VERITAS NetBackup Bare Metal Restore™ 6.0

System Administrator’s Guide

for UNIX, Windows, and Linux
**Disclaimer**

The information contained in this publication is subject to change without notice. VERITAS Software Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VERITAS Software Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

**VERITAS Legal Notice**

Copyright © September 2005 VERITAS Software Corporation. All rights reserved. VERITAS, the VERITAS Logo, and Bare Metal Restore are trademarks or registered trademarks of VERITAS Software Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Portions of this software are derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm. Copyright 1991-92, RSA Data Security, Inc. Created 1991. All rights reserved.

VERITAS Software Corporation
350 Ellis Street
Mountain View, CA 94043
USA
Phone 650-527-8000
Fax 650-527-2908
www.veritas.com

**Third-Party Copyrights**

For a list of third-party copyrights, see the *NetBackup Release Notes* appendix.
# Contents

**Preface** ......................................................... 13
- Getting Help .................................................. 13
  - Finding NetBackup Documentation ............................. 13
  - Accessing the VERITAS Technical Support Web Site .......... 13
  - Contacting VERITAS Licensing ............................... 15
- Accessibility Features .......................................... 15
- Comment on the Documentation ................................. 16

**Chapter 1. Introducing Bare Metal Restore** .......................... 1
- Bare Metal Restore Overview ..................................... 1
- Bare Metal Restore Management Window ......................... 3
- Terminology ...................................................... 3

**Chapter 2. Planning Deployment** ................................... 5
- Identifying the Systems to Protect ................................ 5
- Determining Shared Resource Tree Requirements ................ 5
- Choosing Boot Servers ............................................ 6
- Worksheets ......................................................... 6
  - BMR Boot Server Worksheet ...................................... 7
  - Network Topology Worksheet .................................... 9
- Network Topology Worksheet ...................................... 9
- Network Topology Worksheet ...................................... 10
- Shared Resource Tree Worksheet ................................ 11
- Shared Resource Tree Worksheet ................................ 12
Chapter 3. Installing Bare Metal Restore .......................................... 13
Before Installing BMR ............................................................... 13
Supported Systems ................................................................. 13
Cluster Environments .............................................................. 14
UNIX and Linux Systems ......................................................... 14
  BMR Master Server on UNIX and Linux Systems ....................... 14
    Installation Prerequisites for UNIX and Linux Systems .......... 14
    Installing the BMR Master Server on a UNIX or Linux System ... 15
    Uninstalling the BMR Master Server from a UNIX or Linux System ... 16
  BMR Boot Server on UNIX and Linux Systems ......................... 18
    Boot Server Installation Prerequisites for UNIX and Linux Systems ... 18
    BMR Boot Server in a UNIX Cluster ...................................... 20
    Installing a BMR Boot Server on a UNIX or Linux System ....... 21
    Uninstalling a BMR Boot Server from a UNIX or Linux System ... 22
  BMR Client Software on UNIX and Linux Systems .................... 24
    Client Installation Prerequisites for Linux Systems ............... 24
Microsoft Windows Systems ....................................................... 24
  BMR Master Server on Windows Systems .................................. 24
    Licensing Prerequisites for Windows Systems ....................... 25
    Licensing the BMR Master Server on a Windows System .......... 25
    Uninstalling the BMR Master Server from a Windows System ....... 27
  BMR Boot Server on Windows Systems ..................................... 29
    Boot Server Installation Prerequisites for Windows Systems .... 29
    BMR Boot Server in a Windows Cluster .................................. 29
    Installing a BMR Boot Server on a Windows System ............... 30
    Uninstalling a BMR Boot Server from a Windows System .......... 35
  BMR Client Software on Windows Systems ................................ 37
Migrating from BMR 4.7 ........................................................... 37
  Steps for Migrating to NetBackup BMR 6.0 ............................... 37
    Stopping and Starting the BMR 4.7 Server Daemon .................. 39
Converting External Procedures ........................................ 39
Modify the External Procedure Scripts ................................. 40
Adding External Procedures to the BMR Database .................. 40
Decommissioning BMR 4.7 ................................................... 40
Uninstalling BMR 4.7 Clients .............................................. 41

Chapter 4. Monitoring Activity .............................................. 43
Monitoring Backup Jobs ..................................................... 43
Monitoring BMR Tasks .................................................... 44
Viewing BMR Logs .......................................................... 46
BMR Logging Originator IDs ............................................... 47
Configuring and Using Logging .......................................... 48
Restore Logs ................................................................. 49

Chapter 5. Protecting Clients ................................................ 51
Back Up the Client .......................................................... 51
Configuring Policies to Back Up BMR Clients ......................... 52
Perform Complete Backups ............................................... 53
Perform a Full Backup After a Restore ................................ 53
Ensure Successful Backups ............................................... 54
Save Custom Files ......................................................... 54
Monitor Backups ........................................................... 55
Use the ALL_LOCAL_DRIVES Directive .............................. 55
Use the Same Client Name in Multiple Policies ....................... 55
Configure NetBackup Properties ....................................... 55

Chapter 6. Setting Up Restore Resources .................................. 57
Install Boot Server Software .............................................. 57
Create Shared Resource Trees .......................................... 58
Add Client Resources ................................................... 58
Create Boot Media ......................................................... 58
Chapter 7. Restoring Clients ...................................................... 61

    Restore Process Overview ............................................... 62
    Preparing to Restore a Client ........................................... 64
        Prepare to Restore Client Dialog Box ............................. 65
        Understanding BMR Disk Recovery Behavior ...................... 66
    Restoring UNIX and Linux Clients ..................................... 70
        Restoring UNIX and Linux Clients Using Network Boot ...... 71
            AIX Network Boot .............................................. 71
            HP-UX Network Boot .......................................... 72
            Linux Network Boot .......................................... 74
            Solaris Network Boot ......................................... 74
        Restoring UNIX and Linux Clients Using Media Boot ......... 75
            AIX Media Boot .............................................. 75
            HP-UX Media Boot .......................................... 76
            Linux Media Boot .......................................... 77
            Solaris Media Boot ......................................... 78
    Restoring Windows Clients .............................................. 79
        Preparing for a Windows Restore .................................. 79
        Booting the Client ............................................... 80
            PXE Boot .................................................... 81
        Entering Client Information ...................................... 81
        Entering Partition Information ................................... 83
            Identifying the Vendor Partition During a Restore ........ 85
        Installing Windows into a Temporary Location ................ 86
        Rebuilding Partitions and Restoring Files ........................ 87
    Restoring to a Specific Point in Time ................................. 88
        Understanding the Point in Time Restore Process .............. 88
        When to Use Point in Time Restore ................................ 89
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a Point in Time Restore Configuration</td>
</tr>
<tr>
<td>Restoring to Dissimilar Disks</td>
</tr>
<tr>
<td>Understanding the Dissimilar Disk Restore Process</td>
</tr>
<tr>
<td>When to Use Dissimilar Disk Restore</td>
</tr>
<tr>
<td>Restoring to Dissimilar Disks for UNIX and Linux Clients</td>
</tr>
<tr>
<td>Creating a Restore Configuration for DDR</td>
</tr>
<tr>
<td>Restoring to Dissimilar Disks</td>
</tr>
<tr>
<td>Restoring to Dissimilar Disks for Windows Clients</td>
</tr>
<tr>
<td>Creating a Restore Configuration for DDR</td>
</tr>
<tr>
<td>Restoring to Dissimilar Disks</td>
</tr>
<tr>
<td>Restoring to a Dissimilar System</td>
</tr>
<tr>
<td>When to Use Dissimilar System Restore</td>
</tr>
<tr>
<td>Restoring to a Dissimilar System</td>
</tr>
<tr>
<td>Determining Hardware Differences</td>
</tr>
<tr>
<td>Creating an Editable DSR Configuration</td>
</tr>
<tr>
<td>Adding NIC and MSD Drivers</td>
</tr>
<tr>
<td>Adding Windows Hotfixes</td>
</tr>
<tr>
<td>Changing Network Interfaces</td>
</tr>
<tr>
<td>Mapping Disks</td>
</tr>
<tr>
<td>Creating Boot Media</td>
</tr>
<tr>
<td>Restoring the Client</td>
</tr>
<tr>
<td>First Logon</td>
</tr>
<tr>
<td>Restoring NetBackup Media Servers</td>
</tr>
<tr>
<td>Configuring an Alternate Media Server</td>
</tr>
<tr>
<td>Configuring Automatic Media Server Failover</td>
</tr>
<tr>
<td>Overriding the Original Media Server Manually</td>
</tr>
<tr>
<td>Restoring the Media Server</td>
</tr>
<tr>
<td>Restoring BMR Boot Servers</td>
</tr>
<tr>
<td>Using External Procedures</td>
</tr>
<tr>
<td>External Procedure Points and Names</td>
</tr>
</tbody>
</table>
Chapter 8. Managing Shared Resource Trees .................. 123

Shared Resource Tree Overview ................................ 123
Shared Resource Trees View .................................... 124
Creating a Shared Resource Tree ............................... 126
<table>
<thead>
<tr>
<th>Chapter 9. Managing Boot Media</th>
<th>153</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot Media Overview</td>
<td>153</td>
</tr>
<tr>
<td>About Writing a CD</td>
<td>154</td>
</tr>
<tr>
<td>Creating Boot Media for UNIX and Linux</td>
<td>155</td>
</tr>
<tr>
<td>Creating Boot Media for AIX</td>
<td>156</td>
</tr>
<tr>
<td>Creating Boot Media for HP-UX</td>
<td>157</td>
</tr>
<tr>
<td>Creating Boot Media for Linux</td>
<td>157</td>
</tr>
<tr>
<td>Creating an SRT for UNIX or Linux</td>
<td>128</td>
</tr>
<tr>
<td>Creating an AIX SRT</td>
<td>128</td>
</tr>
<tr>
<td>Creating an HP-UX SRT</td>
<td>130</td>
</tr>
<tr>
<td>Creating a Solaris SRT</td>
<td>132</td>
</tr>
<tr>
<td>Creating a Linux SRT</td>
<td>134</td>
</tr>
<tr>
<td>Creating an SRT for Windows</td>
<td>136</td>
</tr>
<tr>
<td>Adding Software to a Shared Resource Tree</td>
<td>137</td>
</tr>
<tr>
<td>Adding Software to a UNIX or Linux SRT</td>
<td>138</td>
</tr>
<tr>
<td>Adding NetBackup Maintenance Packs</td>
<td>139</td>
</tr>
<tr>
<td>Adding VERITAS Volume Manager and File System</td>
<td>140</td>
</tr>
<tr>
<td>Adding VERITAS Security Services</td>
<td>141</td>
</tr>
<tr>
<td>Adding Other Software</td>
<td>141</td>
</tr>
<tr>
<td>Adding Software to a Windows SRT</td>
<td>142</td>
</tr>
<tr>
<td>Using a Shared Resource Tree Exclusively</td>
<td>143</td>
</tr>
<tr>
<td>Copying a Shared Resource Tree</td>
<td>145</td>
</tr>
<tr>
<td>Copying an SRT on UNIX and Linux</td>
<td>145</td>
</tr>
<tr>
<td>Copying an SRT on Windows</td>
<td>146</td>
</tr>
<tr>
<td>Repairing a Damaged Shared Resource Tree</td>
<td>147</td>
</tr>
<tr>
<td>Breaking a Stale Shared Resource Tree Lock</td>
<td>148</td>
</tr>
<tr>
<td>Deleting a Shared Resource Tree</td>
<td>150</td>
</tr>
<tr>
<td>Deleting an SRT on UNIX and Linux</td>
<td>150</td>
</tr>
<tr>
<td>Deleting an SRT on Windows</td>
<td>151</td>
</tr>
</tbody>
</table>
Creating Boot Media for Solaris ................................. 157
Creating Boot Media for Windows ................................ 158
Rewriting an Archived Boot Floppy .............................. 160
Archived Boot Floppies View ..................................... 160

Chapter 10. Managing Windows Packages .................... 163
Packages Overview .................................................. 163
Packages View ....................................................... 164
Adding a Windows Software Package .......................... 165
Finding the Correct Driver ....................................... 166
Deleting a Windows Software Package ....................... 166

Chapter 11. Managing Clients and Configurations .......... 167
Client Configuration Overview ................................ 167
Bare Metal Restore Clients View ............................... 168
Discovered Configurations View ............................... 170
Copying a Configuration .......................................... 172
New Configuration Dialog Box ................................. 172
Discovering a Configuration ..................................... 174
Prepare to Discover Dialog Box ............................. 175
Modifying a Configuration ....................................... 177
Deleting a Configuration ........................................ 178
Deleting a Client .................................................. 179
Change Configuration Dialog Box ............................ 180
Configuration Summary .......................................... 181
Drivers .............................................................. 183
Bootable Windows Drivers .................................... 184
Discovered Windows Driver Signing ......................... 185
Hosts ................................................................. 186
Hotfixes .............................................................. 188
Network Interfaces .................................................. 190
Importing and Mapping Interfaces ........................................... 191
Changing Interfaces Manually .............................................. 192
UNIX and Linux Boot Interface ............................................ 193
Network Routes .............................................................. 194
Volumes ............................................................................. 196
Mapping and Unmapping Volumes ........................................ 197
Understanding the Views ..................................................... 199

Chapter 12. Managing Boot Servers ........................................ 203
Boot Server Requirements ................................................... 203
General Boot Server Requirements ..................................... 203
HP-UX Boot Server Requirements ..................................... 204
Linux Boot Server Requirements ....................................... 204
Solaris Boot Server Requirements ..................................... 204
Boot Servers View ............................................................. 204
Removing a Boot Server ..................................................... 205

Chapter 13. Troubleshooting .................................................... 207
Problems Booting from CD .................................................. 207
Long Restore Times ........................................................... 208
Restore Fails on Windows Client with Multiple Identical NICs ... 208
Networking Problems at DOS Phase During Restore ............. 209
DSR Troubleshooting .......................................................... 210
Solaris Media Boot Network Parameters Issue .................... 211
To Recover from Deleting a Client Accidentally .................... 211

Index ................................................................................. 213
Preface

This guide describes how to install, configure, and use VERITAS NetBackup Bare Metal Restore™. In this guide, Bare Metal Restore is referred to as Bare Metal Restore or BMR. This document is the same as NetBackup_AdminGuide_BMR.pdf distributed with the Bare Metal Restore software.

Getting Help

You can find answers to questions and get help from the NetBackup documentation and from the VERITAS technical support web site.

Finding NetBackup Documentation

A list of the entire NetBackup documentation set appears as an appendix in the NetBackup Release Notes. All NetBackup documents are included in PDF format on the NetBackup Documentation CD.

For definitions of NetBackup terms, consult the online glossary.

▼ To access the NetBackup online glossary

1. In the NetBackup Administration Console, click Help > Help Topics.
2. Click the Contents tab.
3. Click Glossary of NetBackup Terms.
   Use the scroll function to navigate through the glossary.

Accessing the VERITAS Technical Support Web Site

The address for the VERITAS Technical Support Web site is http://support.veritas.com.

The VERITAS Support Web site lets you do any of the following:
Getting Help

- Obtain updated information about Bare Metal Restore, including system requirements, supported platforms, and supported peripherals
- Contact the VERITAS Technical Support staff and post questions to them
- Get the latest patches, upgrades, and utilities
- View the Bare Metal Restore Frequently Asked Questions (FAQ) page
- Search the knowledge base for answers to technical support questions
- Receive automatic notice of product updates
- Find out about Bare Metal Restore training
- Read current white papers related to Bare Metal Restore

From http://support.veritas.com, you can complete various tasks to obtain specific types of support for Bare Metal Restore:

1. Subscribe to the VERITAS Email notification service to be informed of software alerts, newly published documentation, Beta programs, and other services.

   a. From the main http://support.veritas.com page, select a product family and a product.

   b. Under Support Resources, click Email Notifications.

      Your customer profile ensures you receive the latest VERITAS technical information pertaining to your specific interests.

2. Locate the telephone support directory at http://support.veritas.com by clicking the Phone Support icon. A page appears that contains VERITAS support numbers from around the world.

**Note** Telephone support for Bare Metal Restore is only available with a valid support contract. To contact VERITAS for technical support, dial the appropriate phone number listed on the Technical Support Guide included in the product box and have your product license information ready for quick navigation to the proper support group.

3. Contact technical support using e-mail.
a. From the main http://support.veritas.com page, click the E-mail Support icon. A wizard guides you to do the following:
   ♦ Select a language of your preference
   ♦ Select a product and a platform
   ♦ Provide additional contact and product information, and your message
   ♦ Associate your message with an existing technical support case

b. After providing the required information, click Send Message.

Contacting VERITAS Licensing
For license information, you can contact us as follows:
   ♦ Call 1-800-634-4747 and select option 3
   ♦ Fax questions to 1-650-527-0952
   ♦ In the Americas, send e-mail to amercustomercare@veritas.com.
     In the Asia and Pacific areas, send email to apaccustomercare@veritas.com.
     In all other areas, send email to internationallicense@veritas.com.

Accessibility Features
NetBackup contains features that make the user interface easier to use by people who are visually impaired and by people who have limited dexterity. Accessibility features include:
   ♦ Support for assistive technologies such as screen readers and voice input (Windows servers only)
   ♦ Support for keyboard (mouseless) navigation using accelerator keys and mnemonic keys

For more information, see the NetBackup Installation Guide.
Comment on the Documentation

Let us know what you like and dislike about the documentation. Were you able to find the information you needed quickly? Was the information clearly presented? You can report errors and omissions or tell us what you would find useful in future versions of our manuals and online help.

Please include the following information with your comment:

◆ The title and product version of the manual on which you are commenting
◆ The topic (if relevant) on which you are commenting
◆ Your comment
◆ Your name

Email your comment to NBDocs@veritas.com.

Please only use this address to comment on product documentation. See “Getting Help” in this preface for information on how to contact Technical Support about our software.

We appreciate your feedback.
Introducing Bare Metal Restore

NetBackup protects client systems by backing them up using a policy that is configured for Bare Metal Restore (BMR) protection. Bare Metal Restore rebuilds clients after failure so that NetBackup can restore the original files.

To plan your deployment of BMR, see:
- “Planning Deployment” on page 5

The BMR master server must be installed and licensed so that clients can be protected. For procedures, see:
- “Installing Bare Metal Restore” on page 13

For information about how to protect clients, see:
- “Protecting Clients” on page 51

After clients are protected, you can set up the resources necessary to restore them:
- “Setting Up Restore Resources” on page 57

You can restore clients by using the procedures documented in the following:
- “Restoring Clients” on page 61

Related Topics
- “Bare Metal Restore Overview” on page 1
- “Bare Metal Restore Management Window” on page 3
- “Terminology” on page 3

Bare Metal Restore Overview

BMR automates system recovery by restoring the operating system, the system configuration, and all system and data files with two steps:

1. Run one command from the NetBackup master server.
2. Reboot the client. Separate system backups or reinstallations are not required.
A BMR protection domain consists of:

- 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 than manages BMR operations.

- Media servers. NetBackup media servers control storage devices on which the client files are stored.

- Boot servers. Boot servers provide the environment that is required to rebuild a protected client, including resources such as shared resource trees (SRT). Shared resource trees contain the operating system software and the NetBackup client software that are used to rebuild the protected system so that NetBackup can restore the original files. For UNIX and Linux systems, a boot server also provides the resources used to boot the client system when it performs a network boot prior to restore.

- 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 machine, on a separate machine, or on a combination of machines.

Example of BMR Protection Domain
Bare Metal Restore Management Window

The **Bare Metal Restore Management** view of the NetBackup Administration Console shows the protected clients, the resources used to rebuild protected clients, and the 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.

### Terminology

The following terminology is used in Bare Metal Restore.

**boot server**

A server that contains the resources to boot a client, rebuild the client system, and begin a restore or a discovery.
Terminology

client configuration
A collection of information about the system, including the number of disk drives, volume and file system information, number and type of network adapters, network properties, drivers, and other system software components. Most BMR operations are performed on configurations; a configuration is the template used to rebuild a protected system.

discovery boot
A non-intrusive boot that collects device and disk layout information.

dissimilar disk restore (DDR)
The capability to restore to a machine that has a different disk configuration than the original machine.

dissimilar system restore (DSR)
The capability to restore a machine into a complete different hardware (Windows only).

media boot
The process of booting a client using a CD that contains the shared resource tree.

prepare to discover
Operation that runs on the master server and prepares all the resources necessary to do a discovery boot of a client.

prepare to restore
Operation that runs on the master server and prepares all the resources necessary to restore the client.

protection domain
A logical grouping of Bare Metal Restore servers and clients that includes one BMR master server, one or more BMR boot servers, and one or more protected clients.

restore configuration
The client configuration used to restore a client. You may have to modify the restore configuration so you can restore to dissimilar disks or to a different system.

shared resource tree (SRT)
A source of system resources, including the means to rebuild the client system and restore all system files.
Planning Deployment

BMR deployment planning includes:

- “Identifying the Systems to Protect” on page 5
- “Determining Shared Resource Tree Requirements” on page 5
- “Choosing Boot Servers” on page 6

Worksheets are available to help with deployment planning. For more information, see:

- “Worksheets” on page 6

Identifying the Systems to Protect

You can include systems that run specific levels of the AIX, HP-UX, Solaris, Linux, or Windows operating systems as clients in your BMR installation. A BMR client can be a server for other applications or processes.

For information about supported systems, dependencies, limitations, and operating system installation prerequisites for BMR, see the NetBackup Release Notes.

Determining Shared Resource Tree Requirements

Shared resource trees (SRTs) provide resources to rebuild protected clients.

For general SRT requirements, see “Shared Resource Tree Overview” on page 123.

For information about SRT and boot server versions, see Supported Platforms and Peripherals > NetBackup Add-on Products > NetBackup Bare Metal Restore > BMR Shared Resource Tree Versions in the NetBackup Release Notes.

The “Shared Resource Tree Worksheet” on page 11 provides guidance on gathering information for creating SRTs on your BMR boot servers.
Choosing Boot Servers

Boot servers host the shared resource trees used to rebuild protected clients.

Before choosing the machines on which to install the boot servers, review “Boot Server Requirements” on page 203.

For information about systems on which you can install boot servers, see Supported Platforms and Peripherals > NetBackup Add-on Products > NetBackup Bare Metal Restore > BMR Supported Operating Systems in the NetBackup Release Notes.

Worksheets

The following worksheets and worksheet instructions are designed to help you plan your installation:

◆ “BMR Boot Server Worksheet” on page 7
◆ “Network Topology Worksheet” on page 9
◆ “Shared Resource Tree Worksheet” on page 11
BMR Boot Server Worksheet

Use this worksheet to track your BMR servers and their corresponding operating systems.

For each Network Segment IP on the Topology Worksheet, record the information for it in the Network Segment IP column of the BMR Boot Server Worksheet.

In the Link Speed column, place the end-to-end network bandwidth speed from the network containing the BMR server. For example, if a network segment is located at a remote location accessed via a Frame Relay 56K link, the Link Speed column should be 56K, even though the network segment itself and the network segment containing the BMR server are both high-speed networks.

Then, for each segment determine the number of the different types of BMR clients in that network segment. If a BMR client has multiple network interfaces, count it only once; choose an interface from which it can network boot (UNIX or Linux) to minimize the number of SRTs required. For example, if there are several Solaris machines with multiple interfaces, each having an interface on a single common network segment, count each machine once as being in the common network segment, and do not count the machines again in the other network segment.
### BMR Boot Server Worksheet

Page ___ of ___

<table>
<thead>
<tr>
<th>Network Segment IP</th>
<th>Link Speed</th>
<th>AIX</th>
<th>HP-UX</th>
<th>Linux</th>
<th>Solaris</th>
<th>Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>5.1</td>
<td>5.2</td>
<td>11.10</td>
<td>11.11</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Red Hat 3.0</td>
<td>SuSE 8</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>9</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>XP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Server 2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Network Topology Worksheet

Use this worksheet to describe the network topology of the NetBackup environment.

- **Network Segment IP column.** For each network interface from which the BMR clients can network boot, determine the network segment IP address. The network segment IP address is the dotted decimal IP of the Network Segment. For example, if the client network IP address is 198.3.130.100 and the netmask is 255.255.255.0, the network segment IP address is 198.3.130.0. For each unique network segment IP address, place an entry in the **Network Segment IP** column of the Network Topology Worksheet. For Windows clients, include the network interface's network segment that will be used during a floppy disk or CD boot.

- **The Gateway to NetBackup Server column** is the IP address of a router in this segment that can be used to reach the NetBackup server. If the NetBackup server has a presence on this network, no gateway is required.

- **The Gateway to other Networks column** should contain the IP addresses of the other router interfaces on this segment that can be used to reach other networks.
## Network Topology Worksheet

Page ___ of ___

<table>
<thead>
<tr>
<th>Network Segment IP</th>
<th>Gateway to NetBackup Server</th>
<th>Gateways to other Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Shared Resource Tree Worksheet

Make copies of the Shared Resource Tree Worksheet. For each selected machine designated to be a BMR boot server, fill out a Shared Resource Tree Worksheet. If more than one SRT is to be defined on a BMR boot server, use a separate form for each SRT. Place the BMR boot server’s host name and operating system version in the first two rows of the form.

Fill in all of the network segment IP addresses that the SRT will serve into the Network Segment IP’s Served section.

In the SRT OS and Version table, place the version of the operating system needed to create the SRT. This corresponds to the operating system on the BMR clients protected by the SRT. The NetBackup Client Version is the version of the NetBackup client software to be installed into the SRT.
### Shared Resource Tree Worksheet

<table>
<thead>
<tr>
<th>BMR Boot Server Host Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>BMR Boot Server OS and Version</td>
<td></td>
</tr>
<tr>
<td>Network Segment IP’s Served</td>
<td></td>
</tr>
</tbody>
</table>

### SRT OS and Version

<table>
<thead>
<tr>
<th>SRT OS and Version</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NetBackup Client Version</td>
<td></td>
</tr>
</tbody>
</table>

### VERITAS Software Information

<table>
<thead>
<tr>
<th>Other VERITAS Software Used by BMR Clients</th>
<th>VERITAS Volume Manager</th>
<th>Version:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VERITAS File System</td>
<td>Version:</td>
</tr>
</tbody>
</table>

### Third Party Disk Device Driver and Volume Manager Information

<table>
<thead>
<tr>
<th>Third Party Software or Drivers Used by BMR Clients</th>
<th>OEM Network Drivers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OEM Disk Drivers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td></td>
</tr>
</tbody>
</table>

### Location of Images for SRT Creation

<table>
<thead>
<tr>
<th>OS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NetBackup Client</td>
<td></td>
</tr>
<tr>
<td>Third Party Software</td>
<td></td>
</tr>
<tr>
<td>Network Driver</td>
<td></td>
</tr>
<tr>
<td>Disk Drivers</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
<tr>
<td>Windows License Key</td>
<td></td>
</tr>
</tbody>
</table>
Installing Bare Metal Restore

Bare Metal Restore includes the following software components:
- A master server that controls the operation of BMR.
- Boot server software that manages and provides the resources used to rebuild systems.
- Client software that is installed when the NetBackup client software is installed. No special installation or configuration is required.

This chapter contains instructions for installing and uninstalling BMR and information about migrating from previous BMR releases.

Topics
- “Before Installing BMR” on page 13
- “Supported Systems” on page 13
- “UNIX and Linux Systems” on page 14
- “Microsoft Windows Systems” on page 24
- “Migrating from BMR 4.7” on page 37

Before Installing BMR

Before installing BMR software, read the NetBackup Release Notes, which contains information about dependencies, limitations, and operating system installation prerequisites for BMR.

Supported Systems

For information about supported systems, see Supported Platforms and Peripherals > Other NetBackup Compatibility Lists > NetBackup Bare Metal Restore in the NetBackup Release Notes.
Cluster Environments

For information about supported cluster environments, see Supported Platforms and Peripherals > Other NetBackup Compatibility Lists > NetBackup Bare Metal Restore in the NetBackup Release Notes.

UNIX and Linux Systems

For information about installing the BMR components, see the following:

- “BMR Master Server on UNIX and Linux Systems” on page 14
- “BMR Boot Server on UNIX and Linux Systems” on page 18
- “BMR Client Software on UNIX and Linux Systems” on page 24

BMR Master Server on UNIX and Linux Systems

To install the Bare Metal Restore master server, see the following instructions. Install the BMR master server before you install BMR boot servers.

After you install and license the BMR master server and configure NetBackup so that back ups can occur, you can protect clients.

Tasks

- “Installing the BMR Master Server on a UNIX or Linux System” on page 15
- “Uninstalling the BMR Master Server from a UNIX or Linux System” on page 16

Related Topics

- “Installation Prerequisites for UNIX and Linux Systems” on page 14

Installation Prerequisites for UNIX and Linux Systems

The following are installation prerequisites:

- The BMR master server must be installed on the same system as the NetBackup master server in your environment, and you must install the same version of BMR as NetBackup. The BMR master server cannot be installed on a NetBackup media server or on a NetBackup client.

