bare metal restore of a Solaris10_x64 client can only be created and hosted on a Solaris10_x64 Boot server. The OS and Kernel level should be greater than or the same of the client to be restored. If you want to use `bmrsrtadm` Media Creation to generate BMR-ISO SRTs, you must install the SUNWmkcd package on the boot server.
Windows boot server	Windows boot server requirements are as follows: ■ The network boot services on the boot server require a DHCP server somewhere on the network. ■ The boot server must not run a PXE service or a TFTP service.

About removing a boot server

You can remove a boot server by deactivating it or uninstalling it.

Chapter 12

Troubleshooting

This chapter includes the following topics:

Problems booting from CD or DVD

AIX, Linux, and Solaris platforms use a common bootable CD or DVD format (ISO-9660). HP-UX uses Logical Interchange Format (LIF). If a system cannot boot from the CD or DVD, place it in a system that has a CD drive and examine the contents. (Either UNIX or Windows platforms can read ISO format.)

Do the following:

- If the CD or DVD contents consist of a single file, the CD or DVD was written as a data CD or DVD instead of an ISO-9660 CD or DVD image. Repeat the burning procedure but use the options that are required to burn an ISO image file.
- If the CD or DVD is blank or unreadable, remove it from the drive and examine it closely to determine if it has been written to. Some CD or DVD burning software by default simulates the burning of a CD or DVD to test the capabilities of the CD or DVD burning hardware. It does not burn the CD or DVD until the

test-only option is turned off. Repeat the burning procedure with the test-only option disabled.

- If the boot was partially successful, or if it appears that some files are not present or some are corrupted, then one of the following occurred:
  - The burning process failed. A partially burned CD may be bootable but may not contain significant portions of its content. Lower the CD writing speed to allow a successful burn. Use the test after writing or use the option to verify that some CD writing software offers may help detect unsuccessful CD writes.
  - The file transfer from the BMR boot server to the computer with the CD writer failed.
    A common cause of corruption occurs when the file is transferred with FTP in ASCII transfer mode rather than binary mode.
- If the CD boots successfully on another similar computer, the drive on the restore system may be damaged or dirty. Similarly, the CD itself may be easily damaged or made unreadable by surface contamination after writing. Examine the physical media and the environment in which it is read.
- Verify that you use the correct procedures to boot the client computer from CD.
- Try booting the client from the installation media to ensure that the computer does not have a hardware problem when it boots from the CD.

Long restore times

If a restore takes an unusually long time (for example 20 hours instead of 2 hours), the media speed between the adapter and the switch or hub where it connects may not match. For example, the media speed is set to 100 MB full duplex, but the restore slows down because the hub uses half duplex. Change the media speed to match the hub speed or switch speed, or change the hub-switch setting to match that of the client.

Legacy restore fails on Windows client with multiple identical NICs

If a restore fails during the DOS portion of recovery on a Windows client with multiple identical NICs, the wrong network interface may be activated. (The BMR Restore Wizard displays a red X next to **Retrieving Client Information**.) DOS does not always identify PCI slot numbers in the same way that Windows does. Therefore, during the DOS restore portion, the following may happen: DOS may

not use the correct slot number for the NIC that is specified for the connection to the BMR boot server.

To resolve this problem, do one of the following:

- Move the network cable to the NIC that is active during DOS time. If you choose this solution, when BMR enters the Windows install phase, you must move the cable back to the original slot.
- Specify the slot number to use for the boot interface. For customized boot media, recreate the boot media and specify another slot number for the NIC. For generic boot media, specify the correct slot number during the enter client information phase.

  To identify the correct slot number, perform the following steps:

  - When the failure occurs (the BMR Restore Wizard displays a red X next to **Retrieving Client Information**), press the **F1** key to view error details.
  - Scroll up to see the output from when the DOS driver was loaded. In most cases, you can see the slot values that can be specified and the slot where the driver loaded.
  - Use the slot values to specify the slot number when you enter the client information. (Do this step either when you create the customized boot media or during the restore for generic boot media.) You may have to try each slot number until you use the correct one.
  - If you tried all of the slot numbers, the error may be due to DOS memory problems.
    See "Networking problems at DOS phase during legacy restore" on page 207.