- The NetBackup master server must be installed before you can install the BMR master server. For instructions about installing NetBackup, see the NetBackup Installation Guide for UNIX and Linux.
◆ You must have a valid BMR license key.
◆ For information about operating system installation prerequisites for BMR, see the 
  NetBackup Release Notes.
◆ The compat-libstdc++ library is required on RedHat Linux 3.0 systems. Refer to 
  your Linux distribution documentation to locate this library.
◆ If a BMR main server daemon (bmr) from BMR 4.7 is running on the system, stop it 
  before installing the new BMR master server. After installing the new BMR master 
  server, you can restart the BMR 4.7 daemon. For procedures, see “Stopping and 
  Starting the BMR 4.7 Server Daemon” on page 39.

Installing the BMR Master Server on a UNIX or Linux System

Use this procedure to install the BMR master server on a UNIX or Linux system.

If you are installing and running the BMR master server in a cluster environment, you 
must install it on all systems in the cluster on which the NetBackup master server is 
installed.

▼ To install the BMR master server on a UNIX or Linux system

Note If you are installing BMR in a cluster environment, you must freeze the active node 
before you begin the installation process so that migrations do not occur during 
installation. For information about freezing a service group, see the NetBackup High 
Availibility System Administrator’s Guide.

1. Log in as the root user on the system on which the NetBackup master server is 
   installed.
2. Insert the UNIX optional products CD that contains the BMR software into the 
   CD-ROM drive.
3. Change the working directory to the CD-ROM directory.
   
   cd /cd_rom_directory
   
   Where cd_rom_directory is the path to the directory where you can access the 
   CD-ROM. On some platforms, you may need to mount this directory. For instructions 
   on how to mount the directory, see the NetBackup Installation Guide for UNIX and 
   Linux.
4. Enter the following command:
   
   ./install
5. Select the **NetBackup Add-On Product Software** option.
   A menu of NetBackup product options is displayed.

6. Select the **NetBackup Bare Metal Restore** option.

7. Enter `q` to quit the menu.

8. When asked if the list is correct, answer `y`.
   The installation process begins. When completed, the Installation Options menu appears.

9. Enter `q` to quit the Installation Options menu.

10. In a cluster environment environment, complete step 1 through step 9 for each node on which a NetBackup master server is installed.

**Note** If you are installing BMR in a cluster environment, unfreeze the active node after the installation completes. For information about unfreezing a service group, see the *NetBackup High Availability System Administrator’s Guide*.

---

**Uninstalling the BMR Master Server from a UNIX or Linux System**

The following instructions describe how to remove the BMR master server permanently from a UNIX system without uninstalling NetBackup. These procedures remove BMR completely, including the BMR database and log files.

Before you uninstall BMR, you should delete all BMR-specific items from NetBackup, such as client configurations, SRTs, archived boot floppies, and so on. Although all BMR program components are removed when BMR is uninstalled, configuration items related to NetBackup are not.

All BMR components and configuration information are removed when you use one of the following procedures:

- To remove the BMR master server from a Solaris System
- To remove the BMR master server from a UNIX or Linux system

**▼ To remove the BMR master server from a Solaris system**

**Note** If you are removing BMR in a cluster environment, you must freeze the active node before you begin removing BMR so that migrations do not occur during the removal process. For information about freezing a service group, see *NetBackup High Availability System Administrator’s Guide*.

---
1. Log in as root to the system on which the BMR master server is installed.

2. Execute the following command to uninstall the BMR master server:
   
   ```bash
   pkgrm VRTRsnbbmr
   ```
   
   A message asking if you want to remove the package is displayed:
   
   Do you want to remove this package?

3. Enter `y` to remove the BMR master server.

4. If you are prompted with a message about super-user permissions and you are asked if you want to continue, enter `y`.
   
   Messages that show the progress of the removal process are displayed until the following message appears:
   
   Are you doing this pkgrm as a step in an upgrade process? [y,n,?,q]

5. To remove the BMR master server completely and not upgrade to a newer version, enter `n`.
   
   Messages that ask about removing BMR files will appear.

6. Enter `y` to each prompt to remove the BMR files.

7. In a cluster environment environment, complete step 1 through step 6 for each node on which the BMR master server is installed.

**Note** In a cluster environment, unfreeze the active node after removing BMR from all systems. For information about unfreezing a service group, see the *NetBackup High Availability System Administrator’s Guide*.

▼ **To remove the BMR master server from a UNIX or Linux system**

**Note** If you are removing BMR in a cluster environment, you must freeze the active node before you begin removing BMR so that migrations do not occur during the removal process. For information about freezing a service group, see the *NetBackup High Availability System Administrator’s Guide*.

1. Log in as root to the system on which the BMR master server is installed.

2. Run the following command:
   
   ```bash
   /usr/openv/netbackup/bin/install_bmr -d
   ```
3. In a cluster environment, complete the previous steps for each node on which BMR is installed.

**Note** In a cluster environment, unfreeze the active node after removing BMR from all systems. For information about unfreezing a service group, see the *NetBackup High Availability System Administrator’s Guide*.

### BMR Boot Server on UNIX and Linux Systems

To install boot server software, see the following:

**Tasks**

- “Installing a BMR Boot Server on a UNIX or Linux System” on page 21
- “Uninstalling a BMR Boot Server from a UNIX or Linux System” on page 22

**Related Topics**

- “Boot Server Installation Prerequisites for UNIX and Linux Systems” on page 18
- “BMR Boot Server in a UNIX Cluster” on page 20
- “Boot Server Requirements” on page 203

### Boot Server Installation Prerequisites for UNIX and Linux Systems

The following are the BMR boot server installation prerequisites for UNIX and Linux systems.

**All Systems**

- NetBackup master server, NetBackup media server, or NetBackup client software must be installed on the system on which the boot server software will be installed, and it must be installed before the boot server software is installed. To install the NetBackup software, see the *NetBackup Installation Guide for UNIX and Linux*.
- BMR master and boot servers installed on the same system must maintain the same version of BMR.
- The BMR master server for the environment must be installed and configured before installing and configuring BMR boot servers.
UNIX Systems

- The tftp and bootp services 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.

- 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 network booting of BMR clients. NFS client and server services are required to copy SRTs between boot servers. No /etc/exports configuration is required; Bare Metal Restore will add and remove specific export permissions as required.

  Look for the nfsd process in the process table. If it is not present, make sure the NFS server is installed and configured. (Solaris automatically starts the NFS server if it is installed normally.)

Red Hat Linux Systems

Install the following (unless already installed):

- compat-libstdc++
- tftp-server
- dhcpc

Enable the tftp service by doing the following:

1. Edit the /etc/xinetd.d/tftp file and change disable = yes to disable = no.

2. Start the service by running the following command:

   /etc/init.d/xinetd restart

Create an /etc/dhcpd.conf file and configure it so it defines the networks it will be serving. You do not have to define host information; hosts will be added and removed as needed by the Bare Metal Restore software. The following is an example configuration:

```conf
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 it starts successfully by running:

```bash
/etc/init.d/dhcpd restart
```
/etc/init.d/dhcpd restart

**SuSE Linux Systems**

Install the following RPM packages (unless already installed):

- nfs-utils
- dhcp-base
- dhcp-server
- inetd
- tftp

Enable the tftp service by doing the following:

1. Edit the `/etc/inetd.conf` file and uncomment the tftp line.
2. Start the service by running the following command:
   
   `/etc/init.d/inetd restart`

Modify the `/etc/dhcpd.conf` file so it defines the networks it will be serving. You do not have to define host information; hosts will be added and removed as needed by the Bare Metal Restore software. The following is an example configuration:

```plaintext
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 it starts successfully by running:

`/etc/init.d/dhcpd restart`

**BMR Boot Server in a UNIX Cluster**

For information about the systems on which BMR boot servers can be clustered, see Supported Platforms and Peripherals > Other NetBackup Compatibility Lists > NetBackup Bare Metal Restore in the *NetBackup Release Notes*. 
The following are general instructions for installing and using a BMR boot server in a clustered environment.

1. In the clustering application, set up a virtual IP address on the nodes that will provide the BMR boot server functionality.

2. Install the NetBackup client software on each node.

3. On each node, configure the NetBackup client name to be the name that resolves to the virtual IP address. Use that name for the the last CLIENT_NAME entry in the bp.conf file on the system.

4. Install the BMR boot server software on each node. Switch the virtual address to each node before you install the boot server software.

5. Create a cluster application resource that calls the start/stop script for the boot server daemon:

   ```
   /usr/openv/netbackup/bin/rc.bmrbd start
   /usr/openv/netbackup/bin/rc.bmrbd stop
   ```

6. When creating SRTs, choose a location on a file system on the shared disk.

7. If a boot server fails over and it has pending restore tasks, you must perform a new prepare to restore operation for each pending restore task.

**Installing a BMR Boot Server on a UNIX or Linux System**

Use this procedure to install a BMR boot server on a UNIX or Linux system.

**Note** This installation process 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. That name must be resolvable to an IP address, and the IP address must be the IP address of one of the network interfaces, excluding the loop back address, on the boot server. If the bp.conf file does not have a CLIENT_NAME entry or if it does not meet these criteria, add an entry or fix the bp.conf file before installing the boot server. If you do not follow these guidelines, the boot server will not function.
To install a BMR boot server on a UNIX or Linux system

1. Log in as the root user.

2. Insert the UNIX optional products CD that contains the BMR boot server software into the CD-ROM drive.

3. Change the working directory to the CD-ROM directory.
   
   $ cd /cd_rom_directory
   
   Where cd_rom_directory is the path to the directory where you can access the CD-ROM. On some platforms, you may need to mount this directory. For instructions on how to mount the directory, see the NetBackup Installation Guide for UNIX and Linux.

4. Enter the following command:
   
   $ ./install
   
5. Select the NetBackup Add-On Product Software option.

   A menu of NetBackup product options is displayed.

6. Select the NetBackup Bare Metal Restore Boot Server option.

7. Enter q to quit the menu.

8. When asked if the list is correct, answer y.

   The installation process begins. When completed, the Installation Options menu appears.

9. Enter q to quit the Installation Options menu.

Uninstalling a BMR Boot Server from a UNIX or Linux System

The following instructions describe how to remove a BMR boot server permanently from a UNIX or Linux system. Use one of the following procedures:

- To remove a BMR boot server from a Solaris System
- To remove a BMR boot server from a UNIX or Linux system
To remove a BMR boot server from a Solaris system

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

1. Log in as root to the system on which the BMR boot server is installed.
2. Delete all of the SRTs on the boot server by using the `bmrsrtadm` command.
3. Execute the following command to uninstall the BMR boot server:
   ```
pkg rm VRTSnbbbs
   ```
   A message asking if you want to remove the package is displayed:
   ```
   Do you want to remove this package?
   ```
4. Enter `y` to remove the BMR boot server.
5. If you are prompted with a message about super-user permissions and you are asked if you want to continue, enter `y`.
   Messages that show the progress of the removal process are displayed until the following message appears:
   ```
   Are you doing this pkg rm as a step in an upgrade process? [y,n,?,q]
   ```
6. To remove the BMR boot server completely and not upgrade to a newer version, enter `n`.
   Messages that ask about removing BMR files will appear.
7. Enter `y` to each prompt to remove the BMR files.
8. On the NetBackup master server, run the following command to delete the boot server name from the BMR database:
   ```
   /usr/openv/netbackup/bin/bmrs -o delete -r bootserver -name bootservername
   ```

To remove a BMR boot server from a UNIX or Linux system

You must log in as root when you run the commands in the following procedure.
1. On the BMR boot server, delete all of the SRTs by using the `bmrsrtaadm` command.

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

   ```
   /usr/openv/netbackup/bin/bmrs -o delete -r bootserver -name bootservername
   ```

   To see a list of boot server name, run the following command:

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

3. On the BMR boot server, run the following command:

   ```
   /usr/openv/netbackup/bin/install_bmrboot -d
   ```

**BMR Client Software on UNIX and Linux Systems**

The BMR client software is installed automatically when the NetBackup client software is installed. For information about how to install NetBackup client software, see the *NetBackup Installation Guide for UNIX and Linux*.

**Client Installation Prerequisites for Linux Systems**

For operating system dependencies and installation prerequisites for BMR client systems, see the *NetBackup Release Notes*.

**Microsoft Windows Systems**

For information about installing the BMR components, see the following:

- “BMR Master Server on Windows Systems” on page 24
- “BMR Boot Server on Windows Systems” on page 29
- “BMR Client Software on Windows Systems” on page 37

**BMR Master Server on Windows Systems**

The Bare Metal Restore master server is installed on a Windows system when the NetBackup master server is installed; no separate installation procedure is required. However, to use BMR, you must enter a license key:
Your license key may be a single key for the base NetBackup product and all NetBackup add-ons that you are installing, including BMR. If you have already installed NetBackup and entered the license key, BMR is already licensed.

You may have a separate license key specifically for the BMR option. If so, you will have to enter the BMR license key before you can use BMR (see “Licensing the BMR Master Server on a Windows System” on page 25).

After you license BMR, you must run a wizard to set up the BMR master server.

If you are installing and running the BMR master server in a cluster environment, you must license BMR on all systems in the cluster on which NetBackup master servers are installed.

After you license the BMR master server and configure NetBackup so that backups can occur, you can protect clients. For more information, see “Protecting Clients” on page 51.

**Tasks**

- “Licensing the BMR Master Server on a Windows System” on page 25
- “Uninstalling the BMR Master Server from a Windows System” on page 27

**Related Topics**

- “Licensing Prerequisites for Windows Systems” on page 25

---

**Licensing Prerequisites for Windows Systems**

- The NetBackup master server must be installed and running on the Windows computer.
- You must have a valid BMR license key.

**Licensing the BMR Master Server on a Windows System**

You must perform the following two procedures:

- Add the BMR license key
- Set up the BMR master server

**Note** If you are licensing and setting up BMR in a cluster environment, you must freeze the active node before you begin so that migrations do not occur during this process. For information about freezing a service group, see the *NetBackup High Availability System Administrator’s Guide.*
To add the BMR license key

If you are installing and running the BMR master server in a cluster environment, perform this procedure on all systems on which the NetBackup master server is installed.

If the license key for BMR was included in the license key for the base NetBackup product, you do not have to perform this procedure.

1. From the NetBackup Administration console, choose Help > License Keys.
   The NetBackup License Keys dialog box appears.

2. Click New to display the Add a new License Key dialog box.

3. Enter the BMR license key.

4. Click Add.
   The license key is displayed in the NetBackup License Keys dialog box.

5. Click Close to close the NetBackup License Keys dialog box.

To set up the BMR master server

If you are installing and running the BMR master server in a cluster environment, perform this procedure on the active node.

1. On the Windows BMR master server, select Programs > VERITAS NetBackup > Bare Metal Restore -- Master Server Setup from the Start menu.
   The Master Server Setup Wizard welcome screen 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.

**Note** If you are licensing and setting up BMR in a cluster environment, unfreeze the active node after you complete this process. For information about unfreezing a service group, see the clustering section in the *NetBackup High Availability System Administrator’s Guide* for the cluster software you are running.

---

**Uninstalling 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 must remove the BMR database.
Note If you are removing BMR in a cluster environment, you must freeze the active node before you begin removing BMR so that migrations do not occur during the removal process. For information about freezing a service group, see the NetBackup High Availability System Administrator’s Guide.

▼ To remove the BMR database

If you are running BMR in a cluster environment, perform the following procedure on the active node.

1. Open a Windows command window.

2. Enter the following command:

   C:\Program Files\VERITAS\NetBackup\bin>bmrsetupmaster -undo

   The following prompt appears:

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

3. Type y to remove the BMR database.

▼ To delete the BMR license key

If you are running BMR in a cluster environment, you must delete the BMR license key on every system in the cluster on which the BMR master server is installed.

1. From the NetBackup Administration Console, choose Help > License Keys.

   The NetBackup License Keys dialog box appears.

2. From the list of keys displayed, select the BMR license key.

Caution If BMR was included as part of the base product key, performing the following step will delete your base key and you will be unable to use NetBackup. If you do not want to delete the NetBackup license key, do not continue.

3. Click Delete.

   The BMR license key is deleted from the Current Licenses dialog box, and Bare Metal Restore Management is no longer displayed in the NetBackup Administration Console.
Note In a cluster environment, unfreeze the active node after deactivating BMR from all systems. For information about unfreezing a service group, see the NetBackup High Availability System Administrator’s Guide.

BMR Boot Server on Windows Systems

To install boot server software, see the following

Tasks
“Installing a BMR Boot Server on a Windows System” on page 30
“Uninstalling a BMR Boot Server from a Windows System” on page 35

Related Topics
“Boot Server Installation Prerequisites for Windows Systems” on page 29
“BMR Boot Server in a Windows Cluster” on page 29
“Boot Server Requirements” on page 203

Boot Server Installation Prerequisites for Windows Systems

✦ NetBackup master server, NetBackup media server, or NetBackup client software must be installed on the system on which the boot server software will be installed, and it must be installed before the boot server software is installed. To install the NetBackup software, see the NetBackup Installation Guide for Windows.

✦ BMR master and boot servers installed on the same system must maintain the same version of BMR.

✦ The BMR master server for the environment must be installed and configured before installing and configuring BMR boot servers.

BMR Boot Server in a Windows Cluster

For information about the systems on which BMR boot servers can be clustered, see Supported Platforms and Peripherals > Other NetBackup Compatibility Lists > NetBackup Bare Metal Restore in the NetBackup Release Notes.

The following are general instructions for installing and using a BMR boot server in a clustered environment.
1. In the clustering application, set up a virtual IP address on the nodes that will provide the BMR boot server functionality.

2. Install the NetBackup client software on each node.

3. On each node, configure the NetBackup client name to be the name that resolves to the virtual IP address: start the Backup, Archive, and Restore interface, enter that name as the client name in the Specify NetBackup Machines and Policy Type dialog box, and then make it the current client.

4. Install the BMR boot server software on each node. Switch the virtual address to each node before you install the boot server software.

5. Create a cluster application resource that calls the start/stop script for the boot server service:
   ```
   net start "NetBackup Bare Metal Restore Boot Server"
   net stop "NetBackup Bare Metal Restore Boot Server"
   ```

6. When creating SRTs, choose a location on a file system on the shared disk.

7. If a boot server fails over and it has pending restore tasks, you must perform a new prepare to restore operation for each pending restore task.

### Installing a BMR Boot Server on a Windows System

The following are the installation options:

- **Local installation**: installing to the same computer on which the installer is running
- **Remote installation**: installing to a different computer than the one on which the installer is running

To begin installing a boot server, follow the procedures in “To install a BMR boot server on Windows” on page 30; those procedures then direct you to an additional procedure for remote installation if necessary.

#### To install a BMR boot server on Windows

1. Log on as Administrator on the server on which you will be installing the BMR boot server or the server from which you will push the installation.

2. Insert the NetBackup installation CD in the drive.
   - On Windows systems with AutoPlay enabled for CD-ROM drives, the VERITAS NetBackup installation browser starts automatically.
On Windows systems that have AutoPlay disabled, run `Launch.exe` in the top-level directory on the CD.

3. The NetBackup installation browser appears:

4. Click **Additional Products** in the Main Menu.

5. Click **Additional Product Installations**.

6. Click **BMR Boot Server**.

   A welcome screen appears informing you that the NetBackup setup wizard is about to install the software.

7. Click **Next** to continue.

   The license screen appears.

8. On the License screen, select **I accept the terms of the license agreement** then click **Next**.
The Install Choice screen appears.

9. On the Install Choice screen, do the following:

a. Select either Install to this computer only or Select from available computers on the network.

b. Select Typical installation.

c. Click Next to continue.

   If you chose Select from available computers on the network, go to “To use the remote installation option” on page 33.

   If you are performing a basic installation, the Install screen appears.

10. On the Install screen, click Install.

11. After the installation completes, click Finish on the System Validation Complete screen.

12. To exit the NetBackup installation browser, click Exit.
To use the remote installation option

After you choose Select from available computers on the network and click Next to continue, you can use the NetBackup Remote Features window to install the boot server software on a remote computer:

1. Right-click on Windows Agent/Option Computers in the Destination System window and select one of the following from the shortcut menu:
   - **Add Remote Computer** - Selecting this option lets you select a computer from a list of computers in your Microsoft Windows network.
   - **Add Remote Computer Manually** - Selecting this option lets you enter the name of a computer.
Depending on your selection, one of the following pop-up windows appears:

2. If you selected **Add Remote Computer**, select a computer from the Available Systems window and then click **Next**. If you selected **Add Remote Computer Manually**, enter the domain and computer in the Manual Remote Computer Selection window and then click **Next**.

The NetBackup Remote Features window refreshes and displays the Remote Computer Login Credentials window.

3. Enter your user name, password, and domain and then click **OK**. In addition, you can select the **Remember User Name and Password** checkbox, if you intend to add more remote computers.

The NetBackup Remote Features window refreshes, and the remote machine is displayed in the Destination Systems window.
4. Click Next.
   The Install screen appears.

5. On the Install screen, click Install.

6. After the installation completes, click Finish on the System Validation Complete
   screen.

7. To exit the NetBackup installation browser, click Exit.

Uninstalling a BMR Boot Server from a Windows System

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

1. Log on as Administrator on the boot server.

2. Remove the shared resource trees from the boot server:
   a. From the Start menu on the Windows BMR boot server, select Programs >
      VERITAS NetBackup > Bare Metal Restore Boot Server Assistant.
      The Bare Metal Restore Boot Server Assistant appears.
   b. Click Shared Resource Tree Administration Wizard.
      The Shared Resource Tree Administration wizard welcome screen appears.
   c. Click Next.
The Create or Add Software to a Shared Resource Tree screen appears.

![NetBackup Bare Metal Restore - Share Resource Tree Administration Wizard](image)

- **d.** Select the option to delete a shared resource tree, click **Next**, then follow the prompts to delete a shared resource tree.

- **e.** Repeat until all shared resource trees are removed.

3. Use Windows Add/Remove Programs to remove the boot server software:

- **a.** On the Windows **Start** menu, select **Settings > Control Panel > Add/Remove Programs**.

- **b.** Select **VERITAS Bare Metal Restore Boot Server**.

- **c.** Click **Remove**.

- **d.** 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.
BMR Client Software on Windows Systems

The BMR client software is installed automatically when the NetBackup client software is installed. For information about how to install NetBackup client software, see the NetBackup Installation Guide for Windows.

Migrating from BMR 4.7

There is no upgrade path from earlier versions of BMR to NetBackup BMR 6.0. NetBackup BMR 6.0 supports new installations only of BMR.

However, BMR 4.7 clients can operate with NetBackup 6.0 servers so you can install the new NetBackup BMR 6.0 while you continue to protect your clients with your current version of BMR.

Tasks

“Steps for Migrating to NetBackup BMR 6.0” on page 37
“Converting External Procedures” on page 39
“Decommissioning BMR 4.7” on page 40

Steps for Migrating to NetBackup BMR 6.0

The following is a high level description of the migration process.

Note If you install BMR 6.0 master or boot server software on (or uninstall from) a system that already hosts a BMR 4.7 master server, file server, or boot server, you must stop the BMR 4.7 server daemon (bmrzd) before installing the NetBackup 6.0 server software. For instructions, see “Stopping and Starting the BMR 4.7 Server Daemon” on page 39.

1. Upgrade the NetBackup master server to NetBackup 6.0. For instructions, see the NetBackup Installation Guide for UNIX and Linux or the NetBackup Installation Guide for Windows.

   The NetBackup master server must be on a system that supports the BMR master server. For information about supported systems, dependencies, limitations, and operating system installation prerequisites for BMR, see the NetBackup Release Notes.

   Your existing BMR environment will work with the NetBackup 6.0 master server.
2. Upgrade the NetBackup media servers to NetBackup 6.0. For instructions, see the
NetBackup Installation Guide for UNIX and Linux or the NetBackup Installation Guide for
Windows.

Your existing BMR environment will work with the NetBackup 6.0 media servers.

3. Install and license the BMR 6.0 master server software on the NetBackup 6.0 master
server machine. For instructions, see “Installing Bare Metal Restore” on page 13.

The NetBackup master server must be on a system that supports the BMR master
server. For information about supported systems, dependencies, limitations, and
operating system installation prerequisites for BMR, see the NetBackup Release Notes.

Your existing BMR environment will continue to work.

4. Upgrade the clients to NetBackup 6.0. For instructions, see the NetBackup Installation
Guide for UNIX and Linux or the NetBackup Installation Guide for Windows.

Because the BMR client is part of the NetBackup client code, no additional installation
is needed for BMR clients. After upgrading to the NetBackup 6.0 client code, the old
BMR 4.7 client code will be disabled but will not be removed.

5. On the NetBackup 6.0 master server, configure a policy for BMR protection and back
up the clients you want to protect with BMR. For instructions, see “Protecting Clients”
on page 51.

The BMR agent on the client will run and save the client configuration before the
backup starts; you can view the BMR job in the NetBackup Administration Console
Activity Monitor.

If the backup was successful, the client is protected and will appear in the Bare Metal
Restore Clients view in the NetBackup Administration Console. To restore a client,
you must first install a boot server and create a shared resource tree for that client
type.

If the backup fails or the BMR agent on the client fails, the client is not protected by
the NetBackup BMR 6.0 environment.

6. Set up the restore resources in your NetBackup BMR 6.0 environment. For more
information, see “Setting Up Restore Resources” on page 57.

Your clients can be restored by the NetBackup BMR 6.0 environment.

7. Perform test restores onto different hardware. UNIX and Linux must restore to similar
hardware, and Windows can restore to any x86 hardware.

After successful test restores, you can decommission your BMR 4.7 environment.
Stopping and Starting the BMR 4.7 Server Daemon

*UNIX and Linux only.*

Before you install the BMR 6.0 server software on a system that runs a BMR 4.7 master server, file server, or boot server (or uninstall from), you must stop the BMR 4.7 server daemon (`bmrhd`). After installing or uninstalling the BMR 6.0 server software, you can restart the BMR 4.7 `bmrhd` daemon. For procedures, see the following:

▼ To stop the `bmrhd` daemon

1. Edit the `/etc/inittab` file on the BMR 4.7 server and comment out the line that starts the BMR daemon.

2. Run the following command to refresh `initd`:
   ```
   kill -1 1
   ```

3. Determine the process ID of the BMR 4.7 `bmrhd` process and then kill the `bmrhd` process.

▼ To start the `bmrhd` daemon

1. Edit the `/etc/inittab` file and uncomment the line that starts the BMR daemon.

2. Run the following command to refresh `initd`:
   ```
   kill -1 1
   ```

Converting External Procedures

If you want to use external procedures from your BMR 4.7 environment with NetBackup BMR 6.0, you must do the following:

◆ Modify the external procedure scripts. Commands and environment variables have changed in BMR 6.0, so you have to modify the external procedure scripts to accommodate the changes.

◆ Add the external procedures to the BMR database. BMR 6.0 and later manages external procedures differently than BMR 4.7. You must add them to the BMR database so they will be available during a restore.

The naming convention for external procedures has not changed.
Modify the External Procedure Scripts

Changes in BMR 6.0 require that you modify your existing external procedures if you use them with NetBackup 6.0 and later. The following tables summarizes the changes:

**bmrlog**
The `bmrlog` command has been removed. Use the `bmrc` command to write a message or output from a command to the BMR restore log. For more information, see “External Procedure Logging” on page 110.

**bmrget**
The `bmrget` command has been removed. Use the `bmrc` command to retrieve files from the master server during a restore. For more information, see “External Procedure Data Transfer” on page 109.

**bmrshell**
The `bmrshell` command has been renamed `bmrShell` (case sensitive). Replace `bmrshell` with `bmrShell` in the external procedure scripts. For more information, see “Interaction with External Procedures” on page 110.

**Environment Variables**
The naming scheme for BMR environment variables has changed. The names of many of the environment variables have changed, so you must change them in your external procedure scripts. For more information, see “External Procedure Environment Variables” on page 113.

**bmrc Command Path**
Use the full path to the `bmrc` command:
- `/usr/openv/netbackup/bin` on UNIX and Linux clients
- `%SystemDrive%\BMR\NB\bin` on Microsoft Windows clients.
  At the firstboot external procedure point, the path to the `bmrc` command is `install_path\NetBackup\bin` on Microsoft Windows clients.

Adding External Procedures to the BMR Database

External procedures are no longer stored in the `/var/bmr/epdir` directory; they are stored in the BMR database on the master server.

Use the `bmrepadm` command on the master server to add external procedures to the BMR database. For examples, see “Managing External Procedures” on page 108.

Decommissioning BMR 4.7

After you migrate to NetBackup BMR 6.0, do the following to uninstall your BMR 4.7 environment:
1. Remove the bmrsavecfg command from the bpstart_notify script on every client protected by BMR 4.7.

2. Uninstall the BMR 4.7 client software on every client protected by BMR 4.7.
   For instructions, see “Uninstalling BMR 4.7 Clients” on page 41.

3. Uninstall the BMR 4.7 boot and file servers.
   For instructions, see Tips and Troubleshooting > Tips > Removing BMR Servers in the
   Bare Metal Restore for VERITAS NetBackup System Administrator’s Guide for BMR 4.7.

4. Remove the shared resource trees from the BMR 4.7 file servers.
   Use operating system commands to remove the SRT directories. If the SRTs reside in
   directories that were deleted when you uninstalled the BMR file servers, this step is
   unnecessary.

5. Uninstall the BMR 4.7 main server.
   For instructions, see Tips and Troubleshooting > Tips > Removing BMR Servers in the
   Bare Metal Restore for VERITAS NetBackup System Administrator’s Guide for BMR 4.7.

**Uninstalling BMR 4.7 Clients**

Use one of the following procedures to uninstall the BMR 4.7 clients:

▼ **To uninstall a BMR 4.7 client from a Windows system**
   Use Add/Remove Programs.

▼ **To uninstall a BMR 4.7 client from a Solaris system**
   Use the package remove command:
   `pkg rm BMRclient`

▼ **To uninstall a BMR 4.7 client from a UNIX system**
   On AIX and HP-UX systems, remove the following directories:
   `/usr/lpp/baremetal`
   `/opt/baremetal`
Monitoring Activity

Monitor backup jobs in the Activity Monitor of the NetBackup Administration Console; monitor the progress and status of BMR discovery and restore tasks by using the **Bare Metal Restore Management > Tasks** view. Also, the BMR logs provide detailed information about BMR activity.

**Tasks**

- “Monitoring Backup Jobs” on page 43
- “Monitoring BMR Tasks” on page 44
- “Viewing BMR Logs” on page 46

Monitoring Backup Jobs

You can monitor the jobs that back up 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 on the job, which opens the Job Details dialog box. Two 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, collects the client configuration information, and sends it to the BMR master server. On protected systems that have simple configurations (one or a few disks), the agent will take only a few seconds. More complex systems that have disk or volume groups may take a few minutes, and 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, with each job backing 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 invokes the agent that collects the client configuration (normally, the job with the lowest job ID).
Monitoring BMR Tasks

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

Monitoring BMR Tasks

The Tasks view shows the status and resource allocation for the prepare to restore and prepare to discover operations. 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.

Bare Metal Restore Tasks Window
Actions for Tasks View

<table>
<thead>
<tr>
<th>To</th>
<th>Do the Following</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the tasks and operations that are allocated</td>
<td>Select <strong>Bare Metal Restore Management &gt; Tasks</strong>.</td>
</tr>
<tr>
<td>Display task properties</td>
<td>Right click on a task in the details pane and then select <strong>Properties</strong> from the shortcut menu.</td>
</tr>
<tr>
<td>Clean up a task</td>
<td>Right click on a task in the details pane and then select <strong>Clean Up</strong> from the shortcut menu. The resources 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 tasks that are in an Active or Waiting state.</td>
</tr>
<tr>
<td>Delete a task</td>
<td>Right click on a task in the details pane and then select <strong>Delete</strong> from the shortcut menu. You can delete tasks that are in a Done state.</td>
</tr>
</tbody>
</table>

The following are the columns in the Task view.

Tasks View Columns

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Name</td>
<td>The name of the client.</td>
</tr>
<tr>
<td>Configuration</td>
<td>The configuration used for the task.</td>
</tr>
<tr>
<td>Shared Resource Tree</td>
<td>The SRT used for the task.</td>
</tr>
</tbody>
</table>
| State | The following are the states of restore or discovery tasks:  
  - Active. The task is in progress  
  - Done. The task completed.  
  - Editing. Dissimilar disk restore mapping is occurring.  
  - Queued. The task has not been active yet.  
  - Waiting. The task was active but is waiting for some user action. |
## Viewing BMR Logs

You can monitor BMR activity by viewing the messages generated by BMR. BMR activity log files are stored in the following directories on the master server:

### Tasks View Columns

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Displays Ready when the task is Queued; otherwise, shows the following when the restore is in progress (the State is Active or Waiting):</td>
</tr>
<tr>
<td></td>
<td>- Discovery External Procedure (Active State only). An external procedure is running during the prediscovery phase.</td>
</tr>
<tr>
<td></td>
<td>- Failed (Done State only). The task failed.</td>
</tr>
<tr>
<td></td>
<td>- Finalizing (Active State only). Completing the task.</td>
</tr>
<tr>
<td></td>
<td>- First Boot External Procedure (Active State only). An external procedure is running during the firstboot phase.</td>
</tr>
<tr>
<td></td>
<td>- Formatting (Active State only). Formatting the drives.</td>
</tr>
<tr>
<td></td>
<td>- Initializing (Active State only). Booting the client.</td>
</tr>
<tr>
<td></td>
<td>- Mapping (Waiting State only). Mapping required.</td>
</tr>
<tr>
<td></td>
<td>- Mapped (Active State only). Mapping completed and passed validation.</td>
</tr>
<tr>
<td></td>
<td>- Post-restore External Procedure (Active State only). An external procedure is running during the postrestore phase.</td>
</tr>
<tr>
<td></td>
<td>- Pre-format External Procedure (Active State only). An external procedure is running during the preformat phase.</td>
</tr>
<tr>
<td></td>
<td>- Pre-restore External Procedure (Active State only). An external procedure is running during the prerestore phase.</td>
</tr>
<tr>
<td></td>
<td>- Restoring (Active State only). Restoring files.</td>
</tr>
<tr>
<td></td>
<td>- Restore Canceled (Done State only). The user terminated the restore.</td>
</tr>
<tr>
<td></td>
<td>- User Input Requested (Waiting State only). Waiting for user action.</td>
</tr>
<tr>
<td></td>
<td>- Waiting for Reboot.</td>
</tr>
<tr>
<td>Status</td>
<td>Status codes for the task.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Date and time the task started.</td>
</tr>
<tr>
<td>End Time</td>
<td>Date and time the task ended.</td>
</tr>
<tr>
<td>Type</td>
<td>Restore or Discover.</td>
</tr>
</tbody>
</table>
Viewing BMR Logs

- /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:

51216-119-3892578826-050225-000000000.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 bmrd, 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.
- 000000000 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 will increase by 1.

Three kinds 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 logged depends on the logging level.
- Debug log messages. These are primarily for VERITAS support and engineering. The amount of debug information logged depends on the logging level specified for the NetBackup master server.

**BMR Logging Originator IDs**

The following are the originator IDs for the BMR processes the perform logging:

<table>
<thead>
<tr>
<th>Originator ID</th>
<th>BMR Processes that Use ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>119</td>
<td>bmrd and bmrd, Bare Metal Restore master and boot server services. The bmrd boot server process runs on a BMR boot server.</td>
</tr>
<tr>
<td>121</td>
<td>bmrsavecfg, Bare Metal Restore agent that runs on client systems, collects the client configuration, and saves the client configuration to the master server.</td>
</tr>
<tr>
<td>122</td>
<td>bmrc, Bare Metal Restore utility that clients use to communicate with the BMR master server during a restore. Runs on the restoring client.</td>
</tr>
</tbody>
</table>
Viewing BMR Logs

<table>
<thead>
<tr>
<th>Originator ID</th>
<th>BMR Processes that Use ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>123</td>
<td><code>bmrsl</code>. The Bare Metal Restore command line interface for various activities performed via the GUIs.</td>
</tr>
<tr>
<td>124</td>
<td><code>bmrcreatefloppy.exe</code> (<em>Windows systems only</em>). Bare Metal Restore utility that creates bootable floppy diskettes used to boot protected Windows clients for a restore. Runs on a BMR boot server.</td>
</tr>
<tr>
<td>125</td>
<td><code>bmrsladm</code>. Bare Metal Restore utility that creates and manages shared resource trees and creates bootable CD media for restores. Runs on a BMR boot server.</td>
</tr>
<tr>
<td>126</td>
<td><code>bmrprep</code>. Bare Metal Restore utility that prepares BMR for a client restore or discovery. Runs on the master server.</td>
</tr>
<tr>
<td>127</td>
<td><code>bmrsetupmaster</code> and <code>bmrsetupboot</code>. Bare Metal Restore master server and boot server configuration utilities.</td>
</tr>
<tr>
<td>128</td>
<td>Miscellaneous programs and Bare Metal Restore libraries.</td>
</tr>
<tr>
<td>129</td>
<td><code>bmrconfig</code>. Bare Metal Restore utility that modifies a client's configuration.</td>
</tr>
<tr>
<td>130</td>
<td><code>bmrcreatepkg.exe</code>. 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.</td>
</tr>
<tr>
<td>131</td>
<td><code>bmrsl.exe</code> and <code>bmrmap.exe</code> (<em>Windows systems only</em>). Utilities that restore Windows Bare Metal Restore clients. Run on the restoring client.</td>
</tr>
<tr>
<td>142</td>
<td><code>bmrrepadm</code>. A utility that manages Bare Metal Restore external procedures used during restores. Runs on the master server.</td>
</tr>
<tr>
<td>152</td>
<td><code>bmrrovradm</code>. A utility that manages custom override functions for Bare Metal Restore.</td>
</tr>
</tbody>
</table>

Configuring and Using Logging

The amount of information collected and how long to retain that information is configured on the NetBackup master server in the Logging properties and Clean-up properties. For more information, see the following:

- *NetBackup System Administrator's Guide*:
  - Configuring Host Properties > Master Server, Media Server, and Client Host Properties > Logging Properties
Viewing BMR Logs

- Configuring Host Properties > Master Server, Media Server, and Client Host Properties > Clean-up Properties

The NetBackup Troubleshooting Guide includes more information about using and managing logs (Using Logs and Reports > Debug Logs on Servers > Unified Logging).

BMR activity log files are a special format that require commands to view and manage. Three commands manage unified logging and log files:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vxlogview</td>
<td>Use this command to view the logs created by unified logging.</td>
</tr>
<tr>
<td>vxlogmgr</td>
<td>Use this command to manage unified logging files (for example, to move or delete log files).</td>
</tr>
<tr>
<td>vxlogcfg</td>
<td>Use this command to configure logging settings.</td>
</tr>
</tbody>
</table>

These commands are located in:

- /usr/openv/netBackup/bin directory (UNIX)
- install_path\NetBackup\bin folder (Windows).

For more information, see the following:

- NetBackup Commands for UNIX
- NetBackup Commands for Windows

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.mmdvy (UNIX)
- install_path\NetBackup\logs\bmrrst\client_name\log.mmdvy (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.
Protecting Clients

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

**Topics**

“Back Up the Client” on page 51

**Related Topics**

“Configure NetBackup Properties” on page 55

Back Up the Client

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 NetBackup managed storage device and 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 and appears in the Bare Metal Restore Clients view in the NetBackup Administration Console.

**Tasks**

“Configuring Policies to Back Up BMR Clients” on page 52

**Related Topics**

“Perform Complete Backups” on page 53

“Perform a Full Backup After a Restore” on page 53

“Ensure Successful Backups” on page 54

“Save Custom Files” on page 54

“Monitor Backups” on page 55
Best Practices

“Use the ALL_LOCAL_DRIVES Directive” on page 55

“Use the Same Client Name in Multiple Policies” on page 55

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 either type MS-Windows-NT (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, the Collect disaster recovery information for Bare Metal Restore attribute is set automatically when you create a new MS-Windows-NT or Standard policy.

The Collect true image restore information and with move detection attributes are set automatically when the Collect disaster recovery information for Bare Metal Restore attribute is set. These attributes enable NetBackup to restore only those files present on the system at the time of the backup. Move detection enables NetBackup to correctly restore files that were moved, renamed, or newly installed. These attributes also ensure that all of the restored files will fit in the volumes and file systems created by BMR during the recovery.

If Collect disaster recovery information for Bare Metal Restore attribute is not set, the client will not be protected by BMR.

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.

You should 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 method to obtain a complete backup. If a client has database or application files that you 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.
- 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 additional policies that back up the node that currently owns the resources.
- Logical volumes that are not part of the operating system can be backed up with different policies, but each logical volume must be backed up by a single policy.
VERITAS recommends that you 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- or SAN-attached) require special procedures for restores; understanding the special procedures may help you configure NetBackup so you can minimize the time and effort required for the restores. For more information, see “Restoring NetBackup Media Servers” on page 103.

For instructions for configuring backup policies, see “Managing Backup Policies” in the NetBackup System Administrator’s Guide, Volume I.

Perform Complete Backups

To be able 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 do not get backed up and therefore do not get restored.

Perform 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 will not be able to 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.

▼ To perform a manual backup

1. In the NetBackup Administration Console, expand NetBackup Management > Policies.

2. Select the policy that backs up the client.

   The Manual Backup dialog box appears.

4. Select the Full schedule and the client that you want to back up.

5. Click OK to start the backup.
Ensure Successful Backups

Schedule backups when the risk of an incomplete backup is minimized. If a client cannot be quiesced during a backup:

- For UNIX clients, configure NetBackup to retry file backups if a file changes during the backup attempt. See “Busy File Properties” in NetBackup System Administrator’s Guide, Volume I.


Examine the NetBackup log files regularly to ensure that any backup errors are corrected promptly. Network or server errors that occur during back up can affect the backup.

Save Custom Files

UNIX and Linux clients only.

Usually, client files are restored by NetBackup as the last step in the restore process. On UNIX and Linux clients, you can specify custom files on the client so they will be available in the temporary operating system environment on the client during the restore (the restore environment). For example, if 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 pathname 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 and available during the restore when you enable the SRT for exclusive use. To do so, see:

- “Using a Shared Resource Tree Exclusively” on page 143

Specifying a custom file does not remove it from backups; custom files are also backed up by NetBackup and then restored when NetBackup restores the client files (that is, if the files or their directories are included in the backup directives of the policy).
Monitor 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.

Related Topics

◆ “Monitoring Backup Jobs” on page 43

Use the ALL_LOCAL_DRIVES Directive

To ensure complete system recovery, you should use the ALL_LOCAL_DRIVES directive to back up all local drives, which 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 that you 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.

Use 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 named in the policy that backed up the system files. If you use more than one policy and use a different name in each policy, a client record and its associated configuration will be created for each name of the client. If you choose to restore a client by a name in a policy that does not back up the system files, the prepare to restore operation will fail because BMR can only restore using the client 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.

Configure NetBackup Properties

Configure the following NetBackup properties.

◆ The Allow Client Restore property must be enabled. The BMR restore process requires that both the BMR master server and the BMR client be able to request restores. Allowing client restores is the default NetBackup behavior; ensure that client restores are not disallowed. The Allow Client Restore property is located on the Client Attributes tab of the NetBackup master server properties.
Configure NetBackup Properties

◆ The NetBackup clients must be configured 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 not disallowed. For more information, see “Server-Directed Restores” in the NetBackup System Administrator’s Guide, Volume I.

◆ The **Keep true image restore (TIR) Information** property controls how long TIR information is retained in the NetBackup catalog. TIR information increases catalog size and disk space used. The following 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 0 days. The TIR information is also stored on the backup media, so the catalog size will not increase but restores will be slower.

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

For information about how to configure NetBackup, see the *NetBackup System Administrator’s Guide, Volume I*. 
Setting Up Restore Resources

Before you can restore a protected client, you must set up the resources that will be used during the restore.

You can set up the resources at any time; however, if your recovery time objective (RTO) is short, you may want to have all of the resources in place so your time is used in recovery rather than set up.

Topics

“Install Boot Server Software” on page 57
“Create Shared Resource Trees” on page 58
“Add Client Resources” on page 58
“Create Boot Media” on page 58
“Verify the Protection” on page 59

Install 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, and you must install the BMR boot server software before you can create SRTs and add resources to them.

For information about installing boot server software, see:

◆ “Installing Bare Metal Restore” on page 13

Related Topics

◆ “Planning Deployment” on page 5
◆ “Managing Boot Servers” on page 203
Create Shared Resource Trees

A shared resource tree (SRT) is a collection of operating system files, NetBackup client software, and other programs needed to format drives, create partitions, rebuild file systems, and restore the original files using the NetBackup client software.

For more information about SRTs and procedures for creating and updating SRTs, see:

- “Managing Shared Resource Trees” on page 123

Related Topics
- “Planning Deployment” on page 5

Add Client Resources

Windows clients only.

Dissimilar system restores may require resources that are not included in the protected client’s saved configuration. If so, you must add them to the client configuration used for the restore (the restore configuration). Examples of such resources are:

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

These resources must be in the BMR packages pool so they are available to be added to the restore configuration. For information about adding packages to the packages pool, see “Managing Windows Packages” on page 163.

Related Topics
- “Managing Clients and Configurations” on page 167

Create Boot Media

The BMR restore process begins by booting the client from BMR prepared boot media or from a BMR boot server (UNIX and Linux only).

Microsoft Windows system must be booted by bootable media prepared by BMR, either floppy disk or CD; therefore, you must create boot media to use during the restore.

UNIX and Linux systems can be booted either over the network using a shared resource tree or by CD based boot media. If you use a network boot to begin the restore, boot media is not required.
If you will have minimal network connectivity when you restore a client, VERITAS recommends that you use boot media that contains a shared resource tree.

For more information about boot media and procedures for creating boot media, see:

◆ “Managing Boot Media” on page 153

**Verify 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.

For more information, see “Preparing to Restore a Client” on page 64.
Verify the Protection
Restoring Clients

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

**Topics**

To restore to the same client and use the most recent backup, see:

- “Restoring UNIX and Linux Clients” on page 70
- “Restoring Windows Clients” on page 79

To restore to a specific point in time, see:

- “Restoring to a Specific Point in Time” on page 88

To restore a client in which the disks are different, see:

- “Restoring to Dissimilar Disks” on page 90

*(Windows only)* To restore to a new target system, see:

- “Restoring to a Dissimilar System” on page 97

To restore NetBackup or BMR servers, see:

- “Restoring NetBackup Media Servers” on page 103
- “Restoring BMR Boot Servers” on page 106

**Restore Options**

External procedures allow you to customize the restore process. For more information, see:

- “Using External Procedures” on page 106
Related Topics

“Restore Process Overview” on page 62
“Preparing to Restore a Client” on page 64
“Storage Area Network Support” on page 116
“Multiple Network Interface Support” on page 118
“Port Usage During Restores” on page 121
“Perform a Full Backup After a Restore” on page 53

Restore Process Overview

The NetBackup BMR master server manages the restore process:

◆ The master server creates the necessary restore scripts and configuration files 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 known as the restore environment. On UNIX and Linux systems, the restore environment starts from the shared resource tree. On Windows systems, the restore environment is a temporary Windows installation on the system drive of the client (installed from the SRT).

◆ The client restore environment retrieves the restore script and configuration files from the master server.

◆ The client restore environment executes the customized restore script, which configures disks.

◆ The client restore environment performs an automated restore using the NetBackup client software, restoring all required files and data from the NetBackup server.

◆ The client reboots, which starts the restored operating system and deallocates the boot server.

◆ The temporary Windows installation is removed (Windows systems only).

◆ Dissimilar system restore tasks are completed (dissimilar system restore only).

The following figures show a standard network restore and a media restore.
Chapter 7, Restoring Clients
Preparing to Restore a Client

Before you restore a client, you must prepare to restore the client. During a prepare to restore, the NetBackup master server:

- Retrieves the client configuration from the master server database.
- Creates the restore script and configuration files 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:

- 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, VERITAS recommends that you prepare to restore immediately before you restore a system.

▼ 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 client configuration.

3. Select Actions > Prepare to Restore.

   The Prepare to Restore Client dialog box appears. Some fields may be completed depending on whether you selected a client or a client configuration.

4. Select the appropriate values for the restore.

   For descriptions of fields, see “Prepare to Restore Client Dialog Box” on page 65.

5. Click OK.

   Bare Metal Restore runs all the processes to prepare for a restore. After the processes finish, a dialog box appears.

6. Click OK.

   The client will be listed in the Tasks view, with a State of Queued.

If you ran prepare to restore to verify the protection, use the following procedure to clean up the task (the resources 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 tasks that are in an Active or Waiting state.
Preparing to Restore Client

**To clean up the restore configuration**

1. Select **Bare Metal Restore Management > Tasks** in the NetBackup Administration Console.

2. In the details pane, right click on the client for which you want to clean up the restore configuration.

3. Select **Clean Up** from the shortcut menu.

**Prepare to Restore Client Dialog Box**

Use this dialog box to select the prepare to restore options. If a client or configuration is selected in the Administration Console window, the values and options for that client or configuration are displayed or included in drop-down lists.

**Related Topics**

- “Understanding BMR Disk Recovery Behavior” on page 66

Prepare to Restore Client Dialog Box

![Prepare to Restore Client: w2k119 dialog box](image)
### Prepare to Restore Client Dialog Box Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>The name of the client. If a client was selected in the Administration Console, that client name appears.</td>
</tr>
<tr>
<td>Configuration</td>
<td>The configuration to use for the restore. The drop-down list includes all configurations for the client. If a configuration was selected in the Administration Console, that configuration appears.</td>
</tr>
<tr>
<td>Shared resource tree</td>
<td>The shared resource tree that contains the resources for restoring the client. Select a shared resource tree that has software that matches the configuration of the client (including operating system version and level, service or maintenance pack or level, any VERITAS volume manager used on the protected client, and so on). You can use the Configuration Summary dialog box to help determine the software in a client’s configuration (see “Configuration Summary” on page 181).</td>
</tr>
<tr>
<td>Restore system disks/volumes only</td>
<td>Restore only those volumes that contain the operating system. For more information, see “Understanding BMR Disk Recovery Behavior” on page 66.</td>
</tr>
<tr>
<td>Make available volumes on non-restored disks after the system is restored</td>
<td>Import the volumes. For more information, see “Understanding BMR Disk Recovery Behavior” on page 66.</td>
</tr>
<tr>
<td>Run external procedures</td>
<td>Run external procedures during the restore. See “Using External Procedures” on page 106.</td>
</tr>
<tr>
<td>Enable logging</td>
<td>Write messages to the log file on the master server during the restore. Enable logging if you have adequate space in the file system on which the NetBackup log directory resides on the master server.</td>
</tr>
<tr>
<td>Use quick formatting</td>
<td><em>(Microsoft Windows clients only)</em> Use quick formatting.</td>
</tr>
</tbody>
</table>

### Understanding BMR Disk Recovery Behavior

BMR either restores or imports disks during a restore, defined as follows:
Preparing to Restore a Client

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

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

- **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 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%, %SystemRoot%, and %TEMP% are restored. On Active Directory servers, BMR also restores disks that contain the Active Directory system, database, and log files.

- **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. For more information, see the table “Actions for Disk Classes” on page 68.

The following are the disk classes:

- **System disks** contain the operating system files required to boot the system.

- **Non-system 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 not able to be restored. Typically these are SAN devices. You may not know that these disks cannot be restored until you attempt a restore; if required for a restore, you will be forced to do a dissimilar disk restore (DDR).
  - **Shared disks** are shared with another system using clustering software and may not be controlled by the client during or after the restore.
  - **Missing disks** may or may not have been used and are no longer attached to the system. These disks will be in the restore configuration. For the actions you should perform for missing disks, see the table “Actions for Disk Classes” on page 68.

- **New disks** are attached to the system in previously unused locations and used by any volume or volume group. New disks are not in the original configuration.
Preparing to Restore a Client

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

The following table describes how BMR processes disks depending on the two prepare to restore options:

**BMR Disk Actions**

<table>
<thead>
<tr>
<th>Restore Options</th>
<th>System Disks</th>
<th>Nonsystem Disks</th>
</tr>
</thead>
<tbody>
<tr>
<td>System only$^1$ = true</td>
<td>Restorable</td>
<td>Nonrestorable</td>
</tr>
<tr>
<td>Import$^2$ = true</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restore</td>
<td>Import</td>
</tr>
<tr>
<td>System only = true</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Import = false</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restore</td>
<td>No action</td>
</tr>
<tr>
<td>System only = false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Import = true</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restore</td>
<td>Restore if possible otherwise import</td>
</tr>
<tr>
<td>System only = false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Import = false</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restore</td>
<td>Restore</td>
</tr>
</tbody>
</table>

1. System only is the **Restore system disks/volumes only** option for prepare to restore.

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

The following table describes the actions BMR performs for each disk class and any action you should perform:

**Actions for Disk Classes**

<table>
<thead>
<tr>
<th>Restore Options</th>
<th>System Disks</th>
<th>Nonsystem Disks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Restorable</td>
<td>Nonrestorable</td>
</tr>
<tr>
<td>System only$^2$ = true</td>
<td>Restorable</td>
<td>Nonrestorable</td>
</tr>
<tr>
<td>Import$^3$ = true</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restore</td>
<td>Import</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

NetBackup Bare Metal Restore System Administrator’s Guide
Actions for Disk Classes (continued)

<table>
<thead>
<tr>
<th>Restore Options</th>
<th>System Disks</th>
<th>Nonsystem Disks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Restorable</td>
<td>Nonrestorable</td>
</tr>
<tr>
<td>System only = true</td>
<td>Restore</td>
<td>No action</td>
</tr>
<tr>
<td>Import = false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System only = false</td>
<td>Restore</td>
<td>Restorable</td>
</tr>
<tr>
<td>Import = true</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System only = false</td>
<td>Restore</td>
<td>Restorable</td>
</tr>
<tr>
<td>Import = false</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. To avoid conflicts with other cluster nodes that may be using 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 not holding the share actively during the restore.

2. System only is the **Restore system disks/volumes only** option for prepare to restore.

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

The following table describes the import action for each operating system or volume manager:

**Import Action**

<table>
<thead>
<tr>
<th>OS and/or Volume Manager</th>
<th>What Import Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX Logical Volume Manager</td>
<td>Run <code>importvg</code> at restore time or during first boot</td>
</tr>
<tr>
<td>HP-UX Logical Volume Manager(^1)</td>
<td>Merge <code>lvmtab</code>, merge <code>fstab</code></td>
</tr>
<tr>
<td>Linux</td>
<td>Merge <code>fstab</code></td>
</tr>
</tbody>
</table>

---

Chapter 7, Restoring Clients
Import Action (continued)

<table>
<thead>
<tr>
<th>OS and/or Volume Manager</th>
<th>What Import Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris</td>
<td>Merge vfstab^2</td>
</tr>
<tr>
<td>VERITAS Storage Foundation for Windows</td>
<td>Assign drive letter via MountedDevices, run vxdg import</td>
</tr>
<tr>
<td>VERITAS Volume Manager^3</td>
<td>Run vxdg import, merge fstab^2</td>
</tr>
<tr>
<td>Windows^4</td>
<td>Assign drive letter via MountedDevices</td>
</tr>
</tbody>
</table>

1. 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 will be available. If entries remain in /etc/fstab for the file systems, those file systems will be available.

2. /etc/fstab and /etc/vfstab merging: During a merge, BMR may remove entries in the /etc/fstab or /etc/vfstab files by commenting them out.

3. Auto import. VxVM has the ability (a disk group option) to import disk groups automatically. If there are entries in the /etc/fstab and /etc/vfstab files, the file systems will be available without BMR having to take action.

4. Windows import. Without import, only drive letters that were recreated will be assigned after restore. With import, drive letters assigned to volumes on Trusted disks will be assigned to the same location after the restore. If the volume does not exist or has moved, you must edit the MountDevices registry key.

---

**Restoring UNIX and Linux Clients**

Use these procedures for a standard restore (also known as a *self restore*, which is a restore to the same system and disks). Before you do a standard restore, you must run the prepare to restore operation using the current, saved configuration.

UNIX and Linux clients can boot either over the network or from CD media.

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

**Tasks**

- “Restoring UNIX and Linux Clients Using Network Boot” on page 71
- “Restoring UNIX and Linux Clients Using Media Boot” on page 75
Related Topics  “Preparing to Restore a Client” on page 64
  “Using External Procedures” on page 106
  “Perform a Full Backup After a Restore” on page 53

Restoring UNIX and Linux Clients Using Network Boot

In a network boot, the BMR client boots from the shared resource tree on the BMR boot server.

To network boot clients, BMR uses:
  ♦ bootp or bootparam protocol for UNIX clients.
  ♦ dhcp for Linux clients

How you boot a machine over the network depends on its manufacturer and model. Refer to the appropriate section for your system:

  ♦ “AIX Network Boot” on page 71
  ♦ “Solaris Network Boot” on page 74
  ♦ “HP-UX Network Boot” on page 72
  ♦ “Linux Network Boot” on page 74

AIX Network Boot

The network interface configuration, speed, and duplex mode during AIX booting (either network boot or media boot) may be set to auto-negotiate or 10 half duplex, which 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 prior to a BMR restore.

AIX system restore requires certain information and resources. The information varies according to architecture, but can include:

  ♦ 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 has finished and the client reboots itself, it is completely restored.

**To network boot an AIX system that has AIX installed**

This method updates the NVRAM with the proper addresses for the BMR boot server, client, and gateway address. This method boots via `bootp` from the BMR boot server. If the boot server does not answer the `bootp` request, the machine boots from the hard drive. This method only works when the BMR client is properly prepared for restore.