Networking problems at DOS phase during legacy restore

BMR uses the following `config.sys` during the DOS phase while restoring a Windows client.

```
files=30
SHELL=A:\COMMAND.COM /P /E:4096
DEVICE=A:\BIN\IFSHLP.SYS
lastdrive=z
DEVICE=A:\BIN\HIMEM.SYS
DEVICE=A:\BIN\EMM386.EXE I=B000-B7FF NOEMS
DOS=HIGH,UMB
```

The following line in this file has significant implications:

```
DEVICE=A:\BIN\EMM386.EXE I=B000-B7FF NOEMS
```

Most machines function correctly when using EMM386, but some may not; see the following for corrective action:

- Some machines require that options be added to this line. The DOS phase of the restore may fail, which causes a red X to appear next to the following status lines: **Loading NIC Drivers**, **Starting Networking**, or **Retrieving Client Information**. Press **F1** to view the details; check the status screen for the following error:

  ```
  Error 8: There is not enough memory available.
  ```

  This error indicates that not enough memory is available to enable networking. To configure more memory, change this line to the following:

  ```
  DEVICE=A:\BIN\EMM386.EXE I=B000-B7FF I=E000-EFFF NOEMS
  ```

- Some machines require that the options be removed. Some gigabit network drivers may require the line to be changed to as follows:

  ```
  DEVICE=A:\BIN\EMM386.EXE
  ```

- Some machines require that the line be removed. Some combinations of BIOS and NIC drivers do not work well with EMM386, and the machine may hang while booting DOS. The system then does not respond to any key strokes or to **Ctrl**+**Alt**+**Delete**. For this problem, remove this line from the file.

Dissimilar system restore troubleshooting

Following are possible problems with hardware abstraction layer (HAL) differences warnings.

Problem	Near the end of the restore process, a warning about a different service pack level appears. The message asks if the user wants to copy the kernel files from the restore system to the restored system. The warning message appears when some kernel files are different between the restore environment and the restored system.

Cause	Required hot fixes are not present in the configuration.
Solution	If the restore is not a dissimilar system restore, click **Cancel**. If the restore is a dissimilar system restore, add hot fixes to the configuration and restart the restore. You may also install the hot fixes in the repair Windows installation and click Retry.

Following are possible problems with duplicate IP addresses on the network.

Problem	The client fails to start networking during DOS. The details show that the IP address is already in use.
Cause	The source system may still be on the network when the target system is restored.
Solution	Disconnect the source system from the network.

Solaris media boot network parameters issue

In a media boot of a Solaris client, the Solaris code polls the local subnet. The code polls to determine if any computer on the local subnet has a record of the network parameters for the booting client. If a JumpStart server has network parameters for the client in the `/etc/ethers` or `/etc/bootparams` file, those parameters are used for the boot process. The parameters are used even if they are different than the network parameters for the boot interface that are configured in BMR.

If network parameters for the client exist, the restore may fail.

To work around this issue, do one of the following:

- Remove all references to the client system from the following files in all other computers in the subnet of the client:

```
/etc/ethers file
/etc/bootparams
```

- Unplug the booting client from the network until the media boot configures the network parameters for the restore.

When recovering from deleting a client accidentally

If you delete a client and its current configuration, the next time the client is backed up, its configuration is saved. The client appears again in the **Bare Metal Restore Clients** view.

If the client and configuration are deleted after a client fails (before it is restored), use the `bmrs` command to retrieve the client's previous configuration. (You cannot perform a point in time restore because a deleted client does not appear in the **Bare Metal Restore Clients** view.)