**Caution**  Do not perform this procedure unless you intend to do a restore. Preparing a client for restore may result in a restore.

1. Prepare to restore the client.
   
   For procedures, see “Preparing to Restore a Client” on page 64.

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

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

**HP-UX Network Boot**

HP-UX system restore requires certain information and resources. The information varies according to architecture, but can include:

- 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 has finished and the client reboots itself, it is completely restored.

**To network boot an HP-UX client**

1. Prepare to restore the client.
   
   For procedures, see “Preparing to Restore a Client” on page 64.
2. Ensure that the client is powered down.

3. Turn the client on.

4. Press any key when the following message appears.
   To discontinue, press any key within 10 seconds.
   The Main Menu opens.

5. 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:
     \[ \text{boot lan} \]
   ◆ If there is more than one Ignite server on the subnet or if you are using a boot helper to boot from an Ignite server on a different subnet, specify the Ignite server to boot from by using the following command (replace \textit{x.x.x.x} with the IP address of the Ignite server and \textit{y.y} with the gateway):
     \[ \text{boot lan.x.x.x.y.y} \]

6. Enter \textbf{No} when the prompt asks about interacting with IPL.

7. If the client is a workstation, select the operating system language, by number.
   For example, US English is \textbf{61}.

8. After entering 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 \textbf{Run a Recovery Shell}. Wait while DHCP searching occurs and until the Network Configuration menu opens. Interrupting DHCP searching may cause the BMR restore to fail.

10. Answer the following prompts:
    ◆ Hostname:
    ◆ Internet Protocol Address:
    ◆ Subnet mask:
    ◆ Ignite Server Address (this is typically the BMR boot server):

11. Use the arrow key to scroll to \textbf{OK} and press Enter.
    The system boots from the network.
Linux Network Boot

All the information required for a Linux network boot is gathered during the prepare to restore operation. After the prepare to restore, boot the client and the restore will begin.

▼ To network boot a Linux client

1. Prepare to restore the client.
   For procedures, see “Preparing to Restore a Client” on page 64.

2. Ensure that the client is powered down.

3. Turn the client on.

4. PXE boot the client according to the hardware vendor instructions.
   On some systems, the BIOS will display a message indicating 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.
   The following message appears:
   Press ENTER to start Bare Metal Restore boot:

   Press the ENTER key, or wait 20 seconds for startup to begin automatically.

5. Either press the Enter key or wait until the system boots.
   The system will boot and the restore will begin, with no further user intervention required.

Solaris Network Boot

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 has finished and the client reboots itself, it is completely restored.

▼ To network boot a Solaris client

1. Prepare to restore the client.
   For procedures, see “Preparing to Restore a Client” on page 64.
2. Ensure that the client is powered down.
3. Turn the client on.
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 UNIX and Linux Clients Using Media Boot

Restoring using media boot requires that you first create bootable media. For procedures, see “Creating Boot Media for UNIX and Linux” on page 155.

The procedure for booting the client system depends on the manufacturer and model. See the following:

- “AIX Media Boot” on page 75
- “HP-UX Media Boot” on page 76
- “Linux Media Boot” on page 77
- “Solaris Media Boot” on page 78

AIX Media Boot

The network interface configuration, speed, and duplex mode during AIX booting (either network boot or media boot) may be set to auto-negotiate or 10 half duplex, which 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 prior to a BMR restore.

▼ To media boot an AIX client

1. Prepare to restore the client, using the SRT you created on the bootable media.
   See “Preparing to Restore a Client” on page 64.

2. Boot the client from the boot media you created. For instructions about booting from a CD, see the IBM hardware documentation.
3. The BMR process prompts you for the following:
   - 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

   After you enter the required information, the restore begins.

**HP-UX Media Boot**

▼ **To media boot an HP-UX client**

1. Prepare to restore the client, using the SRT you created on the bootable media.
   For procedures, see “Preparing to Restore a Client” on page 64.

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

3. Turn the client off, then on.

4. When 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 in determining this information.

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

7. Answer **No** to the Interact with IPL prompt.

8. Answer **Yes** to the Run a Recovery Shell prompt.

9. Answer **Yes** to the Start Networking prompt.

10. Enter the default LAN device when prompted to Choose the network interface to boot from.
You must enter the default LAN because the firmware will use 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 to do so:
   ◆ Hostname
   ◆ IP address
   ◆ Default gateway
   ◆ Subnet mask

12. Answer No at the Is this network information temporary prompt.

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

14. The BMR process prompts you for the following:
   ◆ 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.

**Linux Media Boot**

▼ To media boot a Linux client

1. Prepare to restore the client, using the SRT you created on the bootable media. For procedures, see “Preparing to Restore a Client” on page 64.

2. Insert the bootable CD into the CD-ROM drive.
   On some systems, you may have to modify the BIOS settings so that the system will boot from the CD-ROM drive. Consult your hardware documentation for details.

3. Turn the client off, then on.
   The following message appears:
   Press ENTER to start Bare Metal Restore boot:
Press the ENTER key, or wait 20 seconds for startup to begin automatically.

4. The BMR restore process prompts you for the following:
   - 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

After you enter the required information, the restore begins.

**Solaris Media Boot**

▼ **To media boot a Solaris client**

1. Prepare to restore the client, using the SRT you created on the bootable media.
   For procedures, see “Preparing to Restore a Client” on page 64.

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

3. Turn the client off, then 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. The BMR process prompts you for the following:
Restoring Windows Clients

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

Microsoft Windows clients require bootable media to boot the system and begin the restore process. How much you interact with the restore process depends on whether you are using generic or custom boot media, your choices when you create the boot media, and what BMR discovers about the client during the restore process. Also, using external procedures can reduce your interaction with the restore process.

Information about the restore is grouped into the following topics. Refer to each topic for procedures and information. A restore may not include every topic (for example, you do not enter client information if you use customized boot media).

**Tasks**

- “Preparing for a Windows Restore” on page 79
- “Booting the Client” on page 80
- “Entering Client Information” on page 81
- “Entering Partition Information” on page 83
- “Installing Windows into a Temporary Location” on page 86
- “Rebuilding Partitions and Restoring Files” on page 87

**Related Topics**

- “Using External Procedures” on page 106
- “Perform a Full Backup After a Restore” on page 53

**Preparing for a Windows Restore**

Before you do a standard restore, you must run the prepare to restore operation using the current, saved configuration. You also must create media to use to boot the client. For procedures, see:
Restoring Windows Clients

◆ “Creating Boot Media for Windows” on page 158.
◆ “Preparing to Restore a Client” on page 64

Booting the Client

To boot the client, insert the boot media in the appropriate drive and reboot the system.

**Note** If the client supports PXE, you may be able to network boot the client using PXE. For more information, see “PXE Boot” on page 81.

The BMR restore process loads from the boot media and begins the restore. The progress and status of the restore are displayed in a BMR status screen.

- A yellow arrow indicates that the activity is currently in progress.
- A green check marks each activity as it is completed.
- A red X indicates a failed activity.

At any time, press F1 to see more information about the process currently executing or press Esc to quit. The F1 or Esc keys are processed only after the current step completes.
PXE Boot

If the Windows client supports the Pre-boot Execution Environment (PXE), you may be able to network boot the client. PXE boot is useful if the client does not have a drive that supports BMR bootable media.

PXE is one of the components of the Wired for Management open-industry specification that allows a workstation to boot from a server on a network.

**Note** PXE boot is enabled by third-party server software. For instructions about and support for PXE boot, consult your PXE vendor’s documentation and support.

▼ To prepare for PXE boot

1. Create a BMR boot floppy for the client.

2. Use the boot floppy to create a PXE bootable image.
   For procedures, see your PXE vendor’s documentation.

3. Configure the PXE boot server to use the previously created bootable image for the BMR client.
   For procedures, see your PXE vendor’s documentation.

4. Boot the BMR client and use the PXE boot option.

Entering Client Information

*Generic boot floppy only.*

Generic boot floppy media does not contain any client-specific information; therefore, you must enter client-specific information during the restore process. Some or all of the following prompts appear during the restore process. For each prompt, provide the appropriate value(s).

**Client Information**

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the client computer name</td>
<td>The name of the computer. It is possible that the computer name is not the same as the name used in the NetBackup policy that backs up the client.</td>
</tr>
<tr>
<td>Does this client use DHCP (y/n)</td>
<td>If you answer y, the remaining networking prompts do not appear.</td>
</tr>
</tbody>
</table>
## Client Information (continued)

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the IP address of the client</td>
<td>The IP address of the interface. Appears if DHCP is not used.</td>
</tr>
<tr>
<td>Enter the subnet mask of the client</td>
<td>The network mask for the client. Appears if DHCP is not used.</td>
</tr>
<tr>
<td>Enter the default gateway of the client</td>
<td>The gateway to use for the client. Appears if DHCP is not used.</td>
</tr>
<tr>
<td>Set slot number (y/n)?</td>
<td>Answer y to enter the slot number in which the network interface card is located. Usually, you do not have to enter a slot number; however, in rare circumstances, the DOS portion of the restore may fail if a slot number is not specified. To identify the failure and the corrective action required, see “Restore Fails on Windows Client with Multiple Identical NICs” on page 208.</td>
</tr>
<tr>
<td>Enter the slot number</td>
<td>Appears only if you chose to enter a slot number. Ensure that the slot number you enter matches the slot that DOS identifies as the slot in which the NIC used for the restore is installed.</td>
</tr>
<tr>
<td>Enter boot server’s name</td>
<td>The name of the boot server.</td>
</tr>
<tr>
<td>Enter boot server’s IP address</td>
<td>The IP address of the boot server.</td>
</tr>
<tr>
<td>Enter the SRT name</td>
<td>The name of the shared resource tree. Use the same SRT that was used for the prepare to restore operation.</td>
</tr>
<tr>
<td>Enter the NetBackup client name</td>
<td>The name of the client used in the NetBackup policy that backs up the client.</td>
</tr>
<tr>
<td>Enter the client configuration name</td>
<td>The name of the configuration to use for the restore. After you enter the configuration name, the restore process initializes the network interface and retrieves additional client information. After retrieving client information, the restore process prompts you for partition information</td>
</tr>
</tbody>
</table>

If you enter incorrect information, you can reboot the system to begin the recovery process again.
To re-enter client information

1. Enter Ctrl+Alt+Delete (or press the reset button on the computer)

2. When the message Switching to GUI mode appears on the screen, press the Esc key repeatedly until you see the message Do you really want to quit (y/n).

3. Type y then press Enter

4. Reboot the system.

5. Enter the correct data at the next series of prompts.

Entering Partition Information

BMR partitions the disk drives in the client system. After the client information is retrieved, the BMR restore process asks a series of questions about disk partitions; the questions that appear depend on how the boot media was created and the disks in the client. For each prompt, provide the appropriate value(s).

After you enter the appropriate information, the client reboots, formats drive C, retrieves files required by BMR from the SRT, and then the Windows installation process installs Windows into a temporary repair location.

Partition Information

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Following disks are found in the system: &lt;br&gt; lista of disks &lt;br&gt; First disk in the list will be used for the BMR restore partition. Press F2 to continue.</td>
<td>The restore partition contains the temporary Windows repair installation. Note that all data on the restore partition may be lost. &lt;br&gt; Review the list of disks and make sure, based on the description and partition list, that BMR can create the restore partition on the first disk in the list. &lt;br&gt; If the first disk in the list should not be reformatted to create the BMR restore partition, power down the client system, change the disk cabling or disconnect disks until the disk where the BMR restore partition can be created appears as the first disk in the list, then start the client system to restart the restore process.</td>
</tr>
</tbody>
</table>
## Partition Information (continued)

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you want to save a partition&lt;br&gt;(y/n)</td>
<td>Appears only if using a customized boot floppy. Computers may have a special system partition, which is an area of the hard drive that contains configuration, diagnostic, and maintenance utilities usually provided by the vendor of the computer. To save a partition, enter y. To delete any existing partitions and create the working partition required by BMR, enter n. After repartitioning completes, the system reboots.</td>
</tr>
<tr>
<td>Could not find any partitions to save! Do you want to proceed&lt;br&gt;(YES/NO)?</td>
<td>Appears if you chose to save a partition during boot media creation and no partitions are found that can be saved. To stop the restore process, type NO and press Enter. To continue with the restore and create the working partition required by BMR, type YES and press Enter.</td>
</tr>
<tr>
<td>Which partition do you want to save? (1, 3, or 0 if none).</td>
<td>Appears if you chose to save a partition during boot media creation and one or more partitions are found that can be saved. The partitions listed depend on the partitions on the client. The display includes the partition number, the partition’s start cylinder (in decimal), and the partition size (only the partitions that can be saved are displayed). Enter a partition number to save or entry 0 to not save any partition, then press Enter. For more information, see “Identifying the Vendor Partition During a Restore” on page 85. The restore process saves any selected partition, deletes the other partitions, and then creates the working partition required by BMR.</td>
</tr>
<tr>
<td>All partitions will be erased. Type YES to confirm, or type NO to abandon. Proceed with repartitioning&lt;br&gt;(YES/NO)?</td>
<td>Appears if you chose to have a safety prompt during boot media creation and then you chose not to save any partitions during the restore (that is, if you entered 0 to the previous prompt). To stop the restore process, type NO and press Enter. To repartition the disk, type YES and press Enter.</td>
</tr>
</tbody>
</table>
### Identifying the Vendor Partition During a Restore

BMR can save vendor partitions, which are an area of the hard drive that contains configuration, diagnostic, and maintenance utilities usually provided by the vendor of the computer. The partition must meet the following requirements (most vendor partitions meet these):

- The vendor partition must be less than 1 GB.
- The vendor partition must start at the beginning of the drive.
- The vendor partition must not be recognized as a DOS primary partition. DOS can only create a single primary partition.

#### To identify the vendor partition to save

- If more than one partition appears, choose the one with Start Cylinder zero.
Installing Windows into a Temporary Location

After BMR files are retrieved from the SRT, the client reboots, the BMR status screen appears, and the restore process continues. The Microsoft Windows installation process begins to install Windows into a temporary repair location.

This process usually takes 10 to 30 minutes; the time can vary depending on system speed and network behavior (if installing the restore environment from an SRT on a boot server).

Caution  Do not remove the boot media until prompted to do so.

After the first phase of Windows installation is completed, you are prompted to remove the boot media so the client can reboot and use the temporary Windows installation. If you do not remove the boot media, the restore process begins again.

After Windows installation is finished, BMR manages the remainder of the restore process.

No interaction is required during the Windows installation.

The temporary installation is removed from the system after the restore process is finished.
Rebuilding Partitions and Restoring Files

After the temporary Windows installation occurs, the system reboots and the BMR Restore Wizard appears.

The Restore Wizard creates all the required partitions, formats them, and restores the files in each of the partitions. The Details box on the Restore Wizard screen shows details about the current task in progress.

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

Each task is checked as it is completed. A red X indicates failure; if a failure occurs, a Retry wizard appears that shows the task(s) to be retried. Before retrying the task, you can examine the restore log to determine the reasons for failure and correct the problem:

1. To access the temporary Windows installation menus and taskbar, click on the computer icon at the top left of the BMR Restore Wizard screen.
2. Open a command window.
3. Run the following `vxlogview` command (in the `C:\BMR\NBU\BIN` folder):

```none
```
Restoring to a Specific Point in Time

```
vxlogview -i 131
```

In most cases, correcting the problem described in the logs and retrying the failed task is sufficient to complete a successful restore. If a problem persists, contact your VERITAS support representative.

After all tasks are completed, the system reboots. Other action may be required:

- For standard restores, you should log into the client as Administrator so that the `bmrcleanup` task will remove the repair partition and perform other clean up tasks such as updating the client state.
- For dissimilar system restores, you may have to log into the client as Administrator to finish configuring the network information. For more information, see “First Logon” on page 103.

**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 you want to restore to.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>“Creating a Point in Time Restore Configuration” on page 89</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related Topics</td>
<td>“Understanding the Point in Time Restore Process” on page 88</td>
</tr>
<tr>
<td></td>
<td>“When to Use Point in Time Restore” on page 89</td>
</tr>
<tr>
<td></td>
<td>“Preparing to Restore a Client” on page 64</td>
</tr>
<tr>
<td></td>
<td>“Perform a Full Backup After a Restore” on page 53</td>
</tr>
</tbody>
</table>

**Understanding 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.
When to Use Point in Time Restore

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. The point in time restore feature of BMR can be used when any of the following have occurred:

◆ A hardware change has destabilized the system. There may be cases in which the software 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 is for creating the restore configuration for a point in time restore for any client type. After you create the restore configuration, you 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 on the saved configuration for the client (the configuration labelled current), then select New from the shortcut menu.
   
The New Configuration dialog box appears.

3. Enter a name for the new configuration.

4. Click Retrieve from NetBackup then 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 are restoring. Normally; backup jobs occur on separate days and data streams within the same backup job are separated by seconds or minutes.
5. 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.

6. Continue by following the procedures in “Restoring UNIX and Linux Clients” on page 70 or “Restoring Windows Clients” on page 79.

Restoring to Dissimilar Disks

You can restore a protected client even if the disk drives have been 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.

Tasks

“Restoring to Dissimilar Disks for UNIX and Linux Clients” on page 91
“Restoring to Dissimilar Disks for Windows Clients” on page 94

Related Topics

“Understanding the Dissimilar Disk Restore Process” on page 90
“When to Use Dissimilar Disk Restore” on page 91
“Perform a Full Backup After a Restore” on page 53

Understanding 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 deployed 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), initialize that configuration with the new disk layouts, and 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 that BMR have a record of the layouts of the new disks (for example, if you perform a discovery operation (UNIX and Linux only) on the client or if another protected client has the same disks.
During the restore. If you are performing 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, you use the BMR disk mapping utility in the NetBackup Administration console on the master server.

◆ For Windows clients, you can choose to map on the client or on the master server using the BMR disk mapping utility in the NetBackup Administration console. The restore environment on the client has a small screen size, so mappings are easier to do on the master server.

### When to Use Dissimilar Disk Restore

You should use dissimilar disk restore when:

◆ A physical disk was replaced.

◆ The size of one or more disks has decreased and cannot contain the same volume arrangement.

◆ The location of one or more disks has changed.

◆ 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.

---

**Caution**  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.

### Restoring to Dissimilar Disks for UNIX and Linux Clients

Use the following procedures to restore to a system in which the disks are different:

◆ “Creating a Restore Configuration for DDR” on page 92

◆ “Restoring to Dissimilar Disks” on page 92

**Notes 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.
Restoring to Dissimilar Disks

- Linux LVM volume groups that have physical volumes created on top of multidevices cannot be mapped with the same configuration. The physical volumes are mapped to either disks or partitions but not a multidevice.

Creating a Restore Configuration for DDR

*UNIX and Linux systems.*

Use the following procedure 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; to begin a restore and perform disk mapping during the restore itself, see “Restoring to Dissimilar Disks” on page 92.

▾ To create a UNIX or Linux DDR configuration

1. Discover the configuration of the new disks. For procedures, see “Discovering a Configuration” on page 174.

2. Create an editable restore configuration by copying the current configuration. For procedures, see “Copying a Configuration” on page 172.

3. Open the Change Configuration dialog box for the restore configuration. For procedures, see “Modifying a Configuration” on page 177.

4. Initialize the restore configuration with the disk information from the discovered configuration and then map the the original volume configuration to the new disks. For procedures, see “Volumes” on page 196.

After you finish mapping, perform the DDR restore procedure in “Restoring to Dissimilar Disks” on page 92.

Restoring to Dissimilar Disks

*UNIX and Linux systems.*

Use the following procedure to restore to dissimilar disks. If you did not prepare a restore configuration in advance, BMR creates an editable restore configuration during this process.
To perform a UNIX or Linux dissimilar disk restore

1. Prepare to restore the client.
   Use the current configuration or a restore configuration if you prepared one in advance. For procedures, see “Preparing to Restore a Client” on page 64.

2. Begin the restore by booting the client using either network or media boot. For procedures, see “Restoring UNIX and Linux Clients” on page 70.
   If you prepared to restore using a configuration in which the protected system’s volume configuration was 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. Continue to step 3.

3. If you prepared to restore using a configuration that cannot be edited, BMR creates an editable restore configuration by copying 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:
   Enter a name for the editable restore configuration.

4. 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:
   Enter a name for the discovered configuration; BMR saves the discovered configuration. Later, you will import the disk layouts from this discovered configuration into the restore configuration.

5. After the discovered configuration is saved, do the following in the NetBackup Administration Console on the master server:
   a. Open the Change Configuration dialog box for the restore configuration. For procedures, see “Modifying a Configuration” on page 177.
   b. Initialize the restore configuration with the new disk layout from the discovered configuration and then map the original volume configuration to the new disks. For procedures, see “Volumes” on page 196.

6. After you finish mapping, prepare to restore and then restore the client, using the edited restore configuration. For procedures, see “Restoring UNIX and Linux Clients” on page 70.
If the disk mapping in the restore configuration is incomplete, BMR will once again enter DDR mode so you can continue to map volumes to disks.

Restoring to Dissimilar Disks for Windows Clients

Use the following procedures to restore to a system in which the disks are different:

- “Creating a Restore Configuration for DDR” on page 94
- “Restoring to Dissimilar Disks” on page 95

Notes for Windows DDR

- The system drive is always mapped and cannot be moved; however, you can resize it if you are mapping disks before the restore.
- Original disks and their volumes that were clustered cannot be mapped.
- Discovered disks that have the same disk signature as an original disk that was clustered cannot be mapped.

Creating a Restore Configuration for DDR

*Windows systems.*

Use the following procedure to create an editable restore configuration before you begin the restore process.

BMR must have a record of the new disk layouts so you can import them into the restore configuration. If the target disks are the same as disks from another protected client, you can import the disk layout from that client’s configuration into the editable restore configuration. Alternatively, you can install NetBackup client software on the new disks and perform a full BMR backup; the configuration, including disk layouts, will be saved in that client’s configuration and can be imported into the restore configuration.

You do not have to create a restore configuration before you begin the restore; to begin a restore and perform disk mapping during the restore itself, see “Restoring to Dissimilar Disks” on page 95.

To create a Windows DDR configuration

1. Create an editable restore configuration by copying the current configuration. For procedures, see “Copying a Configuration” on page 172.

2. Open the Change Configuration dialog box for the restore configuration. For procedures, see “Modifying a Configuration” on page 177.
3. Initialize the restore configuration with the new disk layouts and then map the original volume configuration to the new disks. For procedures, see “Volumes” on page 196.

After you finish mapping, perform the DDR restore procedure in “Restoring to Dissimilar Disks” on page 95.

Restoring to Dissimilar Disks

Windows systems.

Use the following procedure to restore to dissimilar disks.

If you did not prepare a restore configuration in advance, BMR creates an editable restore configuration during this process. You can choose to perform the mapping on the client or on the master server using the NetBackup Administration console. The restore environment has a small screen size, so mapping is easier to do on the master server.

To prepare boot media, see “Creating Boot Media for Windows” on page 158.

To perform a Windows dissimilar disk restore

1. Prepare to restore the client.
   Use the current configuration or a restore configuration if you prepared one in advance. For procedures, see “Preparing to Restore a Client” on page 64.

2. Begin the restore by booting the client. For procedures, see “Booting the Client” on page 80.

3. If required, enter the client information (generic boot floppy only). For procedures, see “Entering Client Information” on page 81.
   If you prepared to restore using a configuration in which the protected system’s volume configuration was already mapped to the new disks, the restore proceeds as a standard restore. To continue, see “Entering Partition Information” on page 83.
If BMR detects that the disks are different (after the last reboot of installing Windows into a temporary location), a disk mapping utility screen appears:

![Disk Mapping Utility Screen]

4. Select whether to do the mapping on the client or on the master server using the NetBackup Administration Console.

The restore environment on the client has a small screen size, so mappings are easier to do on the master server.

5. If you chose to map on the master server, go to “Windows DDR Mapping on the Server” on page 96. If you chose to map on the client, the disk mapping utility appears; continue with step 6.

6. Map the original volume configuration to the new disks. BMR initializes the editable restore configuration with the new disk information, so you can begin mapping immediately. For procedures, see “Volumes” on page 196.

7. After mapping all the elements you want to move to the new disks, click Done.

The restore continues with rebuilding partitions and restoring files.

To continue, see “Rebuilding Partitions and Restoring Files” on page 87.

**Windows DDR Mapping on the Server**

If you choose to map on the server, two possibilities exist:
Restoring to a Dissimilar System

If the configuration used during the prepare to restore operation can be edited, BMR initializes that configuration with the new disk layout information, and you do the mapping in that configuration.

If the configuration used during the prepare to restore operation is the current configuration (that is, the saved configuration that cannot be edited), BMR creates a configuration you can edit, which is saved on the master server, and then you do the mapping in that configuration. The new configuration will include the volume information from the protected client and the layout of the new disks in the client.

To map on the server

1. If prompted by BMR for a name for the discovered configuration, enter the name to use for the new configuration.
   The configuration will appear for the client in the Bare Metal Restore Clients view in the NetBackup Administration Console. If the configuration does not appear, click Refresh.

2. Open the Change Configuration dialog box for the new, editable restore configuration. For procedures, see “Modifying a Configuration” on page 177.

3. Map the original volume configuration to the new disks. BMR initializes the editable restore configuration with the new disk information, so you can begin mapping immediately. For procedures, see “Volumes” on page 196.

4. After mapping all the elements you want to move to the new disks, click Done.
   The restore continues with rebuilding partitions and restoring files.
   To continue, see “Rebuilding Partitions and Restoring Files” on page 87.

Restoring to a Dissimilar System

Windows systems only.

You can restore a protected Windows client to a completely different system. In a dissimilar system restore, you create a restore configuration that maps the attributes of the protected system to the new, target system. A dissimilar system restore handles differences such as disk controllers and network cards, differences in system bus architecture, and motherboard changes that require a different hardware abstraction layer (HAL) and/or kernel.
If the disk(s) on the target system are different than on the protected system, disk and volume mapping (as performed with a dissimilar disk restore) also will be required.

**Tasks**
“Restoring to a Dissimilar System” on page 99

**Related Topics**
“DSR Troubleshooting” on page 210
“Perform a Full Backup After a Restore” on page 53

**When to Use Dissimilar System Restore**

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

Performing a DSR is useful in the following situations:

- You have changed the preferred vendor for a class of systems in your enterprise.
- You are migrating an application from older hardware to the newer hardware.
- Your system has suffered 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 are staging and verifying an application at a test site with different hardware from the production site (you can migrate the application from test to production).

You should use DSR when any of the following conditions apply:

- The target system has a disk controller that the protected system did not have.
- The target system has a network card that the protected system did 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 had. (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.)

**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.
Restoring to a Dissimilar System

The DSR process has the following steps:

1. Determining Hardware Differences.
2. Creating an Editable DSR Configuration.
3. Adding NIC and MSD Drivers.
5. Changing Network Interfaces.
7. Creating Boot Media.
8. Restoring the Client.

Determining Hardware Differences

The most critical and difficult task in the DSR process is determining the hardware differences between the protected system and the new target system. Before the restore, you need to determine the following:

◆ Whether the mass storage devices (MSDs) and network interface cards (NICs) are different on the target system.

◆ The media access control (MAC) addresses of the NICs of the target system. Without the MAC addresses, the BMR restore procedure will not be able to add the network properties of the target system to that of the restore configuration.

How you determine the MSD and NIC information of the target system depends on its status. The following are examples:

◆ If the target system has the same base operating system as the protected client, install the NetBackup client software and then perform a full backup using a policy configured for BMR. The target system’s configuration will be saved on the master server (including MAC addresses), and the device drivers will be added to the packages pool.

This method collects all of the system information required for a DSR, including the MAC addresses of the NICs and the disk layouts so you can perform disk mapping before the restore (if the disks are different).
Restoring to a Dissimilar System

◆ If the target system has the same base operating system as the protected client, do the following to capture the driver information of the target system:

a. Install the NetBackup client software.

b. Run the following command to extract the MSD and NIC drivers:

   `%ProgramFiles%\VERITAS\NetBackup\bin\bmrsavecfg -infoonly`

   The driver files are written to the following directory:

   `%ProgramFiles%\VERITAS\NetBackup\BareMetal\Client\data`

c. Add the drivers to the packages pool; see “Managing Windows Packages” on page 163.

If you use this method, you also will have to determine the MAC addresses of the NICs in the target system. In addition, if the disks of the target system are different, you can only do DDR disk mapping during the restore.

◆ If the target system is new, use the manufacturer’s web site to determine the drivers used by the machine. Download the drivers used on the target system from the manufacturer’s web site and then add them to the packages pool. For instructions, see “Managing Windows Packages” on page 163.

If you use this method, you also will have to determine the MAC addresses of the NICs in the target system. In addition, if the disks of the target system are different, you can only do DDR disk mapping during the restore.

Creating an Editable DSR Configuration

You must create a configuration to use for the restore of the protected client. Create the DSR configuration by copying an existing configuration of the protected client.

For example, if you are restoring client protected to system target, create a configuration named dsr_to_target by copying the current configuration of client protected.

To copy a configuration, see “Copying a Configuration” on page 172.

After you create the DSR configuration, open the Change Configuration dialog box so you can modify the configuration as described in the following sections. See “Change Configuration Dialog Box” on page 180.
Adding NIC and MSD Drivers

The DSR configuration must include the NIC and MSD drivers required by the target system. The target system drivers were added to the packages pool when you performed one of the procedures described in “Determining Hardware Differences” on page 99, so they will be available to add to the DSR configuration.

To add drivers, you select them in the Available drivers window of the configuration’s Drivers dialog box and then add them to the Drivers to be used during restore window. For more information, see “Drivers” on page 183.

If you added the drivers to the packages pool by saving the target system’s configuration or by extracting the drivers from the target system, the driver description includes the name of the target system, which can help you identify which drivers are required for the target system.

Also remove any drivers from the DSR configuration that are used by the protected system but not by the target system.

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.

Adding Windows Hotfixes

You must add the Windows hotfixes from the protected client that are required for a DSR to the DSR configuration. BMR identifies which hotfixes are required in the DSR configuration’s Hotfixes dialog box: if Yes is displayed in the Dissimilar System Restore Requirement column, you must add that hotfix to the DSR configuration.

Hotfixes are not added to the BMR packages pool when a configuration is saved; therefore, you have to add the hotfixes to the packages pool before you can add them to the DSR configuration. To add hotfixes to the packages pool, see “Managing Windows Packages” on page 163. You can download Windows hotfix installation executable files from the Microsoft web site.

After you add hotfixes to the packages pool, add them to the DSR configuration. Similar to drivers, you select them in the Available hotfixes window of the configuration’s Hotfixes dialog box and then add them to the Hotfixes to be used during restore window. For more information, see “Hotfixes” on page 188.

Changing Network Interfaces

You must change the network interfaces and network identities in the DSR configuration.
Restoring to a Dissimilar System

If you installed NetBackup client software on the target system and backed it up as described in “Determining Hardware Differences” on page 99, you can import the NIC information from that configuration and then map the network identifies (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 and then add the network interface information manually to the DSR configuration.

For procedures for importing and mapping interfaces or changing them manually, see “Network Interfaces” on page 190.

Mapping Disks

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 (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.

If you installed NetBackup client software on the target system and backed it up as described in “Determining Hardware Differences” on page 99, you can import the disk layouts from that configuration and then map disks before the restore. VERITAS 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.

For information about and procedures for DDR, see “Restoring to Dissimilar Disks” on page 90.

Creating Boot Media

If boot media is not available, create media for booting the target system.

See “Managing Boot Media” on page 153.

Restoring the Client

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

For instructions, see “Restoring Windows Clients” on page 79.
First Logon

After the system has been restored, an administrator logon is required to complete the DSR changes. The \texttt{bmrcleanup} utility will run and display 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. Perform the following action depending on which wizard or message screen appears.

- On the “Digital Signature Not Found” screen, click \textbf{Yes} or \textbf{Continue}.
- On the “Found New Hardware wizard” screen, click \textbf{Cancel}.
- On the “New drivers are installed, do you want to reboot?” screen, click \textbf{No}.

\textbf{Note} Do not reboot the system until the \texttt{bmrcleanup} status box has completed.

\textbf{Note} Windows XP and Windows Server 2003 systems may require a product activation after a DSR.

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 colocated with a NetBackup master server). Two options exist for restoring NetBackup media servers:

- If you back up a media server to a different media server, you can restore the protected media server as you would an ordinary protected client. For procedures, see “Restoring UNIX and Linux Clients” on page 70 or “Restoring Windows Clients” on page 79.
- If a media server backs up its own data (using either SCSI- or SAN-attached storage devices), you can use BMR to restore the media server by first configuring NetBackup to use an alternate media server.

\textbf{Tasks}  
“Configuring an Alternate Media Server” on page 104
“Restoring the Media Server” on page 105

\textbf{Related Topics}  
“Perform a Full Backup After a Restore” on page 53
Configuring an Alternate Media Server

Two methods exist to configure an alternate media server in NetBackup. You must perform one of the following:

- Configuring 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 prior to the failure, which results in less time and effort during the restore.

- Overriding 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 if you did not configure automatic media server failover prior to the failure, and you want to perform a temporary media server reassignment so you can restore the original media server.

All backup and restore requests, not just BMR restores, are directed to the alternate media servers.

For more detailed information about configuring NetBackup to use an alternate media server, see the *NetBackup System Administrator’s Guide, Volume I*.

Configuring Automatic Media Server Failover

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

On UNIX and Linux systems, configuring this option 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, naming the media server and failover restore server(s).

3. Stop and restart the NetBackup Request Manager daemon/service on the master server.
Overriding the Original Media Server Manually

If necessary, before you override the media server physically move the media to a library attached to the new media server and 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; NetBackup backup and restore requests will be performed by the original server again.

On UNIX and Linux systems, configuring this option 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, naming the original backup server and the restore server. Click OK.

3. Stop and restart the NetBackup Request Manager daemon/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, and you can perform a standard restore. For procedures, see “Restoring UNIX and Linux Clients” on page 70 or “Restoring Windows Clients” on page 79.

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

▼ To create and modify a media server restore configuration

1. Create a restore configuration. To do so, follow the procedures in “Copying a Configuration” on page 172.

2. Open the Change Configuration dialog box. For procedures, see “Modifying a Configuration” on page 177.

3. Select the Hosts properties.

4. Add the alternate media server as a host. For procedures, see “Hosts” on page 186.
5. Click OK to close the Change Configuration dialog box.

After you create and modify the restore configuration, perform a standard restore. For
procedures, see “Restoring UNIX and Linux Clients” on page 70 or “Restoring Windows
Clients” on page 79.

Restoring BMR Boot Servers

You can restore BMR boot servers if you protect them as BMR clients. You must back them
up, and you must use a shared resource tree on another boot server that contains the
resources that can 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. Recovery of the NetBackup catalogs (which include the
BMR databases) on the NetBackup master server are possible; 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.

For information about how to protect clients, see:

◆ “Protecting Clients” on page 51

Restore boot servers by using the procedures documented in the following:

◆ “Restoring Clients” on page 61

Using External Procedures

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

The following are the two 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 executed only if you select Run External Procedures on the Prepare to
Restore Client or Prepare to Discover dialog box or if you 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 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 `bmr:epadm` command on the master server to manage external procedures.

**Note** Using external procedures requires a general knowledge of scripting.

### External Procedure Points and Names

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

<table>
<thead>
<tr>
<th>External Procedure Point</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prediscover</td>
<td>Before discovery of hardware is reported to the BMR server (UNIX clients only).</td>
</tr>
<tr>
<td>preformat</td>
<td>Before formatting and partitioning of disks. On Windows systems, the preformat takes place after the system drive has been formatted but before any nonsystem drives are formatted.</td>
</tr>
<tr>
<td>prerestore</td>
<td>Before files begin to restore.</td>
</tr>
<tr>
<td>postrestore</td>
<td>After files have been restored.</td>
</tr>
<tr>
<td>firstboot</td>
<td>After the restore is complete and at the first boot of a restored client. On Windows systems, the firstboot external procedure operates as the first user to log on after a client has been restored.</td>
</tr>
</tbody>
</table>

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 external procedures intended for Microsoft Windows systems. BMR adds the appropriate filename 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:
Using External Procedures

`clientname_externalprocedure`

For example, the `sol123_prerestore` external procedure is executed before files are restored on client `sol123` (if Run External Procedures was specified during the prepare to restore).

**Operating System Specific External Procedures Names**

Operating system specific external procedure names are in the following format:

`externalprocedure.ostype`

`ostype` is one of the following:

<table>
<thead>
<tr>
<th><code>ostype</code></th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>aix</td>
<td>AIX systems</td>
</tr>
<tr>
<td>hp</td>
<td>HP-UX systems</td>
</tr>
<tr>
<td>linux</td>
<td>Linux systems</td>
</tr>
<tr>
<td>sol</td>
<td>Solaris systems</td>
</tr>
<tr>
<td>win</td>
<td>Windows systems</td>
</tr>
</tbody>
</table>

For example, the `preformat.linux` external procedure is executed on Linux clients before drives are formatted (if Run External Procedures was specified during the prepare to restore).

**Managing External Procedures**

Use the `bmrepadm` command to:

- Add an external procedure so it will be 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 the following command on the NetBackup master server that is licensed for BMR:

```
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 the *NetBackup Commands for UNIX* or the *NetBackup Commands for Windows* guide.

## Running 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.

To specify external procedures, select **Run External Procedures** in a Prepare To Discover or Prepare to Restore Client dialog box.

Alternatively, use the `bmrep` command `runep` option to specify external procedures. For more information about the `bmrep` command, see the *NetBackup Commands for UNIX* or the *NetBackup Commands for Windows* guide.

**Note** External procedures should be in the BMR database before the prepare to restore or prepare to discover operation is invoked.

## 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 file systems mounted under `/tmp`; all other file systems are read-only during a restore.

On Windows systems, by default transferred files are stored in the current directory, which is `%SystemDrive%\` during restore and the `%HOMEPATH%` directory during the firstboot 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 invoking the `bmrc` command in an external procedure, specify the full path to the `bmrc` command in the restore environment:
Using External Procedures

◆ /usr/openv/netbackup/bin on UNIX and Linux clients
◆ %SystemDrive%\BMR\NB\bin on Microsoft Windows clients. At the firstboot 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 the NetBackup Commands for UNIX or the NetBackup Commands for Windows guide.

Interaction with External Procedures

UNIX and Linux Clients
On UNIX systems, you can enter commands and interact with an external procedure during restore time by invoking 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 simple redirection to send output to the screen from with an external procedure by redirect output to the special device /dev/console (as in echo "Hello World" >> /dev/console).

Note On UNIX and Linux systems, the bmrShell is not available during firstboot.

Microsoft Windows Clients
On Windows systems, you can enter commands and interact with an external procedure during restore time by invoking the Windows command interpreter cmd from within the external procedure script.

On Windows systems, the limited restore environment may not contain DLLs or the exact 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, or add the the location of that DLL to the PATH environment variable.

External Procedure Logging

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

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

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

Procedure Logging
External procedures write messages when starting and finishing. A message includes the date and time the procedure began, the client name, and a description that includes the external procedure name, as in the following examples:


**User Logging**

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 invoking the `bmrc` command in an external procedure, specify the full path to the `bmrc` command in the restore environment:

- `/usr/openv/netbackup/bin` on UNIX and Linux clients
- `%SystemDrive%\BMR\NB\bin` on Microsoft Windows clients. At the firstboot 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 the NetBackup Commands for UNIX or the NetBackup Commands for Windows guide.

**External Procedure Operational States**

During execution of an external procedure, the following operational states are displayed in the NetBackup Administration Console Bare Metal Restore Tasks view:

<table>
<thead>
<tr>
<th>Operational State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery External Procedure</td>
<td>An external procedure is running during the prediscovery phase.</td>
</tr>
</tbody>
</table>
Using External Procedures

<table>
<thead>
<tr>
<th>Operational State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Boot External Procedure</td>
<td>An external procedure is running during the firstboot phase.</td>
</tr>
<tr>
<td>Post-restore External Procedure</td>
<td>An external procedure is running during the postrestore phase.</td>
</tr>
<tr>
<td>Pre-format External Procedure</td>
<td>An external procedure is running during the preformat phase.</td>
</tr>
<tr>
<td>Pre-restore External Procedure</td>
<td>An external procedure is running during the prerestore phase.</td>
</tr>
</tbody>
</table>

**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, if it is not vital to system functionality), ensure that you exit 0 from the external procedure.

**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.

**Note** When a UNIX firstboot external procedure is executed with no terminal defined and the procedure returns non-zero, the Bare Metal Restore process will end.

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

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

If you retry (UNIX and Linux) or try again (Windows), you are asked if you want to transfer the external procedure again from the BMR server before running it. This provides an opportunity to edit the external procedure on the master server before running it again.
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>
<thead>
<tr>
<th>Environment Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$BMRC</td>
<td>Pathname to the bmrc executable file (/usr/openv/netbackup/bin/bmrc)</td>
</tr>
<tr>
<td>$bootServerAddress</td>
<td>Boot Server IP address</td>
</tr>
<tr>
<td>$clAddress</td>
<td>The IP address of the client</td>
</tr>
<tr>
<td>$clAddressHex</td>
<td>Client IP address converted to hex</td>
</tr>
<tr>
<td>$client_firstboot</td>
<td>Name of client specific firstboot external procedure</td>
</tr>
<tr>
<td>$client_postrestore</td>
<td>Name of client specific postrestore external procedure</td>
</tr>
<tr>
<td>$client_prediscover</td>
<td>Name of client specific discover external procedure</td>
</tr>
<tr>
<td>$client_preformat</td>
<td>Name of client specific preformat external procedure</td>
</tr>
<tr>
<td>$client_prerestore</td>
<td>Name of client specific prerestore external procedure</td>
</tr>
<tr>
<td>$clName</td>
<td>The name of the client</td>
</tr>
<tr>
<td>$clOs</td>
<td>BMR abbreviated OS specification</td>
</tr>
<tr>
<td>$configName</td>
<td>The name of the configuration</td>
</tr>
<tr>
<td>$default_firstboot</td>
<td>Name of OS default firstboot external procedure</td>
</tr>
<tr>
<td>$default_postrestore</td>
<td>Name of OS default postrestore external procedure</td>
</tr>
<tr>
<td>$default_prediscover</td>
<td>Name of OS default discover external procedure</td>
</tr>
<tr>
<td>$default_preformat</td>
<td>Name of OS default preformat external procedure</td>
</tr>
</tbody>
</table>
Using External Procedures

<table>
<thead>
<tr>
<th>Environment Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$default_prerestore</td>
<td>Name of OS default prerestore external procedure</td>
</tr>
<tr>
<td>$defaultGateway</td>
<td>The name of the default gateway</td>
</tr>
<tr>
<td>$extProcName</td>
<td>Current External Procedure Name</td>
</tr>
<tr>
<td>$importNonRootVgs</td>
<td>Import nonsystem volume/disk groups</td>
</tr>
<tr>
<td>$logging</td>
<td>Log restore; yes=yes, no=no</td>
</tr>
<tr>
<td>$newConfig</td>
<td>Name of the configuration to discover</td>
</tr>
<tr>
<td>$onEpError</td>
<td>Restore behavior on External Procedure Error:</td>
</tr>
<tr>
<td></td>
<td>0=cancel</td>
</tr>
<tr>
<td></td>
<td>1=prompt</td>
</tr>
<tr>
<td></td>
<td>2=ignore</td>
</tr>
<tr>
<td>$runEp</td>
<td>Execute external procedures if found 0=no, 1=yes</td>
</tr>
<tr>
<td>$runMode</td>
<td>Mode of BMR process discover or restore</td>
</tr>
<tr>
<td>$serverAddress</td>
<td>NetBackup server IP address</td>
</tr>
<tr>
<td>$serverGateway</td>
<td>Gateway to the NetBackup server</td>
</tr>
<tr>
<td>$serverName</td>
<td>NetBackup server name</td>
</tr>
</tbody>
</table>

**AIX Environment Variables**

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
Using External Procedures

HP-UX Environment Variables
The following exported operating system environment variables are set at restore:

$DEFAULT_RELEASE_DIR  $EDITOR  $ENV
$ERRNO  $PCEDIT  $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_LIP_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 invoke the Windows command-line interpreter during restore.
Storage Area Network Support

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

- %ALLUSERSPROFILE%
- %APPDATA%
- %CommonProgramFiles%
- %COMPUTERNAME%
- %ComSpec%
- %HOMEDRIVE%
- %HOME%
- %LOGONSERVER%
- %NUMBER_OF_PROCESSORS%
- %OS%
- %Os2LibPath%
- %Path%
- %PATHEXT%
- %PROCESSOR_ARCHITECTURE%
- %PROCESSOR_IDENTIFIER%
- %PROCESSOR_LEVEL%
- %PROCESSOR_REVISION%
- %ProgramFiles%
- %PROMPT%
- %SystemDrive%
- %SystemRoot%
- %TEMP%
- %TMP%
- %USERPROFILE%
- %USERNAME%
- %windir%

Storage Area Network Support

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

**Note** BMR does not support SAN restores on Linux systems.

You can restore the system disks only of the system attached to the SAN or the entire system:

- For a system only restore, select **Restore system disks/volumes only** on the Prepare to Restore Client dialog box.
- To restore the entire system, do *not* select **Restore system disks/volumes only** on the Prepare to Restore Client dialog box.
Caution Use caution when choosing to restore the entire system. If the HBA drivers and their configuration are not available in the SRT, BMR will not be able to restore the entire system. In these cases, BMR will go into dissimilar disk restore mode and prompt you to save the configuration so you can map disks.

SANs and Dissimilar Disk Restores

UNIX clients only.

Before beginning the restore, disconnect from the SAN.

Do not restore the SAN disks.

After a Solaris system is recovered using the dissimilar disk restore feature, you may need to perform the following steps for SAN-attached volumes.

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 and add them to the /etc/vfstab file or uncomment the corresponding lines 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.

SANs and Dissimilar System Restores

If you are performing 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.

To add drivers, see “Adding NIC and MSD Drivers” on page 101.
SAN Persistent Bindings Required

In SAN environments, BMR may require the use of persistent bindings. You may need to modify the HBA driver configuration files to bind specific devices on the SAN to specific targets on the hosts.

Multiple Network Interface Support

BMR recovery occurs in two major stages: boot stage and restore files stage. Each stage uses an interface defined as follows:

**Boot Interface**

The network interface and address to boot from (that is, how to connect to the BMR boot server when network booting and installing the restore environment).

Windows clients do not network boot, but a boot interface is required if the restore environment is installed from an SRT on a BMR boot server. If a client boots and installs the restore environment from CD media, a network boot interface is not required.

**Restore Interface**

The network interface and address to restore from (that is, how to connect to the NetBackup master and media servers to initiate file restore).

BMR can restore systems that have multiple network interfaces (also known as multihomed environments).

Multihomed UNIX and Linux Clients

*Network boot only.*

UNIX and Linux clients must use a single interface to boot from and to restore through. Therefore, the interface used for the restore stage must be the same interface used for the boot stage.

A client can network boot and restore over any interface that supports network boot if the BMR boot server and NetBackup media servers are on a network that can be reached by that interface. *Exception:* Because of Ignite restrictions, an HP-UX client must network boot and restore over its internal interface.
**Multihomed Windows Clients**

BMR activates one interface on a Windows client during the boot stage of a restore, and you specify that boot interface when you create the boot media.

BMR configures and activates all network interfaces during the restore stage, but only one is used for the restore.

The following diagram illustrates a configuration that can occur with multihomed Windows clients. For this configuration, you should specify the network interface for Network 1 when you create the boot media for the client.

Simple Multihomed Example

![Diagram of multihomed network interfaces]

**Client Configuration Using Gateways**

BMR clients can use gateways to communicate with BMR and NetBackup servers during a restore operation. The following table describes three gateway attributes used during a restore. 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 gateways for the NetBackup master and media servers in the
Multiple Network Interface Support

restore configuration's Hosts dialog box and 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.

Network Gateways

<table>
<thead>
<tr>
<th>Gateway</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Gateway</td>
<td>Defines the default network gateway for the client during the restore.</td>
</tr>
<tr>
<td>Master Server Gateway</td>
<td>Defines the gateway from the client to the NetBackup master server.</td>
</tr>
<tr>
<td>Media Server Gateway</td>
<td>Defines the gateway from the client to the NetBackup media server used to restore the files.</td>
</tr>
</tbody>
</table>

The following diagram shows how gateways can be used during a BMR client restore. The client in this diagram cannot communicate with all of the servers it needs to by using only the default gateway. For this configuration, you should specify the default gateway as G1, the master server gateway as G2, and the media server gateway as G3.

Gateway Example

![Gateway Diagram]

120 NetBackup Bare Metal Restore System Administrator's Guide
Port Usage During Restores

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

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>UNIX</th>
<th>Linux</th>
<th>Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootp</td>
<td>67, 68</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>ping</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lockd</td>
<td>Unreserved</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>mountd</td>
<td>Unreserved</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>nfssd</td>
<td>2049</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>portmapper</td>
<td>111</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>rpcbind</td>
<td></td>
<td>X(^1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>statd</td>
<td>Unreserved</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>tftp</td>
<td>69</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>vnetd</td>
<td>13724</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Windows File Sharing</td>
<td>445</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

1. For bootparam on Solaris only.
Port Usage During Restores
Managing Shared Resource Trees

The following provide information about creating and managing shared resource trees.

**Tasks**
- “Creating a Shared Resource Tree” on page 126
- “Adding Software to a Shared Resource Tree” on page 137
- “Using a Shared Resource Tree Exclusively” on page 143
- “Copying a Shared Resource Tree” on page 145
- “Repairing a Damaged Shared Resource Tree” on page 147
- “Breaking a Stale Shared Resource Tree Lock” on page 148
- “Deleting a Shared Resource Tree” on page 150

**Related Topics**
- “Shared Resource Tree Overview” on page 123
- “Shared Resource Trees View” on page 124

**Shared Resource Tree Overview**

A shared resource tree (SRT) is a collection of operating system files, NetBackup client software, and other programs needed to format drives, create partitions, rebuild file systems, and restore the original files using the NetBackup client software. An SRT also provides the resources needed to boot the client system and begin the restore process.

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

Each client type and operating system version requires its own SRT. For example:

- Solaris 9 requires a Solaris 9 SRT, Windows Server 2003 requires a Windows Server 2003 SRT, and so on.

- Windows SRTs require the appropriate service packs. If you have some Windows XP protected clients at Service Pack 1 and others at Service Pack 2, you need two SRTs.
Shared Resource Trees View

You create SRTs on boot servers of the same operating system, and the boot server must run the same or later version of the operating system installed in the SRT. For example, a Solaris 9 SRT must reside on a Solaris 9 or later boot server, a Windows Server 2003 SRT must reside on a Windows Server 2003 boot server, and so on. For information about the supported operating systems for clients, SRTs, and boot servers, see the NetBackup Release Notes.

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

Depending on the operating system for which an SRT is created, the SRT requires 100 MB to 600 MB of disk space. For disk space requirements, see the NetBackup Release Notes.

Related Topics

♦ “Managing Boot Media” on page 153

Shared Resource Trees View

The Shared Resource Trees view shows all the SRTs that are defined for the protection domain. 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.
Shared Resource Trees View

Actions for Shared Resource Trees View

To | Do the Following
---|---
View SRT properties | Right click on an SRT in the Bare Metal Restore Shared Resource Trees pane and then select Properties from the shortcut menu.
Use this option to determine the software installed in an SRT.
Creating a Shared Resource Tree

Creating a Shared Resource Tree

Shared Resource Tree View Columns

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the shared resource tree.</td>
</tr>
<tr>
<td>Operating System</td>
<td>The operating system of the shared resource tree.</td>
</tr>
<tr>
<td>State</td>
<td>The state of a shared resource tree can be:</td>
</tr>
<tr>
<td></td>
<td>• READY. Ready for use. It may be copied, deleted, modified, or</td>
</tr>
<tr>
<td></td>
<td>allocated to a restore task.</td>
</tr>
<tr>
<td></td>
<td>• LOCKED_READ. Locked against modification because it is being</td>
</tr>
<tr>
<td></td>
<td>copied. This SRT may be allocated to a restore task.</td>
</tr>
<tr>
<td></td>
<td>It cannot be copied, deleted, or modified until the lock is</td>
</tr>
<tr>
<td></td>
<td>released.</td>
</tr>
<tr>
<td></td>
<td>• LOCKED_WRITE. Locked against all use because it is being</td>
</tr>
<tr>
<td></td>
<td>created or modified. No operations can be performed on this</td>
</tr>
<tr>
<td></td>
<td>SRT until the lock is released.</td>
</tr>
<tr>
<td></td>
<td>• BAD. Unusable and cannot be repaired. This can happen, for</td>
</tr>
<tr>
<td></td>
<td>example, if a boot server crashes in the middle of an SRT</td>
</tr>
<tr>
<td></td>
<td>delete operation. The only operation allowed on the SRT is</td>
</tr>
<tr>
<td></td>
<td>delete.</td>
</tr>
<tr>
<td></td>
<td>• DAMAGED. Unusable but it may be possible to repair it.</td>
</tr>
<tr>
<td></td>
<td>This can occur when an SRT operation was interrupted before</td>
</tr>
<tr>
<td></td>
<td>it could finish, such as when canceling the bmrsrtadm</td>
</tr>
<tr>
<td></td>
<td>command using Ctrl+c and choosing to leave the SRT on the</td>
</tr>
<tr>
<td></td>
<td>server. You can try to repair a damaged SRT (UNIX or Linux),</td>
</tr>
<tr>
<td></td>
<td>or you can delete it.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of shared resource tree: network or CD.</td>
</tr>
<tr>
<td>Path</td>
<td>The absolute path where the shared resource tree resides on</td>
</tr>
<tr>
<td></td>
<td>the boot server.</td>
</tr>
<tr>
<td>Boot Server</td>
<td>The BMR boot server on which the shared resource tree is</td>
</tr>
<tr>
<td></td>
<td>resides.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the SRT.</td>
</tr>
</tbody>
</table>

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 media or images for the following:

- Operating system.
- NetBackup client software.
- For Linux SRTs, the Bare Metal Restore Third-Party Products CD. This CD contains open source products that may not be included in the vendor Linux distribution.
- Optionally, other applications or packages (such as VERITAS Volume Manager or VERITAS File System).
- Optionally, patches, maintenance levels, maintenance packs, service packs, filesets, or drivers required by the operating system or other software installed in the SRT. You must install any operating system patches required by the NetBackup client software into the SRT; if they are not installed, NetBackup will not function correctly in the temporary restore environment and the restore may fail. For package or patch dependencies, see the “NetBackup Product Dependencies” section of the NetBackup Release Notes.

If you need more than one SRT of the same operating system (for example, to restore clients that have different versions of VERITAS Volume Manager or different drivers), you should consider creating an SRT with only the operating system and NetBackup client software and then make as many copies as you need, adding the different versions of the other software to the copies. Copying an existing SRT usually is faster than creating an SRT.

During SRT creation, you are prompted for the path to the installation media or software:

- If you place the installation media in a removable media drive of the boot server, provide the path to that removable media drive.
- If you copy the contents of the installation media to a local directory, you can provide the path to that local directory.
- If you copy the contents of the installation media to a remote directory available to the boot server via NFS or network share, you can provide the path to that remote directory or share location.

Creating an SRT takes 5 to 60 minutes, depending on factors such as the speed of the system, the operating system of the SRT being created, and other software being installed.

**Tasks**

“Creating an SRT for UNIX or Linux” on page 128

“Creating an SRT for Windows” on page 136
Creating a Shared Resource Tree

Creating an SRT for UNIX or Linux

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

To copy an SRT to a bootable CD (that is, to create boot media), see “Creating Boot Media for UNIX and Linux” on page 155.

▼ To start the `bmrstadm` command

1. On the boot server on which you want to create the SRT, change to the following directory:
   
   `/usr/openv/netbackup/bin`

2. Enter the following command:
   
   `./bmrstadm`

   The following appears:

   Select one of the following options:

   1. Create a new Shared Resource Tree.
   2. Create a new CD image based Shared Resource Tree.
   3. Copy an existing Shared Resource Tree to a new location.
   4. Modify an existing Shared Resource Tree.
   5. Delete an existing Shared Resource Tree.
   7. Quit.

   Enter your selection (1-7) [1] :

3. Select the option to create a new SRT.

4. To continue with creating the specific SRT type, see the following:
   
   ◆ “Creating an AIX SRT” on page 128
   ◆ “Creating an HP-UX SRT” on page 130
   ◆ “Creating a Solaris SRT” on page 132
   ◆ “Creating a Linux SRT” on page 134

Creating an AIX SRT

When you create an AIX SRT, you are guided through the process of installing:

◆ The operating system software
- NetBackup client software.

The following are the prompts that appear when you create an AIX SRT.

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Action/Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the name of the SRT to create</td>
<td>The name of the SRT also is used for the directory that contains it. Only alphanumeric characters and the underscore (_) character are allowed.</td>
</tr>
<tr>
<td>Enter the description of the new SRT</td>
<td>A description of the SRT.</td>
</tr>
<tr>
<td>Enter desired OS level of AIX</td>
<td>The prompt includes the levels you can create based on the operating system version of the boot server.</td>
</tr>
<tr>
<td>Enter the directory in which to place the new SRT</td>
<td>The path to the directory in which to create the SRT. The pathname to the SRT location, including the SRT name, is the root of the SRT (called the SRT path). The default is either <code>/export/srt</code> or the directory where an SRT was last created successfully. The directory must exist.</td>
</tr>
<tr>
<td>Source of AIX install images</td>
<td>Enter the name of the device in which the operating system installation media 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.</td>
</tr>
<tr>
<td>Enter the source of the VERITAS NetBackup install images. Specify a device name or an NFS path (host:/path form), or a local directory</td>
<td>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.</td>
</tr>
</tbody>
</table>

**The following appears when the NetBackup client software installation process begins:**

VERITAS Installation Script
Copyright 1993 - 2005 VERITAS Software Corporation, All Rights Reserved.
Installing NetBackup Client Software
NOTE: To install NetBackup Server software, insert the appropriate NetBackup Server cdrom.

Do you wish to continue? [y,n] (y) y Enter \( y \).
Creating a Shared Resource Tree

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Action/Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you want to install the NetBackup client software for this client?</td>
<td>Enter y.</td>
</tr>
<tr>
<td>y,n] (y)</td>
<td></td>
</tr>
<tr>
<td>Enter the name of the NetBackup server:</td>
<td>Enter any nonblank value; the server name is replaced at restore time with the correct values for the BMR client being restored.</td>
</tr>
<tr>
<td>Would you like to use “servername” as the configured name of the NetBackup client? [y,n] (y)</td>
<td>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.</td>
</tr>
</tbody>
</table>

After installing the AIX and NetBackup software, the `bmrstart` 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). For information about adding other software, see “Adding Software to a Shared Resource Tree” on page 137.

Creating an HP-UX SRT

When you create an HP-UX SRT, you are guided through the process of installing:

- Ignite software

  **Note** If the SRT is to be used to restore PA-RISC2-based clients, you must use Ignite-UX 5.3x or later to create the SRT.

- The operating system software

- NetBackup client software

The following are the prompts that appear when you create an HP-UX SRT.

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Action/Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the name of the SRT to create</td>
<td>The name of the SRT also is used for the directory that contains it. Only alphanumeric characters and the underscore (_) character are allowed.</td>
</tr>
<tr>
<td>Enter the description of the new SRT</td>
<td>A description of the SRT.</td>
</tr>
<tr>
<td>SRT OS level</td>
<td>The prompt includes the levels you can create based on the operating system version of the boot server.</td>
</tr>
<tr>
<td>Prompt</td>
<td>Action/Explanation</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Enter the directory in which to place the new SRT</td>
<td>The path to the directory in which to create the SRT. The pathname to the SRT location, including the SRT name, is the root of the SRT (called the SRT path). The default is either <code>/export/srt</code> or the directory where an SRT was last created successfully. The directory must exist.</td>
</tr>
</tbody>
</table>
| Location (device or directory path) of the Ignite install media. | BMR will search 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 will look for a file named INSTCMDS from the tar file supplied in one the following directories (note that `-PA indicates Ignite version B41). If the file is not found, BMR will be unable to install Ignite.  
Ignite-UX/BOOT-KERNEL/`opt/ignite/data`  
Ignite-UX/BOOT-KERNEL-PA/`opt/ignite/data` |
| 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` | If your version of Ignite requires a patch, you are prompted to provide the path to the specific patch version required.  
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`: |
Creating a Shared Resource Tree

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Action/Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location (device or path) of the VERITAS NetBackup install media</td>
<td>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.</td>
</tr>
</tbody>
</table>

The following appears when the NetBackup client software installation process begins:

VERITAS Installation Script
Copyright 1993 - 2005 VERITAS Software Corporation, All Rights Reserved.
Installing NetBackup Client Software
NOTE: To install NetBackup Server software, insert the appropriate NetBackup Server cdrom.

Do you wish 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 installing the HP-UX and NetBackup software, the bmrsrtadm command provides options to install other software in the SRT. You can either add other sofware now or quit (you can always add software later). For information about adding other software, see "Adding Software to a Shared Resource Tree" on page 137.

Creating a Solaris SRT

When you create a Solaris SRT, you are guided through the process of installing:

◆ The operating system software.
◆ NetBackup client software.

BMR can create a new SRT from the Solaris installation media, the installation media copied to a local or remote directory, or the Solaris software installed in an existing SRT. Furthermore:

◆ For CD media, use the Software 1 of 2 CD
If you are creating a Solaris 9 SRT using a network shared CD, both slice 0 and slice 1 must be shared.

**Related Topics**
- "Patches, Packages, and Solaris SRTs" on page 142

The following are the prompts that appear when you create a Solaris SRT.

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

**The following appears when the NetBackup client software installation process begins:**

VERITAS Installation Script  
Copyright 1993 - 2005 VERITAS Software Corporation, All Rights Reserved.  
Installing NetBackup Client Software  
NOTE: To install NetBackup Server software, insert the appropriate NetBackup Server cdrom.
Creating a Shared Resource Tree

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Action/Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you wish to continue? [y,n] (y)</td>
<td>Enter y.</td>
</tr>
<tr>
<td>Do you want to install the NetBackup client software for this client?</td>
<td>Enter y.</td>
</tr>
<tr>
<td>[y,n] (y)</td>
<td></td>
</tr>
<tr>
<td>Enter the name of the NetBackup server:</td>
<td>Enter any nonblank value; the server name is replaced at restore time with the correct values for the BMR client being restored.</td>
</tr>
<tr>
<td>Would you like to use “servername” as the configured name of the NetBackup client? [y,n] (y)</td>
<td>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.</td>
</tr>
</tbody>
</table>

After installing the Solaris and NetBackup software, the bmrstartadm 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). For information about adding other software, see “Adding Software to a Shared Resource Tree” on page 137.

Creating a Linux SRT

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

- The operating system software.

- VERITAS BMR Third-Party Products, which are open source products that may not be included in the vendor Linux distribution. You may download a CD image, at no charge, from http://seer.support.veritas.com/docs/275782.htm.

- NetBackup client software.

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

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

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

The bmrstartadm command on Linux also allows you to specify the path to a file system image file (in addition to specifying 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, which can be downloaded and used as the source image or written to CD media.
The following are the prompts that appear when you create a Linux SRT.

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Action/Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the name of the SRT to create</td>
<td>The name of the SRT also is used for the directory that contains it. Only alphanumeric characters and the underscore (_) character are allowed.</td>
</tr>
<tr>
<td>Enter the description of the new SRT</td>
<td>A description of the SRT.</td>
</tr>
<tr>
<td>Enter the directory in which to place the new SRT</td>
<td>The path to the directory in which to create the SRT. The pathname to the SRT location, including the SRT name, is the root of the SRT (called the SRT path). The default is either /export/srt or the directory where an SRT was last created successfully. The directory must exist.</td>
</tr>
<tr>
<td>The following media is required: Linux distribution - disc x of x Please load the media now. Load media from:</td>
<td>The prompt includes the Linux distribution (Red Hat or SuSE) and the disk required. The bmrSRTadm command prompts you for several of the Linux installation discs. Some systems try to mount media loaded in the CD drive automatically (such as the Red Hat magicdev process). When prompted for media on those systems, load the media into the drive, close the drive tray, and wait for the drive light to stop flashing before pressing Enter.</td>
</tr>
<tr>
<td>The following media is required: VERITAS BMR Third-Party Products CD (3PPCD) Please load the media now. Load media from:</td>
<td>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 components used by BMR on Linux systems.</td>
</tr>
<tr>
<td>The following media is required: NetBackup x.x Client Please load the media now. Load media from:</td>
<td>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.</td>
</tr>
</tbody>
</table>
Creating a Shared Resource Tree

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Action/Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The following appears when the NetBackup client software installation process begins:</strong></td>
<td></td>
</tr>
<tr>
<td>VERITAS Installation Script</td>
<td></td>
</tr>
<tr>
<td>Copyright 1993 - 2005 VERITAS Software Corporation, All Rights Reserved.</td>
<td></td>
</tr>
<tr>
<td>Installing NetBackup Client Software</td>
<td></td>
</tr>
<tr>
<td>NOTE: To install NetBackup Server software, insert the appropriate NetBackup Server cdrom.</td>
<td></td>
</tr>
<tr>
<td>Do you wish to continue? [y,n] (y)</td>
<td>Enter y.</td>
</tr>
<tr>
<td>Do you want to install the NetBackup client software for this client? [y,n] (y)</td>
<td>Enter y.</td>
</tr>
<tr>
<td>OS Level Options</td>
<td>Always choose Red Hat 2.4 -- even when creating a SuSE Linux SRT.</td>
</tr>
<tr>
<td>1. IBMzSeriesLinux2.4.21</td>
<td></td>
</tr>
<tr>
<td>2. RedHat2.4</td>
<td></td>
</tr>
<tr>
<td>q. To quit from this script</td>
<td></td>
</tr>
<tr>
<td>Enter the name of the NetBackup server:</td>
<td>Enter any nonblank value; the server name is replaced at restore time with the correct values for the BMR client being restored.</td>
</tr>
<tr>
<td>Would you like to use &quot;servername&quot; as the configured name of the NetBackup client? [y,n] (y)</td>
<td>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.</td>
</tr>
<tr>
<td>After installing the Linux and NetBackup software, the bmrsrcadm 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). For information about adding other software, see “Adding Software to a Shared Resource Tree” on page 137.</td>
<td></td>
</tr>
</tbody>
</table>

**Creating an SRT for Windows**

Use the following Windows installation CD resources to create a Windows SRT:

- To create a Windows 2000 SRT, use a Windows 2000 Professional, Server, or Advanced Server CD.

An SRT created with a Windows 2000 Server or Advanced Server CD can restore all Windows 2000 clients; however, if use a Windows 2000 Professional SRT to restore a Windows 2000 Server or Advanced Server client, volume layout limitations exist.

Windows 2000 OEM installation CDs are not recommended for creating an SRT, although they will work in many cases.

**To create a Windows SRT**

1. From the **Start** menu on the Windows BMR boot server that will host the SRT, select **Programs > VERITAS 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.

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:
   - **Name**. The name of the SRT also is used for the directory that contains it. Only alphanumeric characters and the underscore (_) character are allowed.
   - **Description**.
   - **Path to the Windows installation image**.
   - **License key for Windows**.
   - **Location for the SRT**.
   - **Path to the NetBackup client software image**.

   For more information, see the Shared Resource Tree Administration wizard help.

### Adding Software to a Shared Resource Tree

Install additional software into an existing SRT only if it is required during the restore, such as an operating system patch or fileset required by NetBackup client software. The software in an SRT is not installed on the restored system, it is used only to bring the protected system to a state from which the original files can be restored. Therefore, you do not need to install all of the patches, maintenance levels, maintenance packs, service packs, filesets, 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.
Adding Software to a Shared Resource Tree

**Tasks**

“Adding Software to a UNIX or Linux SRT” on page 138

“Adding Software to a Windows SRT” on page 142

**Adding Software to a UNIX or Linux SRT**

The `bmrsrtadm` command provides options to install the following additional software in an existing UNIX or Linux SRT (not all options are supported on all systems):

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

**Note** Use only the specific VERITAS options to add VERITAS products to an SRT.

If you did not add the required NetBackup software when you created the SRT, you will be prompted to add it when you choose 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. If you are adding software during SRT creation, continue with step 5 on page 139.

▼ **To add software to a UNIX or Linux SRT**

1. On the BMR boot server on which the SRT resides, change to the following directory:
   ```
   /usr/openv/netbackup/bin
   ```

2. Enter the following command:
   ````
   ./bmrsrtadm
   ```
   The following appears:
   ```
   Select one of the following options:
   1. Create a new Shared Resource Tree.
   2. Create a new CD image based Shared Resource Tree.
   3. Copy an existing Shared Resource Tree to a new location.
   4. Modify an existing Shared Resource Tree.
   5. Delete an existing Shared Resource Tree.
   ```
7. Quit.

Enter your selection (1-7) [1]:

3. Select the option to modify an existing shared resource tree.

4. Enter the name of the SRT to modify.

A menu similar to the following following appears (the wording for option 4 depends on the operating system installed in the SRT):