The following is the format of the `bmrs` command to use on the master server:

```
bmrs -resource config -operation retrieve -client clientName
-destination newConfigname -enddate dateFormat -policy policyName
```

For more information about the `bmrs` command, see *NetBackup Commands*.

Chapter 13

Legacy Windows restore procedures

This chapter includes the following topics:

About legacy restores on Windows

This section provides details about the Legacy Restore procedure in NetBackup Bare Metal Restore.

Note: NetBackup Bare Metal Restore 6.5 introduced a Fast Restore process for Windows systems. This new simplified and faster process covers most system restores.

Use the legacy process in the following scenario:

- Restoration of system using Veritas Storage Foundation for Windows.

Installation, deployment, and backup operation is unchanged for systems requiring the Legacy Restore procedure.

The legacy process differs from normal operation in the following ways:

- A different SRT type

See "Creating a legacy shared resource tree" on page 213.

- A different type of boot media
  See "Creating CD boot media for a Windows client" on page 213.
- Completely different approach to the restore process

Using the legacy procedures, the boot media boots into WinPE and performs an automated installation of Windows onto the hard drive. This new temporary installation of Windows is automatically booted and the recovery process begins. From initial boot of the boot media to final reboot, the legacy restore procedure requires between five and eight system reboots.

Changes in the Legacy Restore function in BMR 7.0.1 and later versions

In BMR 7.0.1 and later versions, the Legacy Restore function is modified with the following changes:

- PC-DOS is no longer required to run a Legacy Restore. In BMR 7.0.1 and later versions, the Legacy Restore function boots from a WinPE boot image. This change in the boot process of the Legacy Restore option reduces maintenance and overheads.
  BMR 7.0.1 and later versions, you do not need to do the following tasks:
  - Download and store DOS extensions.
  - Maintain the floppy disks, which are now outdated as media.
  - Download and maintain DOS-compatible drivers.
  - Maintain Floppy Disk Drives (FDDs) for BMR Restore purpose.
- As a result of PC-DOS elimination, you do not need to create Boot Floppy. Therefore the Legacy Boot Floppy Wizard link on the Boot Server Assistant screen is removed.
- PC-DOS is replaced with WinPE, therefore the Legacy Restore can boot with the PXE-based network option.
- Unlike PC-DOS, WinPE does not require a 16-bit Windows Installer binary. Therefore, BMR 7.0.1 and later versions provide the Legacy Restore support also for the 64-bit editions of Windows.
- PC-DOS-based Legacy Restore requires approximately eight reboots during the restore. With WinPE-based Legacy Restore, the number of reboots is reduced to approximately five.

Note: With WinPE in place of PC-DOS, the Legacy Restore requires an additional free space of 2 GB to 4 GB in the system's boot partition. The boot partition is the one that contains the operating system.

Creating a legacy shared resource tree

Before a system can be restored with the Legacy Restore procedures, you must create a legacy style SRT.

The SRT Creation Wizard requests the following items:

- Windows Install media
- Windows License Key
- NBU client install package

To create a legacy shared resource tree

1. On the Windows BMR boot server, select **Programs > Symantec NetBackup > Bare Metal Restore Boot Server Assistant** from the **Start** menu. The **Bare Metal Restore Boot Server Assistant** panel appears.
2. Click **Shared Resource Tree Administration Wizard**.
3. Select the option for **Create a Bootable CD/DVD from a Shared Resource Tree**.
4. Select an SRT that is marked **(Legacy)**.

   If the SRT is the boot server that is an Active Directory Server, set the following security parameters to allow the legacy restore method to share SRTs with restoring clients:

   - **Microsoft network server: Digitally sign communications (always)** - Set to **Disabled**
   - **Microsoft network server: Digitally sign communications (if client agrees)** - Set to **Enabled**

Creating CD boot media for a Windows client

Before you begin a system restoration of a Windows system using the legacy procedures, you must first create a boot CD. The boot media automatically installs Windows from the SRT onto the hard drive of the system. The boot CDs access a copy of the CD that is copied to the CD itself. To create a media type, a legacy Windows SRT must already exist.