```
SRT name: srtnname
Location: /export/srt/srtnname
Description: SRT description
Exclusive use: (none)
```

You may make modifications to this SRT. What do you want to do?

1. Install VERITAS NetBackup Maintenance Pack.
2. Install VERITAS Volume Manager and VERITAS File System.
4. Install additional drivers.
5. Change SRT description.
6. Change client exclusive use of this SRT.
7. Quit.

Enter your selection (1-7) [1]:

5. Select an installation option.

The `bmrstatsadm` command guides you through installing the software. Usually, you have to enter the path to the installation media or image for the software. To continue, see the following information about the software you are installing:

- “Adding NetBackup Maintenance Packs” on page 139
- “Adding VERITAS Volume Manager and File System” on page 140
- “Adding VERITAS Security Services” on page 141
- “Adding Other Software” on page 141

**Adding NetBackup Maintenance Packs**

If a NetBackup maintenance or feature pack is installed on the clients protected by the SRT, install that maintenance or feature pack in the SRT.
Adding Software to a Shared Resource Tree

When you install a maintenance or feature pack, you are prompted for the location of the installation media or image:

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

**Adding VERITAS Volume Manager and File System**

*Not supported on Linux systems.*

If VERITAS Volume Manager (VxVM) and VERITAS File System (VxFS) are installed on the systems protected by the SRT, you must install them in the SRT so that 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 will be unable to access the file systems and volumes.

If protected clients have different versions of VxVM and/or VxFS, you need to create a separate SRT for each of those versions. However, SRTs that include VxFS and VxVM can be used to restore clients that do not have VxFS or VxVM installed. If you need more than one SRT of the same operating system (for example, to restore clients that have different versions of VERITAS Volume Manager or different drivers), you should consider creating an SRT with only the operating system and NetBackup client software and then make as many copies as you need, adding the different versions of the other software to the copies. Copying an existing SRT usually is faster than creating an SRT.

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

**Caution** On Solaris systems, verify that any patches support the `patchadd -c` flag; if they do not, do not install them into the SRT. Most patches for VxFS and VxVM do not support the `patchadd -c` flag. Testing has shown that clients that use patched versions of VxFS and VxVM can perform a restore successfully even when using an SRT that contains unpatched versions.

The “Install VERITAS Volume Manager and VERITAS File System” option in the `bmrsrcadm` 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 prompted for the path to each component, enter a path to the extracted packages or to the root directory of the installation media (the directory that contains the `file_system` and `volume_manager` directories).
For operating system dependencies for VxVM and VxFS, see the NetBackup Release Notes.

**Adding VERITAS Security Services**

If you use NetBackup Access Management to administer access to your NetBackup environment, install the VERITAS Security Services (VxSS) software. When you select Install VERITAS Security Services from the menu, you are prompted to install:

**VERITAS Authentication subsystem (VRTSat)**

Install the client Authentication subsystem (VRTSat) software into SRTs that will restore clients in environments that use NetBackup Access Management. The Authentication subsystem verifies who users are.

**VERITAS Authorization subsystem (VRTSaz)**

Install the client Authorization subsystem (VRTSaz) into Solaris SRTs that contain NetBackup media server software. Add this subsystem if the SRT is used to restore a media server that is backed up to its own devices and restores itself from its own devices. The Authorization subsystem verifies that users have permission to perform actions.

For each option, you must provide the path to the installation image, package, fileset, or RPM (depending on OS).


**Adding Other Software**

**Note** Use only the specific VERITAS options to add VERITAS products to an SRT.

The menu option that appears for other software depends on the operating system of the SRT:

- **AIX** Maintenance levels (MLs) or additional filesets
- **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 location of the installation media, image, package, patch, fileset, RPM, and so on (depending on operating system).
Adding Software to a Shared Resource Tree

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

BMR boot servers can be damaged by patches that do not support the `patchadd -C` flag the same as JumpStart servers can be damaged by patches that do not support the `patchadd -C` flag if they are installed into the miniroot. Therefore, do not install patches that do not support the `patchadd -C` flag into an SRT.

Installing Device Drivers into Linux SRTs
To add or update device drivers in a Linux SRT, 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]:

Some hardware vendors provide drivers in a floppy image file; use the first option to install these drivers, which installs both the kernel driver module and any related hardware identification information contained in the image.

To update an existing kernel driver module, choose the second option. Do not use this option to add new driver modules; it loads the driver module only and not the hardware identification information 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
- NetBackup client software
- VERITAS Storage Foundation for Windows
- NetBackup Security Services
▼ To add software to a Windows SRT

1. From the Start menu on the Windows BMR boot server that hosts the SRT, select Programs > VERITAS 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.

3. Click Next on the Welcome screen.

4. Select the option to update an SRT.

5. Select the resource 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 VERITAS Security Services to an SRT.

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

   For more information, see the Shared Resource Tree Administration wizard help.

Using a Shared Resource Tree Exclusively

UNIX and Linux clients only.

If you save custom files with the client configuration, you can copy those custom files into the SRT so they 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:
   - Run a prepare to restore operation
   - Run a prepare to discover operation
   - Create a bootable CD (if you are creating a bootable CD that contains an SRT that has custom files)
Using a Shared Resource Tree Exclusively

**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 will fail.

Related Topics

- “Save Custom Files” on page 54

▼ **To enable or disable SRT exclusive use**

1. On the boot server on which the SRT resides, change to the following directory:
   
   `/opt/openv/netbackup/bin`

2. Enter the following command:
   
   `./bmrsrcadm`

   The following appears:

   Select one of the following options:

   1. Create a new Shared Resource Tree.
   2. Create a new CD image based Shared Resource Tree.
   3. Copy an existing Shared Resource Tree to a new location.
   4. Modify an existing Shared Resource Tree.
   5. Delete an existing Shared Resource Tree.
   7. Quit.

   Enter your selection (1-7) [1] :

3. Select the option to modify an existing shared resource tree.

4. Enter the name of the SRT to modify.

   A menu similar to the following following appears:

   ```
   SRT name: srtnamex
   Location: /export/srt/srtnamex
   Description: SRT description
   Exclusive use: (none)
   ```

   You may make modifications to this SRT. What do you want to do?

   1. Install VERITAS NetBackup Maintenance Pack.
   2. Install VERITAS Volume Manager and VERITAS File System.
4. Install additional drivers.
5. Change SRT description.
6. Change client exclusive use of this SRT.
7. Quit.
Enter your selection (1-7) [1] :

5. Select the option to change exclusive use of the SRT.
The following appears:

This action reserves the SRT for the exclusive use by a specified client. You may specify a client name here to reserve this SRT for that client. If you leave this blank then the exclusive use function will be disabled.

Enter client name (or blank to disable) :

6. Enter a client name to enable exclusive use or press Enter without entering anything to disable exclusive use.

Copying a Shared Resource Tree

You can create a new SRT by copying another SRT.

The new SRT will be created on the boot server on which 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 copying to a different boot server.

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 on which you want to create the SRT:

   `/usr/openv/netbackup/bin`
Copying a Shared Resource Tree

2. Enter the following command:

   ./bmrsrtadm

   The following appears:

   Select one of the following options:

   1. Create a new Shared Resource Tree.
   2. Create a new CD image based Shared Resource Tree.
   3. Copy an existing Shared Resource Tree to a new location.
   4. Modify an existing Shared Resource Tree.
   5. Delete an existing Shared Resource Tree.
   7. Quit.

   Enter your selection (1-7) [1]:

3. Select the option to copy an existing shared resource tree.

4. Follow the prompts to enter the required information:
   - 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 being copied to a Linux boot server on which 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.

▼ To copy an SRT on Windows

1. From the Start menu on the boot server on which you want to create the SRT, select
   Programs > VERITAS NetBackup > Bare Metal Restore Boot Server Assistant.
   The Bare Metal Restore Boot Server Assistant appears.

2. Click Shared Resource Tree Administration Wizard.
3. Select the option to copy an SRT, 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**

*UNIX and Linux boot servers only.*

If BMR places an SRT into a DAMAGED state, it may be possible to repair it so it returns to a READY state. You may choose to do this if an SRT was marked DAMAGED because a previous `bmrsrtadm` command was interrupted. In this case, successful recovery is likely. If you are unsure why an SRT was marked DAMAGED, the safest course of action is to delete it and create a new one from scratch.

SRT states are displayed in the Shared Resource Trees view of the NetBackup Administration Console. Alternatively, on UNIX and Linux systems, you can view the SRT states by using the list shared resource trees option of the `bmrsrtadm` command. For a description of the SRT states, see “Shared Resource Trees View” on page 124.

▼ **To attempt recovery of a damaged SRT**

1. Change to the following directory on the boot server on which the SRT resides:
   
   ```bash
   /usr/openv/netbackup/bin
   ```

2. Run the following command:
   
   ```bash
   ./bmrsrtadm
   ```

   The following appears:

   Select one of the following options:

   1. Create a new Shared Resource Tree.
   2. Create a new CD image based Shared Resource Tree.
   3. Copy an existing Shared Resource Tree to a new location.
   4. Modify an existing Shared Resource Tree.
   5. Delete an existing Shared Resource Tree.
   7. Quit.
Enter your selection (1-7) [1] :

3. Select the option to modify an existing shared resource tree. The following appears:
   Enter the name of an existing SRT:

4. Enter the name of the damaged SRT.
   The following appears:
   The SRT you selected is in a DAMAGED state. This typically means that an interrupt occurred while previously performing some operation on the SRT.

   If you believe this SRT is still usable, you may choose to continue.

   If you are not sure this SRT is still usable, you should not continue and should choose to delete the SRT instead.

   Are you sure you want to continue? (y/n) :

5. Enter y.
   The bmrsrtadm program will attempt to repair the SRT. If SRT components are missing, you will be guided through installing them.

   If repair is successful, the bmrsrtadm modify menu appears. When you quit the program, the SRT will be in a READY state.

---

**Breaking a Stale Shared Resource Tree Lock**

*UNIX and Linux boot servers only.*

An SRT in the LOCKED_READ or LOCKED_WRITE state is busy and most operations will not be 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. Alternatively, on UNIX and Linux systems, you can view the SRT states by using the list shared resource trees option of the `bmsrtdm` command. For a description of the SRT states, see “Shared Resource Trees View” on page 124.

▶ **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:

   `./bmsrtdm`

   The following appears:

   Select one of the following options:

   1. Create a new Shared Resource Tree.
   2. Create a new CD image based Shared Resource Tree.
   3. Copy an existing Shared Resource Tree to a new location.
   4. Modify an existing Shared Resource Tree.
   5. Delete an existing Shared Resource Tree.
   7. Quit.

   Enter your selection (1-7) [1] :

3. Select the option to modify the Shared Resource. The following appears:

   Enter the name of an existing SRT :

4. Enter the name of the locked SRT and press ENTER. The following appears:

   The SRT you selected is in a LOCKED state. This typically means that the SRT is busy, and you should wait for it to come unlocked before you continue.

   Would you like to wait for the SRT to come free? (y/n) [y] :

   **Caution**  If you break the lock of an SRT while it is in use, it may become corrupted.

5. Enter **n** to break the lock.

   The following appears:

   If you are ABSOLUTELY SURE nobody is using this SRT and this is a stale lock, you may choose to break the lock and continue.
Deleting a Shared Resource Tree

If you break the lock while somebody is using the SRT, you may corrupt the SRT.

Are you ABSOLUTELY SURE you want to break the lock and continue? (y/n) [n] :

Caution If you break the lock of an SRT while it is in use, it may become corrupted.

6. Enter y to break the lock.

The stale lock will be broken, and the bmrsrtadm command modify menu appears.
When you quit the program, the SRT will be in a READY state.

Deleting a Shared Resource Tree

You can delete an SRT by using the 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 using the bmrsrtadm command

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

   The following appears:

   Select one of the following options:

   1. Create a new Shared Resource Tree.
   2. Create a new CD image based Shared Resource Tree.
   3. Copy an existing Shared Resource Tree to a new location.
   4. Modify an existing Shared Resource Tree.
   5. Delete an existing Shared Resource Tree.
Deleting a Shared Resource Tree

7. Quit.
   Enter your selection (1-7) [1] :

3. Select the option to delete an existing shared resource tree.
   You are prompted to enter the SRT name.

4. Type the name of the SRT and press Enter.
   The following appears:
   You have chosen to delete the "srtname" SRT from the server.
   Are you sure you want to delete this SRT? (y/n) :

5. Enter y to delete the SRT.
   If the SRT is locked, this operation will fail. If this happens, see “Breaking a Stale
   Shared Resource Tree Lock” on page 148.

Deleting an SRT on Windows

On Windows boot servers, use the Shared Resource Tree Administration wizard to delete
an SRT.

▼ To delete an SRT using the shared resource tree wizard

1. From the Start menu on the Windows BMR boot server that hosts the SRT, select
   Programs > VERITAS 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.

3. Select the option to delete an SRT, then follow the prompts.
Deleting a Shared Resource Tree
Managing Boot Media

The following provide information about creating and managing boot media.

Tasks

“Creating Boot Media for UNIX and Linux” on page 155
“Creating Boot Media for Windows” on page 158
“Rewriting an Archived Boot Floppy” on page 160

Related Topics

“Boot Media Overview” on page 153
“About Writing a CD” on page 154
“Archived Boot Floppies View” on page 160

Boot Media Overview

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 are using 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 the shared resource tree for the protected system must exist.

Boot media is created from the resources stored in an SRT, and the boot media must be compatible with the commands and libraries in the SRT and the client.

UNIX and Linux systems can boot from CD media. (Alternatively, UNIX and Linux clients can boot from a BMR boot server on a network. If you use a network boot to begin the restore, boot media is not required.)
Microsoft Windows systems must boot from media, either floppy disk or CD. The following table shows the boot media options for Windows.

<table>
<thead>
<tr>
<th>Windows Boot Media Options</th>
<th>Generic</th>
<th>Custom</th>
<th>SRT Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Floppy Disk</td>
<td>X</td>
<td>X</td>
<td>Network</td>
</tr>
<tr>
<td>CD</td>
<td></td>
<td>X</td>
<td>On the CD</td>
</tr>
</tbody>
</table>

Generic boot media is for clients that have the same brand and type of network interface card. Generic boot media requires that you enter information about the client during the restore process; therefore, you can use generic boot media for more than one client.

Custom boot media is for a specific client. It requires less intervention during the restore process because you enter the client information when you create the boot media.

Boot floppy media can be archived on the boot server so you can recreate a boot floppy without re-entering all of the required information.

BMR does not support DVD boot media.

### About Writing a CD

CD media must be bootable by the system for which you are creating it. To determine the correct way to create a bootable CD for the specific system, see the instructions provided with your CD writing software.

In addition, consider the following:

- The CD image 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 writing software. Burn the CD image onto a CD-ROM using CD writing software that supports ISO-format images for AIX, Linux, and Solaris or supports binary images for HP-UX. The procedures for writing CDs vary between applications; refer to the documentation for procedures.

- The CD writing software may require that ISO-format or binary CD image files end in a `.iso` extension. If necessary, you can add a `.iso` extension to the CD image before you write it.

- If the BMR boot server does not have CD writing hardware and software, transfer the CD image to a system that has CD writing hardware and software. Ensure that the CD image file is transmitted as a binary file and is transferred without errors; corrupted CD image files produce unpredictable results.
Creating Boot Media for UNIX and Linux

For CD media that includes an SRT, the name of the SRT appears as the content of the root directory on the CD.

Label the CD for easy identification. Include the client name (Windows clients), the NetBackup version used, the operating system of the SRT installed, and any extra software installed.

BMR does not use the CD image file after it is created, so you can move, rename, or delete the image file after you write the CD.

Creating Boot Media for UNIX and Linux

On UNIX and Linux systems, use the bmrsrta dm command to create a bootable CD image that contains an SRT. After you create the CD image, you must use CD writing software to burn the image onto a CD.

This process copies an existing SRT to the CD media; therefore, an SRT that supports the client must exist.

The following is the basic information required:

- The name of the SRT you are copying.
- The name to use for the SRT on the CD.
- The path to a directory that has enough free space to store the CD image.

To start the bmr srta dm command

1. On Solaris systems only, use the following command to verify that the vold process is not running on the boot server on which the SRT resides:

   
   ```
   # ps -ef | grep vold
   
   If it is running, do the following:
   
   a. Eject any CD that might be loaded:

   ```

   ```
   # eject
   
   b. Stop the vold process:

   ```

   ```
   # /etc/init.d/volmg t stop
   ```

2. On the boot server on which the SRT resides, change to the following directory:

   ```
   /usr/openv/netbackup/bin
   ```
3. Enter the following command:

```
./bmrsrcadm
```

The following appears:

Select one of the following options:

1. Create a new Shared Resource Tree.
2. Create a new CD image based Shared Resource Tree.
3. Copy an existing Shared Resource Tree to a new location.
4. Modify an existing Shared Resource Tree.
5. Delete an existing Shared Resource Tree.
7. Quit.

4. Select the option to create a new CD image based shared resource tree.

5. To continue with creating the CD image, see the following for more information about the operating system type:
   - “Creating Boot Media for AIX” on page 156
   - “Creating Boot Media for HP-UX” on page 157
   - “Creating Boot Media for Linux” on page 157
   - “Creating Boot Media for Solaris” on page 157

Creating Boot Media for AIX

You must have the AIX installation media that was used to create the SRT you are copying to the CD (even if you created the SRT from a network copy of the media), and you must enter the device name that contains the installation media.

The directory for the CD image should not be a direct prefix of the directory that contains the SRT you are copying. For example, for SRT /export/srt/aix433esm:

- Do not specify /, /export, or /export/srt for the location.
- Specifying /export/srt/mb is valid because it is not a direct prefix of the SRT path.

It is possible, but unusual, that an AIX SRT will be too large to reside on a CD if additional packages are added (such as IBM maintenance levels or VERITAS Volume Manager and File System). If so, the bmrsrcadm command will notify you that the SRT is too large for the CD. For such large AIX SRTs, you must use network boot.
Creating Boot Media for HP-UX

HP-UX uses a binary format that is different from ISO. The CD image file is a binary image of the CD and does not contain an extension; however, you can add a .iso extension to the CD image if your CD writing software requires it.

CD recording programs that are known to work for HP-UX images are as follows:

- Sony CD Extreme. Add a .iso extension to the image file name and use the Global Image or Other Image option from the File menu options.
- Nero. Add a .iso extension to the image file name, and use the Burn Image to Disc option.

**Note** The ROXIO Easy CD Creator recording program does *not* work for HP-UX images.

Creating Boot Media for Linux

For Linux, the `bmrsrtadm` command creates a bootable ISO image file using the name of the SRT with an .iso extension. Any standard CD writing software can be used to write media from this file.

Creating Boot Media for Solaris

You must have the Solaris installation media (Software 1 of 2) that was used to create the SRT you are copying to the CD, and you must enter the device name that contains the installation media.

After entering the information about the SRT, the information you enter depends on the following:

- If VERITAS Volume Manager is installed on the BMR boot server, the following prompt 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 using a raw partition for temporary storage, you will be prompted to continue.
Creating Boot Media for Windows

- If VERITAS Volume Manager is not installed on the BMR boot server, the following prompt 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 image is created, restart the `vold` process (`/etc/init.d/volmgtd start`) if you stopped it before running `bmrsrcadm`.

Creating Boot Media for Windows

Windows systems boot from an image on a floppy disk or CD. The following are the options to create Windows boot media:

- To create floppy disk media, use the Create Windows Boot Floppy wizard.

- To create a bootable CD image, use the Shared Resource Tree Administration wizard. After you create the CD image, you must use CD writing software to write the image onto a CD.

  A generic boot floppy can be used to restore multiple clients; however, it will prompt for the client information at the boot time. A customized boot floppy requires less user input during the restore. The bootable CD is always customized for a client; you need to prepare the client for restore before the CD image can be created.

▼ To create boot media for a Windows client

1. On the Windows BMR boot server, select Programs > VERITAS NetBackup > Bare Metal Restore Boot Server Assistant from the Start menu.

   The Bare Metal Restore Boot Server Assistant screen appears.

2. For floppy disk media, click Boot Floppy Creation Wizard; for CD media, click Shared Resource Tree Administration Wizard.

3. Follow the prompts to create the boot media.

   For more information, see the wizard help.
The following table shows the information required for each boot media type:

<table>
<thead>
<tr>
<th>Item</th>
<th>Floppy Disk Media</th>
<th>CD Media</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Generic</td>
<td>Customized</td>
</tr>
<tr>
<td>Add a manual confirmation (that is, a safety prompt) so that the restore process prompts you to continue before formatting the drive(s) of the target system.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Add a prompt to save any special vendor hardware partition during the restore.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Use extended memory and customize the config.sys file.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>DOS driver to enable SCSI adapter (if the client has a SCSI adapter installed).</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Microsoft client software DSK3-1.EXE and DSK3-2.EXE.¹</td>
<td>X³</td>
<td>X³</td>
</tr>
<tr>
<td>DOS driver for the network interface card in the client.</td>
<td>X³</td>
<td>X³</td>
</tr>
<tr>
<td>Client name and configuration.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Network interface information for the client.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>The path to a directory that has enough free space to store the CD image.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The name of the SRT you are copying.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOS driver for the CD drive of the client.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

¹ You can download this software from ftp://ftp.microsoft.com/BusSys/Clients/MSCLIENT/.
² Only the first time you create a bootable floppy on the boot server.
³ If you cannot obtain the NIC DOS driver, VERITAS recommends that you restore from a CD; CD boot media for Windows does not require a NIC DOS driver.
⁴ BMR includes a default driver that should work with most ATAPI CD-ROM devices.
Rewriting an Archived Boot Floppy

If you archived a customized boot floppy, you can write the image to a diskette without repeating the create boot floppy process.

▼ To rewrite an archive boot floppy for a Windows client

1. On the Windows BMR boot server, select Programs > VERITAS NetBackup > Bare Metal Restore Boot Server Assistant from the Start menu.
   The Bare Metal Restore Boot Server Assistant screen appears.

2. Click Boot Floppy Creation Wizard.

3. Click Next on the Welcome screen.

4. Click Rewrite archived boot floppy and then click Next.

5. Follow the prompts to rewrite the floppy.
   For more information, see the wizard help.

Archived Boot Floppies View

The Archived Boot Floppies view shows the customized Microsoft Windows boot floppy diskette images that have been archived. 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.

When you create a customized Windows boot floppy, you can archive the floppy disk image so you can write a new boot floppy diskette without re-entering information and collecting the resources needed to create a boot floppy.
Archived Boot Floppies Window

Actions for Archived Boot Floppies

<table>
<thead>
<tr>
<th>To</th>
<th>Do the Following</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the archived boot floppies</td>
<td>Select Bare Metal Restore Management &gt; Resources &gt; Archived Boot Floppies.</td>
</tr>
<tr>
<td>Delete an archived boot floppy</td>
<td>Right click on the name in the details pane and then select Delete from the shortcut menu.</td>
</tr>
</tbody>
</table>
Managing Windows Packages

The following provide information about adding Windows software packages to BMR and managing those packages.

**Tasks**

“Adding a Windows Software Package” on page 165
“Deleting a Windows Software Package” on page 166

**Related Topics**

“Packages Overview” on page 163
“Packages View” on page 164

**Packages Overview**

Windows packages are Windows hotfixes, 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 stored in the database comprise the packages pool, the common pool of packages that can be added to restore configurations.

Packages may be required when restoring to a different system, in which case you add them to the restore configuration. If a driver or hotfix required for a dissimilar system restore is not in the Packages view, you have to add it to Bare Metal Restore. **Exception:** you do not have to add a driver to BMR or the restore configuration if it is on the Windows installation media that was used to create the shared resource tree for the target system.

If a package required for a dissimilar system restore is already shown in the Packages view, you can add it to the restore configuration by using the procedures in “Drivers” on page 183.
Packages View

The Packages view shows all the Windows drivers and hotfixes in the BMR packages pool. 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.

If a package includes Discovered in the description, it was discovered during a backup of a protected client.

Packages Window

Actions for Packages

<table>
<thead>
<tr>
<th>To</th>
<th>Do the Following</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete a package</td>
<td>Right click on the driver in the details pane then select Delete from the shortcut menu.</td>
</tr>
</tbody>
</table>
Adding a Windows Software Package

Add a package as follows:

- Use the Windows Software Package wizard on any Windows boot server to add a Windows hotfix, network interface card (NIC) driver, or mass storage device (MSD) driver. (For Windows hotfixes, you must use the wizard.)
- Alternatively, install NetBackup client software on the target system and perform a full BMR backup; the drivers will be saved in that client’s configuration and available for use during a dissimilar system restore. (Windows hotfixes are not saved with a client configuration.)

Before you can add a package, you must have the installation files for the package. Obtain them from the vendor’s Web site, from the installation media provided with the NIC or MSD device, or from another BMR Windows client in your environment. You can download Windows hotfix installation executable files from the Microsoft web site.

**Note** You can add only NIC and MSD drivers and Windows hotfixes. All other types of drivers (audio, video, modem, and so on) must be installed on the system after the restore is complete.

▼ To add a software package using the Windows Software Package wizard

1. From the Start menu on any Windows boot server, select **Programs > VERITAS NetBackup > Bare Metal Restore Boot Server Assistant**.
   The Bare Metal Restore Boot Server Assistant appears.

2. Click **Create Software Package**.
   The Windows Software Package wizard appears.

3. Follow the prompts to add the software package:
   - The type of 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

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 on the computer

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 shown here. The option name in the .inf file should be the same or similar to this one.

Deleting a Windows Software Package

The following procedure deletes a software package.

Caution Do not delete any packages required for a restore.

▼ To delete a software package

1. In the NetBackup Administration Console on the NetBackup master server, expand Bare Metal Restore Management > Resources > Packages.

2. In the details pane, right click on the driver or hotfix you want to delete.

3. Select Delete from the shortcut menu.

4. A confirmation screen appears.

5. Click Yes.

6. The selected package is deleted.
Managing Clients and Configurations

The following provide information about creating and managing clients and configuration.

Tasks

“Copying a Configuration” on page 172
“Discovering a Configuration” on page 174
“Modifying a Configuration” on page 177
“Deleting a Configuration” on page 178
“Deleting a Client” on page 179

Related Topics

“Client Configuration Overview” on page 167
“Bare Metal Restore Clients View” on page 168
“Discovered Configurations View” on page 170
“Change Configuration Dialog Box” on page 180

Client Configuration Overview

Logically, a BMR client is a collection of configurations. A configuration is a collection of information about the system, including the number of disk drives, volume and file system information, number and type of network adapters, network properties, drivers, and other system software components. Most BMR operations are performed on configurations; a configuration is the template used to rebuild a protected system.

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.
Bare Metal Restore Clients View

The saved, current configuration is read-only; you use the current configuration to restore the original protected system to its state at the most recent backup (a *standard* or *self restore*). To restore to a different point in time, different disks, or a different system, you must create a restore configuration by copying a current configuration and then modify the restore configuration.

**Bare Metal Restore Clients View**

The Bare Metal Restore Clients view shows the clients that are protected by BMR and the configurations for each client. You can expand the configuration for a client to see its components:

- Discovered Devices shows the devices that were discovered in the system. *Microsoft Windows clients only.*
- Discovered Hotfixes shows the Windows hotfixes installed on the protected client. *Microsoft Windows clients only.*
- Hosts shows the NetBackup media servers, Bare Metal Restore boot servers, and network hosts that are used during a restore.
- Network Interfaces shows the interfaces defined in the configuration.
- Packages shows other software packages defined in the configuration. *Microsoft Windows clients only.*
- Volumes shows the volumes (and their layouts) in a configuration.

Use the **Refresh** option to update the details pane with new information retrieved from the master server:

- If the Bare Metal Restore Clients node is selected, all the clients and configurations are updated.
- If a single client is selected, all the configurations for that client are updated.
- If a single configuration is selected, only that configuration is updated.
Bare Metal Restore Clients View

Bare Metal Restore Clients Window

<table>
<thead>
<tr>
<th>Client Name</th>
<th>Operating System</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>sx180</td>
<td>AIX 4.3.3.3-40</td>
<td>6.0</td>
</tr>
<tr>
<td>sx181</td>
<td>SunOS 5.9</td>
<td>6.0</td>
</tr>
<tr>
<td>sx180</td>
<td>SunOS 5.9</td>
<td>6.0</td>
</tr>
<tr>
<td>sx181-4</td>
<td>SunOS 5.9</td>
<td>6.0</td>
</tr>
<tr>
<td>sx181</td>
<td>Linux SUSE 6.0</td>
<td>6.0</td>
</tr>
<tr>
<td>sx181-4</td>
<td>Windows 2000</td>
<td>6.0</td>
</tr>
<tr>
<td>sx181</td>
<td>Windows Server 2003</td>
<td>6.0</td>
</tr>
<tr>
<td>sx180</td>
<td>Windows XP</td>
<td>6.0</td>
</tr>
</tbody>
</table>

Actions for Bare Metal Restore Clients View

<table>
<thead>
<tr>
<th>To</th>
<th>Do the Following</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepare to restore</td>
<td>Right click on a client and then select <strong>Prepare to Restore</strong> from the shortcut menu.</td>
</tr>
<tr>
<td>Prepare to discover</td>
<td>Right click on a client and then select <strong>Prepare to Discover</strong> from the shortcut menu. <strong>UNIX and Linux clients only.</strong></td>
</tr>
<tr>
<td>Copy a configuration</td>
<td>Right click on a configuration in the All Bare Metal Restore Clients tree view, select <strong>New</strong> from the shortcut menu, and then complete the fields in the New Configuration dialog.</td>
</tr>
</tbody>
</table>
Discovered Configurations View

Actions for Bare Metal Restore Clients View

<table>
<thead>
<tr>
<th>To</th>
<th>Do the Following</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify a configuration</td>
<td>Right click on a configuration in the All Bare Metal Restore Clients tree view, select Change from the shortcut menu, and then modify the configuration. The current configuration cannot be modified. See “Modifying a Configuration” on page 177.</td>
</tr>
<tr>
<td>Delete a configuration</td>
<td>Right click on a configuration in the All Bare Metal Restore Clients tree view then select Delete from the shortcut menu. A confirmation dialog box appears.</td>
</tr>
<tr>
<td>Delete a client</td>
<td>Right click on a client then select Delete from the shortcut menu. A confirmation dialog box appears.</td>
</tr>
</tbody>
</table>

Discovered Configurations View

The Discovered Configurations view shows all the configurations that have been created by discovering clients. A discovered configuration contains information about physical disks, devices, and other hardware attached to the system. Use the Refresh option to update the details pane with new information retrieved from the master server.

UNIX and Linux client configurations are discovered by running a Prepare to Discover operation.

Windows client configurations are discovered when the client is booted during the restore process and the configuration of the client differs from the configuration used in the Prepare to Restore operation.

Usually, you discover the configuration of a target system so you can map disks during a dissimilar disk restore or map the attributes of a protected system to the target system during a dissimilar system restore.
Discovered Configurations View

Discovered Configurations Window

![Example Image]

Actions for Discovered Configurations View

<table>
<thead>
<tr>
<th>To</th>
<th>Do the Following</th>
</tr>
</thead>
<tbody>
<tr>
<td>View a configuration’s properties</td>
<td>Right click on a configuration in the details pane and then select <strong>Properties</strong> from the shortcut menu.</td>
</tr>
<tr>
<td>Delete a configuration</td>
<td>Right click on a configuration in the details pane and then select <strong>Delete</strong> from the shortcut menu.</td>
</tr>
<tr>
<td>Discover a configuration</td>
<td>Select <strong>Actions &gt; Prepare to Discover. UNIX and Linux clients only.</strong></td>
</tr>
</tbody>
</table>
Copying a Configuration

Copy a configuration so you can:

♦ Restore a client to a state that was saved in a backup prior to the last backup. For more information, see “Restoring to a Specific Point in Time” on page 88.

♦ Restore a client in which the disks have changed. For more information, see “Restoring to Dissimilar Disks” on page 90.

♦ Restore a Windows client to a different system. For more information, see “Restoring to a Dissimilar System” on page 97.

♦ Restore a client to the same hardware but different network properties.

A copied configuration used for a restore is a restore configuration. After you create the restore configuration, you modify it so it matches the target hardware properties (exception: you do not have to modify the point in time restore configuration).

▼ To copy a 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 tree pane, expand the view of the client that contains the configuration you want to copy.

3. Right click on the configuration you want to copy.

4. On the shortcut menu, select New.

   The New Configuration dialog box appears.

5. Complete the fields.

6. Click OK.

To modify the configuration, see “Modifying a Configuration” on page 177.

New Configuration Dialog Box

Use this dialog box to create a new configuration for a client:

♦ A copy of a configuration, usually so you can change configuration values when performing a dissimilar disk restore or dissimilar system restore.
◆ A configuration retrieved from a backup (also known as *point in time*), from which you can restore the client to its state on the date of the backup. For more information, see “Restoring to a Specific Point in Time” on page 88.

New Configuration Dialog Box

![New Configuration Dialog Box](image)

New Configuration Dialog Box Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Configuration Name</td>
<td>Enter the name of the new configuration.</td>
</tr>
<tr>
<td>Copy/Import Configuration</td>
<td>Select to copy an existing configuration of the client so you can edit it.</td>
</tr>
<tr>
<td>Source Configuration</td>
<td>Select the configuration you want to copy.</td>
</tr>
<tr>
<td>Retrieve from backup</td>
<td>Select to retrieve a configuration from the client’s backup image. This read-only configuration restores the system to the state that was saved at the time of the backup.</td>
</tr>
<tr>
<td>Policy</td>
<td>Select the name of the policy used to back up the client. Backups from the selected policy appear in the End Date field.</td>
</tr>
</tbody>
</table>
Discovering a Configuration

New Configuration Dialog Box Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>End Date</td>
<td>Select the date of the backup from which to retrieve the configuration. 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 are restoring. Normally, backup jobs occur on separate days and data streams within the same backup job are separated by seconds or minutes.</td>
</tr>
</tbody>
</table>

Discovering a Configuration

UNIX and Linux clients only.

You can discover the configuration of a UNIX or Linux system; the system does not have to be a NetBackup client. A discovered configuration contains the hardware and software information of a host.

Discovering a configuration adds it to the discovered configurations pool, and the elements of the configuration (such as disk layout) can then be used when performing operations such as dissimilar disk restore.

▼ To discover a configuration

1. In the Bare Metal Restore Management node, select Actions > Prepare to Discover. The Prepare to Discover dialog box appears. If you selected a client in the Hosts > Bare Metal Restore Clients view, the values for that client are included in the dialog box.

2. Complete the fields and enter data as necessary. If you are discovering a client that will be the target of a dissimilar disk restore (DDR) and the protected client’s disks are managed by VERITAS Volume Manager (VxVM), you must specify an SRT that has VxVM installed.

3. Click OK.

4. Boot the client to start the hardware discovery operation.

If using media boot, when BMR prompts you for the client name you must enter the client’s name as it appears in the Tasks view from the prepare to discover operation.
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.

**Prepare to Discover Dialog Box**

*UNIX and Linux clients only.*

Use this dialog box to discover the configuration of a system. The system does not have to be a NetBackup client.

**Prepare to Discover Dialog Box**

If a client is selected in the NetBackup Administration Console window, the values and options for that client are displayed or included in drop-down lists.
Discovering a Configuration

Discovering a configuration adds it to the discovered configurations pool, and the elements of the configuration (such as disk layout) can then be used when performing operations such as dissimilar disk restore.

### Prepare to Discover Dialog Box Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>The operating system of the machine to discover. If a client is selected, the value for that client is displayed.</td>
</tr>
</tbody>
</table>
| Shared Resource Tree      | The shared resource tree to use for the discovery operation. If a client is selected, the list includes the SRTs that match that client’s operating system and level.  
If you are discovering a client that will be the target of a dissimilar disk restore and the protected client’s disks are managed by VERITAS Volume Manager, you must specify an SRT that has VxVM installed. |
| Architecture              | The architecture for the system. If a client is selected, the value for that client is displayed.                                                                                                                                 |
| NetBackup Master Server IP Address | The IP address of the NetBackup master server.                                                                                                                                                                |
| Gateway to the NetBackup Master Server | The gateway to reach the NetBackup master server during the discovery operation.                                                                                                                               |
| Console Device Name       | *AIX systems only.* The name of the device to write messages to. If you do not enter a device, the LEDs on the machine to discover are used to display operational status.  
*Linux systems only.* The name of the device to use as system console; to use the system default, leave this field blank. For a virtual console, specify a device name such as `tty1`. For a serial console, specify a device name and speed, such as `ttyS0,57600`. For information about console naming conventions, see the `serial-console.txt` Linux kernel documentation file.  
If a client configuration was selected for the discovery operation, the field is populated with the values from the configuration. |
| Preload Values from Interface | *Active if Prepare to Discover is selected from the Clients view.* Select an interface to populate the network properties with the values from the interface.                                                      |
Prepare to Discover Dialog Box Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the machine to discover. If an interface is selected in the Preload Values from Interface field, the value from that interface is displayed.</td>
</tr>
<tr>
<td>Network Mask</td>
<td>The network mask of the machine to discover. If an interface is selected in the Preload Values from Interface field, the value from that interface is displayed.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>The gateway for the network routes during the discovery operation. If an interface is selected in the Preload Values from Interface field, the value from that interface is displayed.</td>
</tr>
<tr>
<td>Hardware MAC Address</td>
<td>The media access control (MAC) address of the interface used to boot the client at discovery time. If an interface is selected in the Preload Values from Interface field, the value from that interface is displayed.</td>
</tr>
<tr>
<td>New Configuration Name</td>
<td>The name for the configuration that will be created by the discovery operation.</td>
</tr>
<tr>
<td>Run External Procedure</td>
<td>Run external procedures during the discovery operation. You must create the external procedures and add them to the BMR database. See “Using External Procedures” on page 106.</td>
</tr>
<tr>
<td>Enable Logging</td>
<td>Log events on the master server. Enable logging if you have adequate space in the file system on which the NetBackup log directory resides on the master server. Discovery can increase a restore log file by up to 15 MBs.</td>
</tr>
</tbody>
</table>

Modifying a Configuration

Modify a configuration so you can:

- Restore a client to a state that was saved in a backup prior to the last backup. For more information, see “Restoring to a Specific Point in Time” on page 88.
- Restore a client in which the disks have changed. For more information, see “Restoring to Dissimilar Disks” on page 90.
- Restore a Windows client to a different system. For more information, see “Restoring to a Dissimilar System” on page 97.
- Restore a client to the same hardware but different network properties.
Deleting a Configuration

You cannot modify the configuration named current; you must create a configuration you can edit. For procedures, see “Copying a Configuration” on page 172.

▼ To modify a 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, expand the view of the client that contains the configuration you want to modify.

3. Right click on the configuration you want to modify.

4. On the shortcut menu, select Change.

   The Change Configuration dialog box appears; see “Change Configuration Dialog Box” on page 180.

5. Modify any properties necessary.

Deleting a Configuration

You cannot delete a current configuration.

▼ To delete a 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, expand the view of the client that contains the configuration you want to delete.

3. Right click on the configuration you want to delete.

4. On the shortcut menu, select Delete.

   A confirmation dialog box appears.

5. Click Yes.
Deleting a Client

Deleting a client removes the client and its configuration from the BMR database; it does not remove the NetBackup software on the client, remove it from NetBackup, or delete the backups of the client.

If you delete a client but do not remove it from the NetBackup policy that backs it up (the policy that collects BMR information), the client will be reregistered with BMR the next time it is backed up and will appear in the Bare Metal Restore Clients view.

▼ To delete a client

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

2. Right click on the client you want to delete.

3. On the shortcut menu, select Delete.

   A confirmation dialog box appears.

4. Click Yes.
Change Configuration Dialog Box

Use the Change Configuration dialog boxes to map the attributes of the configuration on the protected system to the restore configuration. Configuration mapping is used to enable point in time restore, dissimilar disk restore, or dissimilar system restore.

- “Configuration Summary” on page 181
- “Drivers” on page 183
- “Hosts” on page 186
- “Hotfixes” on page 188
- “Network Interfaces” on page 190
- “Network Routes” on page 194
- “Volumes” on page 196

Configuration changes are saved differently depending on which NetBackup administration interface you are using:

- 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.

▼ To open the Change Configuration dialog box

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, expand the view of the client that contains a copied configuration.
   You cannot open and edit the current configuration.

3. Right click on the copied configuration.

4. On the shortcut menu, select Change.
Configuration Summary

Use Configuration Summary to view a summary of the configuration or to change a license key for software on the protected system that requires a license key.

Also use this summary information to determine the components of the restore configuration so you can select an SRT that has the appropriate software for the restore.

Configuration Summary
Change Configuration Dialog Box

License Key Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add License Key</td>
<td>Opens a dialog box in which you can change the license key for the selected software.</td>
</tr>
<tr>
<td>Change License Key</td>
<td>Opens a dialog box in which you can change the license key for the selected software.</td>
</tr>
</tbody>
</table>

Client and Configuration Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Items</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The name of the client.</td>
</tr>
<tr>
<td>Operating System</td>
<td>The operating system of the client.</td>
</tr>
<tr>
<td>Service Pack</td>
<td><em>Windows clients only.</em> The service pack version on the client.</td>
</tr>
<tr>
<td>Architecture</td>
<td><em>UNIX and Linux clients only.</em> The architecture of the client.</td>
</tr>
<tr>
<td>NetBackup Version</td>
<td>The NetBackup software version on the client.</td>
</tr>
<tr>
<td>VERITAS Volume Manager Version</td>
<td>The version of VERITAS Volume Manager or VERITAS Storage Foundation for Windows (if any).</td>
</tr>
<tr>
<td><strong>Configuration Items</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The name of the configuration.</td>
</tr>
<tr>
<td>State</td>
<td>The state of the configuration. <em>Saved</em> indicates a configuration that cannot be edited; <em>Copied</em> indicates that the configuration can be edited.</td>
</tr>
<tr>
<td>Last Modification</td>
<td>The date and time the configuration was last modified.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the configuration.</td>
</tr>
</tbody>
</table>
Drivers

*Microsoft Windows clients only.*

Use the **Drivers** dialog box to add mass storage device (MSD) drivers and network interface card (NIC) drivers to the restore configuration:

- If you are restoring to different disks, you may have to add MSD drivers.
- If you are restoring to a different system, you may have to add MSD and NIC drivers.

You also can specify which drivers to load during the DOS phase of the restore and whether to use only BMR discovered drivers.

Drivers Dialog Box

The **Available drivers** windows show the drivers in the packages pool that match the operating system of the client. Select the drivers required for the devices on the target system and click **Add** to move them to the **Drivers to be used during restore** window.
Note If drivers required for a restore are included in the Windows installation CD, they do not need to be listed in the Drivers to be used during restore window.

Related Topics

◆ “Bootable Windows Drivers” on page 184
◆ “Discovered Windows Driver Signing” on page 185

Drivers Mapping Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Moves the selected driver from the Available drivers window to the</td>
</tr>
<tr>
<td></td>
<td>Drivers to be used during restore window.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Opens a dialog box in which you can specify which drivers to load</td>
</tr>
<tr>
<td></td>
<td>during the DOS phase of the restore and whether to use only drivers</td>
</tr>
<tr>
<td></td>
<td>discovered by BMR.</td>
</tr>
<tr>
<td>Remove</td>
<td>Moves the selected driver from Drivers to be used during restore</td>
</tr>
<tr>
<td></td>
<td>window to the Available drivers window.</td>
</tr>
</tbody>
</table>

Bootable Windows Drivers

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 on which 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 associated with the boot partition is loaded. Do so if loading all of the MSD drivers interferes with the boot process of the restore.

▼ To load only the boot partition driver during the boot phase

1. In the Drivers dialog box, click Advanced.

   The Advanced Mass Storage Driver Dialog box appears.

2. Move the MSD driver for the boot partition from the Available Mass Storage Drivers window to the Bootable Drivers window.

3. Click OK.
Discovered Windows Driver Signing

When BMR saves third party drivers from a protected system (third party drivers are those that are not part of the Windows distribution), the driver signing is lost. During the BMR restore process, the Windows 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 drivers during the restore

1. In the Drivers dialog box, click Advanced.
   
   The Advanced Mass Storage Driver Dialog box appears.

2. Select Use Bare Metal Restore Discovered Drivers.

3. Click OK.
**Change Configuration Dialog Box**

**Hosts**

Use the **Hosts** 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.

**Hosts Dialog Box**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Opens a dialog box in which you can add a new host, specify its role, and enter its IP address and gateway.</td>
</tr>
</tbody>
</table>
### Change Configuration Dialog Box

**Hosts Mapping Actions (continued)**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change</td>
<td>Opens a dialog box in which you can change the properties for the selected host.</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes the selected host. If you did not want to remove the host, click <strong>Cancel</strong> to exit the Change Configuration dialog box without applying the changes.</td>
</tr>
</tbody>
</table>

**NetBackup Client Information**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Name</td>
<td>The name by which NetBackup knows the client. The client name specified here must match the client name in the NetBackup policy that backs up the client.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the client. All IP addresses defined in the network interfaces are in the drop-down list.</td>
</tr>
<tr>
<td>NetBackup Version</td>
<td>The NetBackup software version on the client.</td>
</tr>
</tbody>
</table>
Hotfixes

Microsoft Windows clients only.

Dissimilar system restore only.

Use the Hotfixes dialog box to add Windows hotfixes to the restore configuration for a dissimilar system restore.

Hotfixes Dialog Box

The Original Hotfixes window shows the hotfixes that are on the protected system. If Yes is displayed in the Dissimilar System Restore Requirement column, you must add that hotfix to the restore configuration (that is, move the hotfix from the Available hotfixes window to the Hotfixes to be used during restore window). DSR-required hotfixes are ones that apply to the Windows kernel.
BMR saves information about hotfixes on a protected client in the client’s current configuration, but BMR does not add those hotfixes to the packages pool. If the hotfix is not listed in the **Available hotfixes** window, you must use the Windows Software Package wizard to add it to the BMR database; after it is added, it will appear in the **Available hotfixes** window. For procedures, see “Managing Windows Packages” on page 163.

### Hotfixes Mapping Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Moves the selected hotfix from the <strong>Available hotfixes</strong> window to the <strong>Hotfixes to be used during restore</strong> window.</td>
</tr>
<tr>
<td>Remove</td>
<td>Moves the selected hotfix from <strong>Hotfixes to be used during restore</strong> window to the <strong>Available hotfixes</strong> window.</td>
</tr>
</tbody>
</table>
Network Interfaces

Use the Network Interfaces dialog box to add or remove interfaces or change the network identity associated with an interface.

Network Interfaces Dialog Box

The Original Network Information is read-only. The New Network Information shows the values used for the restore. If the configuration has not been edited, the top and bottom panes show the same information.

Related Topics

- “Importing and Mapping Interfaces” on page 191
- “Changing Interfaces Manually” on page 192
- “UNIX and Linux Boot Interface” on page 193
Network Interface Mapping Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initialize</td>
<td>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.</td>
</tr>
<tr>
<td>Unmap All</td>
<td>Unmaps all mapped interfaces in the New Network Information window and changes all interfaces in the Original Network Information window to Unmapped. Unmapping removes the name, IP addresses, network masks, gateways, and DHCP and bootable attributes. MAC addresses are not removed.</td>
</tr>
<tr>
<td>Map</td>
<td>Right click on an interface in the Original Network Information window and select Map from the shortcut menu. The Map Interface dialog box appears, in which you select an interface to map the IP address, netmask, and domain name from the source network card to. The MAC address of the original interface is not mapped to the target interface.</td>
</tr>
<tr>
<td>Unmap</td>
<td>Right click on an interface in the New Network Information window and select Unmap from the shortcut menu. Unmapping an interface removes the name, IP addresses, network masks, and DHCP and bootable attributes. MAC addresses are not removed.</td>
</tr>
<tr>
<td>Change</td>
<td>Right click on an interface in the New Network Information window, select Change from the shortcut menu.</td>
</tr>
</tbody>
</table>
Change Configuration Dialog Box

▲ To import and map interfaces

1. Click Initialize.
   The Import Configuration dialog box appears.

2. Select the client configuration to import.

3. Click OK.
   The network hardware information is imported into the New Network Information window, replacing the interfaces that were in the window. The network identify (IPs, routes, and so on) is not imported.

4. Right-click on an interface in the Original Network Information window and select Map from the shortcut menu.
   The Map or Change Interface dialog box appears.

5. Select an interface from the Map to Interface drop-down list.

6. Click OK.
   The IP address, netmask, and fully qualified domain name will be applied to that interface on the restored system.

Changing Interfaces Manually

If you are restoring to a dissimilar system and you did not save the target system’s configuration, you can change the interface properties to use during a restore manually.

You must first determine the MAC addresses of the NICs in the target system.

▲ To change an interface manually

1. Right-click on an interface in the New Network Information window and select Change from the shortcut menu.
   The Map or Change Interface dialog box appears. Because you are changing an interface, the dialog box includes the **Hardware MAC Address** field.

2. If using DHCP, select **Use DHCP**. Go to step 5.

3. Select a row of attributes in the Attributes for Network Interface window and click Change.
   The Add Network Identify dialog box appears.
4. Enter the IP address, netmask, and fully qualified domain name from the interface on the protected system and 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.

**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 which interface 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.

Use the following table to determine the correct interface.

<table>
<thead>
<tr>
<th>Platform or Hardware Type</th>
<th>Bootable Network Interface(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX ¹,²</td>
<td>Integrated Ethernet, Ethernet card, or Token Ring</td>
</tr>
<tr>
<td>HP-UX</td>
<td>Integrated Ethernet only</td>
</tr>
<tr>
<td>Linux</td>
<td>Any Ethernet device</td>
</tr>
<tr>
<td>Solaris</td>
<td>Any Ethernet device</td>
</tr>
</tbody>
</table>

¹. Chp hardware only.

². Booting the RS/6000 from a network adapter requires support in the system firmware.

▼ **To specify a boot interface**

1. In the New Network Information window of the Network Interfaces dialog box, right click on the interface that you want to use as the boot interface.

2. Select **Change** from the shortcut menu.

   The Map or Change Interface Dialog box appears.

3. Click **Bootable**.

4. Click **OK**.
Network Routes

Use the Network Routes dialog box to add a network route to use during the restore.

Network Routes Dialog Box

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 can occur during disaster recovery at a different location, when you move servers from one subnet to another, or when intervening routers 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 will be successful. However, if the IP address of the router between them changes, the client may not be able to reach the master server because the configuration does not include the correct route to it. Therefore, you would 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 dialog box)
- Network routes specified on this screen
- The default route specified on this screen

### Network Routes Mapping Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Gateway</td>
<td>The gateway to use if no other route reaches a host.</td>
</tr>
<tr>
<td>Add</td>
<td>Opens a dialog box in which you can enter the properties for a new network route.</td>
</tr>
<tr>
<td>Change</td>
<td>Opens a dialog box in which you can change the properties for the selected route.</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes the selected route.</td>
</tr>
</tbody>
</table>
Volumes

Use the Volumes dialog box to map the volume configuration from the protected client to the new disks of the restore configuration.

Volumes Dialog Box

You can perform the following volume mapping and configuration change operations:
- Change the disks that make up a disk group
- Control which file systems are restored
- Control which logical volumes 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/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.

Topics

◆ “Mapping and Unmapping Volumes” on page 197
◆ “Understanding the Views” on page 199

Mapping and Unmapping Volumes

Wizards guide you through the mapping process; the appropriate wizard appears depending on what you selected to map.

Mapping is saved between sessions, so you can stop mapping and then resume mapping later (unless you are mapping during a dissimilar disk restore process, in which case when 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 contained in it are mapped or unmapped.

The following are the main options:

◆ 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. 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.

Notes for UNIX and Linux DDR

◆ Shared disks in a cluster are marked restricted.
◆ Unused VxVM disks on Solaris clients are marked restricted.
◆ Linux LVM volume groups that have physical volumes created on top of multidevices cannot be mapped with the same configuration. The physical volumes are mapped to either disks or partitions but not a multidevice.

Notes for Windows DDR

◆ The system drive is always mapped and cannot be moved; however, you can resize it if you are mapping disks before the restore.
◆ Original disks and their volumes that were clustered cannot be mapped.
Change Configuration Dialog Box

◆ Discovered disks that have the same disk signature as an original disk that was clustered cannot be mapped.

▼ 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. Click the appropriate map option on the shortcut menu (the map options are context sensitive). The mapping wizard starts with the appropriate context:
   ◆ 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, followed by the volume mapping wizard for each volume (the required properties will be set). If the element is a disk that is not in a disk group, not part of a volume group (AIX), and none of its volumes span other disks (mirrors, stripes, and so on), the disk mapping wizard appears and all the volumes and file systems will be populated into the target disk. The mapped state will be set for both source and target elements (disks, volumes and file systems).
   ◆ Map Disk Group. The disk group mapping wizard appears.

The mapping wizards will not allow the size of a volume or partition to be reduced below the space required by all the files to be restored.

▼ To unmap an element

1. In the Table View or Disk View, right click on 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: Unmap, Unmap Disk, Unmap Volume, and so on.)

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 on the volume in the New Volume Layout window.

2. Click Change Size on the shortcut menu.
3. Change the size of the volume.

▼ To restrict a disk or remove restriction

1. In the Table View or Disk View, right click on the disk in the New Volume Layout window.

2. Click either Restrict or Remove Restriction on the shortcut menu:
   - Restrict prevents a disk to be used as a target for mapping; also, it will not be formatted, and the volume groups or volumes on it will not be created or restored.
   - Remove Restriction removes the restriction so the disk can be used as a target; if mapped, it will be formatted and its volumes and volume groups will be created and restored.

▼ To promote a disk to dynamic on Windows

1. In the Table View or Disk View, right click on 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

If the disk is a basic disk, first promote it to a dynamic disk.

1. In the Table View or Disk View, right click on the element in the New Volume Layout window.

2. Click either Add Mirror or Remove Mirror on the shortcut menu.

3. If you are adding a mirror, select the disk to use for the mirror.

Understanding the Views

The tree view (the left pane) shows the elements that are part of the disk layout. The elements in the tree change depend on the operating system of the client and the volume managers that are enabled. The tree view filters the details pane on the right; selecting an element in the tree displays its attributes in the right pane and filters out all other elements so they do not appear in the details pane.

Indicators show an element’s state throughout the mapping process:
   - Unmapped. The element has not been mapped into the new configuration.
Change Configuration Dialog Box

- Mapped. The element is mapped into the new configuration.
- Restricted. The disk is or was being shared or manually restricted and cannot be used.

The details pane on the right contains a Tables View and Disks View tab.

- 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 is shown 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 Original Volume Layout (the top window) shows the volume layout and the source elements (such as disks, disk groups, volumes, and so on) in the original system.

The amount of space used and the size of the disk is shown. To view the properties for an element, right click on the element and select Properties from 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, you must map elements from the Original Volume Layout to the New Volume Layout.

Hierarchy of Elements

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.

Elements

The following tables show the various elements in the tree view and what is displayed in the Table View tab and Disk View tab.

### AIX and HP-UX Logical Volume Manager Elements

<table>
<thead>
<tr>
<th>Selected Element</th>
<th>Displayed in Table View</th>
<th>Displayed in Disk View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Volume Manager</td>
<td>Volume groups and volumes.</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>
### AIX and HP-UX Logical Volume Manager Elements (continued)

<table>
<thead>
<tr>
<th>Selected Element</th>
<th>Displayed in Table View</th>
<th>Displayed in Disk View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume groups</td>
<td>Volume groups in the configuration.</td>
<td>Disks that are part of any volume group (ordered by volume group).</td>
</tr>
<tr>
<td>A specific volume group</td>
<td>Disks that are part of that volume group.</td>
<td>Disks that are part of that volume group.</td>
</tr>
<tr>
<td>Volumes</td>
<td>All the volumes managed by the LVM.</td>
<td>Disks that have LVM volumes.</td>
</tr>
<tr>
<td>A specific volume</td>
<td>Disks that contain that volume.</td>
<td>Disks that contain that volume.</td>
</tr>
</tbody>
</table>

### Empty Disks Elements

<table>
<thead>
<tr>
<th>Selected Element</th>
<th>Displayed in Table View</th>
<th>Displayed in Disk View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empty disks</td>
<td>Disks not used.</td>
<td>Disks not used.</td>
</tr>
</tbody>
</table>

### Nonmanaged Solaris Elements

<table>
<thead>
<tr>
<th>Selected Element</th>
<th>Displayed in Table View</th>
<th>Displayed in Disk View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-managed</td>
<td>Disks and partitions.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Disks</td>
<td>All disks that are not managed by VxVM and are not in an SVM disk set.</td>
<td>All disks that are not managed by VxVM and are not in an SVM disk set.</td>
</tr>
<tr>
<td>Slices</td>
<td>All slices that are not managed and are not used as SVM metadevices.</td>
<td>All disks that contain nonmanaged slices.</td>
</tr>
</tbody>
</table>

### Solaris Volume Manager Elements

<table>
<thead>
<tr>
<th>Selected Element</th>
<th>Displayed in Table View</th>
<th>Displayed in Disk View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris Volume Manager</td>
<td>Disk sets and volumes.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Disks sets.</td>
<td>All named (nonlocal) sets.</td>
<td>Disks that are part of a named (nonlocal) set (ordered by disk set).</td>
</tr>
<tr>
<td>A specific disk set</td>
<td>Disks that are part of that disk set.</td>
<td>Disks that are part of that disk set.</td>
</tr>
</tbody>
</table>
### Change Configuration Dialog Box

Solaris Volume Manager Elements (continued)

<table>
<thead>
<tr>
<th>Selected Element</th>
<th>Displayed in Table View</th>
<th>Displayed in Disk View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volumes</td>
<td>All SVM volumes.</td>
<td>Disks that have SVM volumes.</td>
</tr>
<tr>
<td>A specific volume</td>
<td>Disks that include that volume.</td>
<td>Disks that include that volume.</td>
</tr>
</tbody>
</table>

VERITAS Volume Manager and Storage Foundation for Windows Elements

<table>
<thead>
<tr>
<th>Selected Element</th>
<th>Displayed in Table View</th>
<th>Displayed in Disk View</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERITAS Volume Manager</td>
<td>Disk groups, volume sets, and volumes.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Disk groups</td>
<td>Disk groups in the configuration.</td>
<td>Disks that are part of any disk group.</td>
</tr>
<tr>
<td>A specific disk group</td>
<td>Disks that are part of that disk group.</td>
<td>Disks that are part of that disk group.</td>
</tr>
<tr>
<td>Volumes</td>
<td>All the volumes managed by Volume Manager.</td>
<td>Disks that contain Volume Manager volumes (ordered by disk group)</td>
</tr>
<tr>
<td>A specific volume</td>
<td>Disks that contain that volume.</td>
<td>Disks that contain that volume.</td>
</tr>
</tbody>
</table>

Windows Elements

<table>
<thead>
<tr>
<th>Node</th>
<th>Displayed in Table View</th>
<th>Displayed in Disk View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Disk Management</td>
<td>Disk and volumes</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Disks</td>
<td>All disks in the system.</td>
<td>All disks in the system.</td>
</tr>
<tr>
<td>Volumes</td>
<td>All volumes defined in the system, managed or unmanaged.</td>
<td>Disks that contain volumes, regardless of which volume manager created them.</td>
</tr>
<tr>
<td>One specific volume</td>
<td>Disks that the volume spans.</td>
<td>Disks that the volume spans.</td>
</tr>
</tbody>
</table>
Managing Boot Servers

Boot servers provide the environment that is required to rebuild a protected client, including resources such as shared resource trees (SRT). For UNIX systems, a boot server also provides the resources used to boot the client system when it performs a network boot prior to restore.

Boot server software is installed from the NetBackup installation media.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>“Removing a Boot Server” on page 205</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>“Installing Bare Metal Restore” on page 13</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Topics</th>
<th>“Boot Server Requirements” on page 203</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>“Boot Servers View” on page 204</td>
</tr>
</tbody>
</table>

Boot Server Requirements

The following are the requirements for boot servers

For general SRT requirements related to boot servers, see “Shared Resource Tree Overview” on page 123.

General Boot Server Requirements

- 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. Also, a client at a specific operating system version requires a boot server of the same or later operating system version. For example, to restore a Solaris 8 client, you need a boot server at Solaris 8 or later version.

- A boot server must run an operating system at the same or later version of the SRTs it will host.
HP-UX Boot Server Requirements

- Each network segment with HP-UX clients must have an HP-UX boot server that can support the clients.
- The Ignite version of an SRT on an HP-UX boot server must match the Ignite version that is installed on the boot server.
- A single HP-UX boot server can only serve a single SRT at a time. For example, an HP-UX 11.11 BMR boot server can serve either an HP-UX 11.11 SRT or an HP-UX 11.00 SRT, but not both at the same time. A newly created SRT invalidates the existing SRT.

Linux Boot Server Requirements

- Each network segment that has Linux clients must have a Linux boot server.

Solaris Boot Server Requirements

- Each network segment with Solaris clients must have a Solaris BMR boot server that can support the clients; however, there are ways to minimize the impact of this requirement:
  - When needed, you can install BMR boot server software on a Solaris machine in the network segment and create an an SRT after the client has failed and needs to be restored.
  - The Solaris BMR boot server can be defined on a Solaris machine that has a physical IP presence on multiple networks.
    That is, a single Solaris BMR boot server with multiple network interfaces can be used for Solaris BMR clients on each of the network segments to which it is attached.
  - You can configure a relay boot server to allow Solaris machines on remote subnets to boot from a BMR boot server that can be reached using a network gateway. Contact your support representative for a Tech Note that describes the procedure.

Boot Servers View

The Boot Servers view shows all the boot servers that are defined for the current master server. You can select one server only in the details pane. 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.
Removing a Boot Server

You can remove a boot server by uninstalling it. For procedures, see:
Removing a Boot Server

- “Uninstalling a BMR Boot Server from a UNIX or Linux System” on page 22
- “Uninstalling a BMR Boot Server from a Windows System” on page 35
Troubleshooting

See the following for troubleshooting information:

- “Problems Booting from CD” on page 207
- “Long Restore Times” on page 208
- “Restore Fails on Windows Client with Multiple Identical NICs” on page 208
- “Networking Problems at DOS Phase During Restore” on page 209
- “DSR Troubleshooting” on page 210
- “Solaris Media Boot Network Parameters Issue” on page 211
- “To Recover from Deleting a Client Accidentally” on page 211

Problems Booting from CD

AIX, Linux, and Solaris platforms use a common bootable CD format (ISO-9660); HP-UX uses Logical Interchange Format (LIF). If a system will not boot from the CD, place it in a system that has a CD-ROM drive and examine the contents (ISO format can be read by either UNIX or Windows platforms):

- If the contents of the CD are a single file, it was written as a data CD instead of an ISO-9660 CD image. Repeat the burning procedure but use the options required to burn an ISO image file.

- If the CD is blank or unreadable, remove it from the drive and examine it closely to determine if it has been written to. Some CD burning software by default simulate burning a CD to test the capabilities of the CD burning hardware and will not burn the CD until the test-only option is turned off. Repeat the burning procedure with the test-only option disabled.

- If booting was partially successful or if it appears that some files are present but some are missing or corrupted, either the burning process or the file transfer from the BMR boot server to the machine with the CD writer may have failed.
Long Restore Times

- A partially burned CD may be bootable but may be missing significant portions of its content. Lowering the CD writing speed may allow a successful burn. Using the test after writing or verify option offered by some CD writing software may help detect unsuccessful CD writes.

- A common cause of corruption is transferring the file with FTP in ASCII transfer mode rather than binary mode.

- Determine if the CD boots successfully on another, similar machine. 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 being read.

- Verify that you are using the correct procedures to boot the client machine from CD.

- Try booting the client from the installation media to ensure that the machine is not having a hardware problem booting from the CD.

Long Restore Times

If a restore takes an unusually long time (20 hours versus 2 hours), there may be a mismatch of media speed between the adapter and the switch/hub to which it is connected. For example, if the media speed is set to 100MB full duplex, the restore slows down because it is connected to a hub which uses half duplex.

Try changing the media speed to match that of the hub/switch, or change the hub/switch settings to match that of the client.

Restore Fails on Windows Client with Multiple Identical NICs

If a restore fails during the DOS portion of the recovery on a Windows client that has multiple identical network interface cards (the BMR Restore Wizard displays a red X next to Retrieving Client Information), the wrong network interface may be activated. DOS does not always identify PCI slot numbers in the same way that Windows does. Therefore, during the DOS portion of the restore, DOS may not use the correct slot number for the NIC 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.
Networking Problems at DOS Phase During Restore

- 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:

  a. When the failure occurs (the BMR Restore Wizard displays a red X next to Retrieving Client Information), press the F1 key to see the details of the error.

  b. 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 onto which the driver loaded.

  c. Use the slot values to specify the slot number when you enter the client information (either when creating 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 have tried all of the slot numbers, the error may be caused by DOS memory problems. See “Networking Problems at DOS Phase During Restore” on page 209.

Networking Problems at DOS Phase During Restore

BMR uses the following config.sys during the DOS phase while restoring a Windows client.