Note: In BMR 7.0.1 and later versions, floppy-based restore is not supported on Windows platform.

Before creating a bootable CD, verify that you have done the following:

- You have created a legacy SRT that matches the OS version to be restored. If you restore a Windows 2003 Server, you need a Windows 2003 Legacy SRT. To verify, navigate to the **Bare Metal Restore Management > Resources > Shared Resource Trees** tab on the NetBackup Administration Console. Legacy SRTs are flagged **(Legacy)** in the **Name** Column.

  Note: BMR 7.0.1 also supports Windows 2008 legacy restore.

- You have done a Prepare-To-Restore for the system to be restored. A legacy boot CD is customized for a specific BMR Client system to allow full automation. See "Preparing a client for restore" on page 54.

To create CD boot media for a Windows client

1. On the Windows BMR boot server, select **Programs > Symantec NetBackup > Bare Metal Restore - Boot Server Assistant** from the **Start** menu. The **Bare Metal Restore - Boot Server Assistant** screen appears.
2. Click **Shared Resource Tree Administration Wizard**.
3. Click **Next** on the **Welcome** panel.
4. Select the **Create a Bootable CD/DVD from a Shared Resource Tree** option and click **Next**.
5. Select an SRT that is marked **(Legacy)**.
6. Select the Client and Configuration to be restored.
7. Follow the prompts to create the boot media.

About restoring a system with legacy procedures

Before you start a restore, make sure that you have done a prepare-to-restore, created an SRT, and created the boot media.

Booting the legacy restore media

Use the procedure below to boot the client.

To boot the legacy restore media

- Insert the boot media in the appropriate drive and reboot the system.

  The BMR restore process loads from the boot media and begins the restore. The progress and status of the restore appear in a BMR status screen.

  - A yellow arrow indicates that the activity is currently in progress.
  - A green check marks each activity as it completes.
  - A red X indicates a failed activity.

  At any time, press **F1** to see more information about the current process or press **Esc** to quit. The **F1** or **Esc** keys are processed only after the current step completes.

About using the BMR Restore Utility

After the temporary Windows installation, the system reboots and the BMR Restore Utility appears. This utility creates all the required partitions, formats them, and restores the files in each of the partitions. The **Details** box of the **Restore Utility** screen shows details about the current task in progress.

Note: If NetBackup access management is used in your environment, provide the proper credentials when prompted so that NetBackup can restore the client files.

Each task is checked as it completes. A red X indicates failure; if a failure occurs, a Retry wizard appears that shows the tasks to be retried. Before you retry a task, examine the restore log to determine the reasons for failure and correct the problem accordingly.

About restoring to dissimilar disks for Windows clients

To restore a system whose disks are different, you may edit a configuration on the server first, which may cause a fully automated restoration. Or, you may start a restore and allow BMR to detect the different disks. If the new disks do not support the original disk layout, BMR automatically launches the Dissimilar Restore Mapping utility during the restore process.

For procedures to edit a configuration before starting a restore, see Modifying a configuration.

Loading only the boot partition driver during the boot phase

Windows systems often use more than one mass storage device (MSD) driver. However, only one of them is associated with the boot partition of the drive where Windows is installed.

By default, BMR loads all MSD drivers during the boot phase of the restore. You can edit the configuration so that only the driver that is associated with the boot partition is loaded. Do so if the loading all of the MSD drivers interferes with the boot process of the restore.

The system drive is always mapped and cannot be moved. However, you can resize it if you map disks before the restore.

To load only the boot partition driver during the boot phase

1. In the **Device & Drivers** dialog box, select the correct driver from the bottom box, and click **Change**.
2. Check that the box labeled **Bootable driver to be used during text mode portion of the installation**.
3. Click **OK**.

Index

D

E

H

I

J

L

M

N

O

P

T

U

V

W

Z