```plaintext
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:

```plaintext
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 options added to this line. The DOS phase of the restore may fail, indicated by a red “X” next to the Loading NIC Drivers, Starting Networking or Retrieving Client Information status lines. If this occurs, press F1 to view the details; check the status screen for the following error:

  Error 8: There is not enough memory available.
DSR Troubleshooting

This error indicates that not enough memory is available to enable networking. To configure more memory, change this line to the following:

```text
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:
  ```text
  DEVICE=A:\BIN\EMM386.EXE
  ```

- Some machines require that the line be removed. Some BIOS and NIC driver combinations do not work well with EMM386, and the machine may hang while booting DOS. The system will not respond to any key strokes or to Ctrl+Alt+Delete. For this problem, remove this line from the file.

**DSR Troubleshooting**

**HAL Differences Warning**

**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 is missing some required hotfixes.

**Cause**
Required hotfixes are missing from the configuration.

**Solution**
If the restore is not a dissimilar system restore, click **Cancel**.

If the restore is a dissimilar system restore, add hotfixes to the configuration and restart the restore. You may also install the hotfixes in the repair Windows installation and click **Retry**.

**Duplicate IP Addresses on 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 being 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 to determine if any machine 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 even if they are different than the network parameters for the boot interface configured in BMR.

If network parameters for the client exist, the restore may fail.

The work around this issue, do one of the following:

- Remove all references to the client system from the following files in all other machines in the subnet of the client:

  /etc/ethers file
  /etc/bootparams

- Unplug the booting client from the network until after the media boot has configured the network parameters for the restore.

To Recover 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, and the client appears again in the Bare Metal Restore Clients view.

However, if the client and configuration are deleted after a client fails and before it is restored, you can use the bmrs command to retrieve the client’s configuration from a previous point in time. (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 clientIdname
-destination newConfigname -enddate dateformat -policy policymename
```

For more information about the bmrs command, see the NetBackup Commands for UNIX or NetBackup Commands for Windows manual.
To Recover from Deleting a Client Accidentally
Index

A
accessibility features 15
Active Directory
   Windows 67
   activity
      monitoring 43
      using the Tasks view 44
      viewing BMR logs 46
add client resources 58
adding clustering software to an SRT 137
adding license key 182
adding new driver 165
adding to packages pool 165
AIX
   boot interface 193
   external procedure environment
      variables 114
   media boot 75
   network boot 71
ALL_LOCAL_DRIVES directive 55
archived boot floppy
   rewriting 160

B
backups
   ALL_LOCAL_DRIVES directive 55
   back up the client 51
   configuring policies to back up BMR
   clients 52
   ensure successful 54
   job status 43
   monitoring 43
   perform complete 53
   save custom files 54
   use the same client name in multiple
      policies 55
Bare Metal Restore
   overview 1
   Bare Metal Restore Clients view 168
Bare Metal Restore Management window 3
boot floppy
   rewriting archived 160
boot interface
   AIX 193
   client 193
   HP-UX 193
   Linux 193
   Solaris 193
   specifying 193
   UNIX and Linux 193
boot media
   creating for AIX 156
   creating for HP-UX 157
   creating for Linux 157
   creating for Solaris 157
   creating for UNIX and Linux 155
   creating for Windows 158
   custom defined 154
   DVD 154
   generic defined 154
   overview 153
   rewriting an archived boot floppy 160
boot server
   choosing 6
   defined 203
   network segment 204
   removing 205
   requirements 203
   restoring 106
Boot Servers view 204
booting Windows clients
   PXE boot 81
   breaking a stale shared resource tree
      lock 148

C
CD
   ISO format 154
writing 154
Change Configuration dialog 180
changing license key 182
clean up restore task 64
client
  deleting 179
deleing accidentally 211
clusters
  adding clustering software to an SRT 137
  and dissimilar disk restore 91
configuration
  changing 177
  collecting and saving during backup 43
copying 172
creating restore 172
current 168
defined 4
deleting 178
deleting accidentally 211
discovering 174
editing 177
  modifying 177
  modifying a restore 177
restore 4, 172, 177
retrieved from backup 173
saved 168
Configuration Summary dialog 181
copying a client configuration 172
creating a restore configuration 172
creating boot media 58

D

  DDR see dissimilar disk restore
decommissioning BMR 4.7 40
deleting a client 179
deployment planning worksheets 6
dialog
  Configuration Summary 181
  Drivers 183
  Hosts 186
  Hotfixes 188
  Network Interfaces 190
  Network Routes 194
  Prepare to Discover 175
  Prepare to Restore Client 65
  Change Configuration 180
discovered drivers
  using during restore 185
discovering a configuration 174
discovery 177
  running external procedures 177
discovery boot 174
disk recovery behavior
  overview 66
dissimilar disk restore
  and clusters 91
  introduction 90
  Linux notes 91
  mapping before the restore 90
  mapping during the restore 91
  overview 90
  SAN 117
  UNIX and Linux clients 91
  UNIX notes 91
  when to performing mapping 90
  when to use 91
  Windows clients 94
  Windows notes 94
  Windows shared disks 94
dissimilar system restore
  adding MSD drivers 101
  adding NIC drivers 101
  adding Windows hotfixes 101
  creating boot media 102
  creating restore configuration 100
determining hardware differences 99
  first logon 103
  introduction 97
  mapping disks 102
  restoring the client 102
  SAN 117
  when to use 98
DOS driver
  for network interface card 159
drivers
  bootable Windows 184
discovered Windows 185
  DOS driver for NIC 159
  finding the correct 166
  signing 185
  using discovered 185
  Drivers properties 183
  DSR see dissimilar system restore
  DVD
    boot media 154
dynamic disk
  promoting in Windows 199
external procedures
adding to database 108
client-specific names 107
converting from 4.7 39
data transfer 109
environment variables 113
AIX 114
HP-UX 115
Linux 113
Solaris 115
UNIX 113
Windows 115
error handling 112
exit codes 112
interaction with 110
logging 110
names 107
naming 107
operating system specific names 108
operational states 111
points 107
running 109
running during discovery 177
running during restore 66
using 106

hosts
adding to configuration 186
changing in configuration 186
removing from configuration 186
Hosts properties 186
hotfixes 165
adding to configuration 188
Hotfixes properties 188
HP-UX
boot interface 193
external procedure environment
variables 115
media boot 76
network boot 72

identifying the systems to protect 5
Internetwork Packet Exchange 101
IPX 101

job status 43

license key
adding 182
adding on Windows systems 26
changing 182
Linux
boot interface 193
boot server location 204
dissimilar disk restore notes 91
external procedure environment
variable 113
installing device drivers in SRT 142
media boot 77
network boot 74
SAN not supported 116
logging
configuring and using 48
during a discovery 177
during a restore 66
external procedures 110
log file location 46
log filenames defined 47
originator IDs 47
restore log locations 49
viewing logs 46
vxlogcfg command 49
vxlogmgr command 49
vxlogview command 49
logging during 177

mapping
disk groups 197
disk sets 197
disks 197
network interfaces in configuration 190
volume groups 197
volumes 197
mapping and unmapping volumes
dissimilar disk restore
mapping and unmapping
volumes 197
mass storage device
adding drivers to configuration 183
adding drivers to packages pool 165
bootable Windows drivers 184
finding correct drivers 166
media boot
AIX 75

Index
HP-UX 76
Linux 77
Solaris 78
Microsoft
  Active Directory 67
  client software 159
migrating from BMR 4.7 37
modifying a restore configuration 177
modifying client configuration 177
monitoring
  activity 43
  backups 43
MSD see mass storage device
multiple network interface
  (multihomed) 118

N
  network boot
    AIX 71
    HP-UX 72
    Linux 74
    Solaris 74
network interface card
  adding driver to configuration 190
  adding drivers to configuration 183
  adding drivers to packages pool 165
  DOS driver 159
  finding correct drivers 166
Network Interfaces properties 190
network routes
  adding to configuration 194
  configuring in configuration 194
  removing from configuration 194
Network Routes properties 194
NIC see network interface card

O
  one-button restore
    external procedures 106
  originator IDs 47

P
  packages
    adding new driver 165
    adding to packages pool 165
  packages pool 164
    defined 163
  Packages view 164
  patchadd 142
  pkgadd 142
  point in time restore
    creating configuration for 89
    introduction 88
    overview 88
    when to use 89
    prepare to discover
      defined 4
  Prepare to Discover dialog 175
  prepare to restore
    client 64
    enabling logging 66
    importing disks 66
    nonrestored disks 66
    quick formatting for Windows disks 66
    running external procedures 66
    system disks and volumes only 66
  Prepare to Restore Client dialog 65
  protection domain
    defined 4
    overview 2
  PXE boot
    preparing for 81
    Windows clients 81

R
  refresh 3
  restore
    BMR boot servers 106
    clean up 64
    dissimilar system
      creating configuration for 100
      enabling logging during 66
      formatting Windows disks 66
      importing disks 66
      log locations 49
      nonrestored disks 66
      overview 62
      point in time
        creating configuration for 89
        overview 88
        when to use 89
      process overview 62
      running external procedures 66
      system disks and volumes only 66
      task state 45
      unallocate resources 64
      Windows
        boot the client 80
        clients 79
UNIX boot from CD 207

U
updating information in the views 3
using external procedures 106
using the NetBackup Activity Monitor 43
using the Tasks view 44

V
verify client protection 59
VERITAS Cluster Server 137
VERITAS Storage Foundation for Windows
and clusters 94
shared disks 94
viewing BMR logs 46
Volumes properties 196
vxlogcfg command 49
vxlogmgr command 49
vxlogview command 49
VxSFW see VERITAS Storage Foundation for
Windows
VxVM see VERITAS Volume Manager

W
Windows
Active Directory 67
adding drivers to configuration 183
adding drivers to packages pool 165
bootable mass storage device drivers 184
discovered drivers 185
dissimilar disk restore notes 94
driver signing 185
dynamic disk
promoting 199
external procedure environment
variables 115
finding correct drivers 166
formatting disks 66
worksheets
BMR boot server 8
network topology 9
shared resource tree 12
writing a CD 154