NetBackup™ Bare Metal Restore Administrator's Guide

UNIX, Windows, Linux

Release 11.2

VERITAS
now part of Cohesity

NetBackup™ Bare Metal Restore™ Administrator's Guide

Last updated: 2026-05-28

Legal Notice

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1

Introducing Bare Metal Restore

This chapter includes the following topics:

About Bare Metal Restore

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

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

- Run a single command or a single mouse click from the NetBackup master server.
- Reboot the client to get client recover automatically.
  Separate system backups or reinstallations are not required.

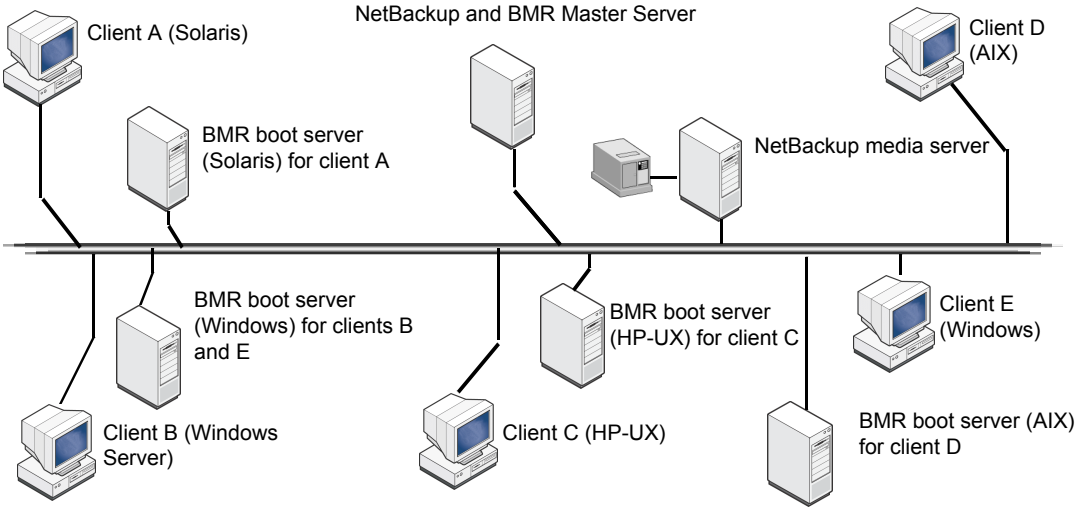
Table 1-1 shows the components of a BMR protection domain.

Table 1-1 BMR components

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

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

Figure 1-1 Example of BMR protection domain



Server DR protection using BMR

The process of Protecting servers from disaster using BMR occurs in three phases. These phases are

- BMR Enabled backup

  NetBackup backup policy needs to be BMR-enabled so that during client backup, client system skeleton information is backed up which is required to recover client when DR is intended. This system skeleton info comprises OS details, disk information, volume details, file system information and network information. For details about BMR Backup process, refer chapter *Protecting clients.*

- Recovery Pre-requisites

  Setting of restore prerequisite can be done any time prior to DR of client is intended. It is recommended to have this prerequisite little prior to avoid any delay in recovery. During this phase, recovery critical software i.e., share resource tree needs to be prepared on BMR Boot server. This SRT forms a staging environment to do client recovery. Single SRT can be used to recover clients belonging to same operating system family. For details about recovery pre-requisites, refer chapter *Setting up restore environments.*

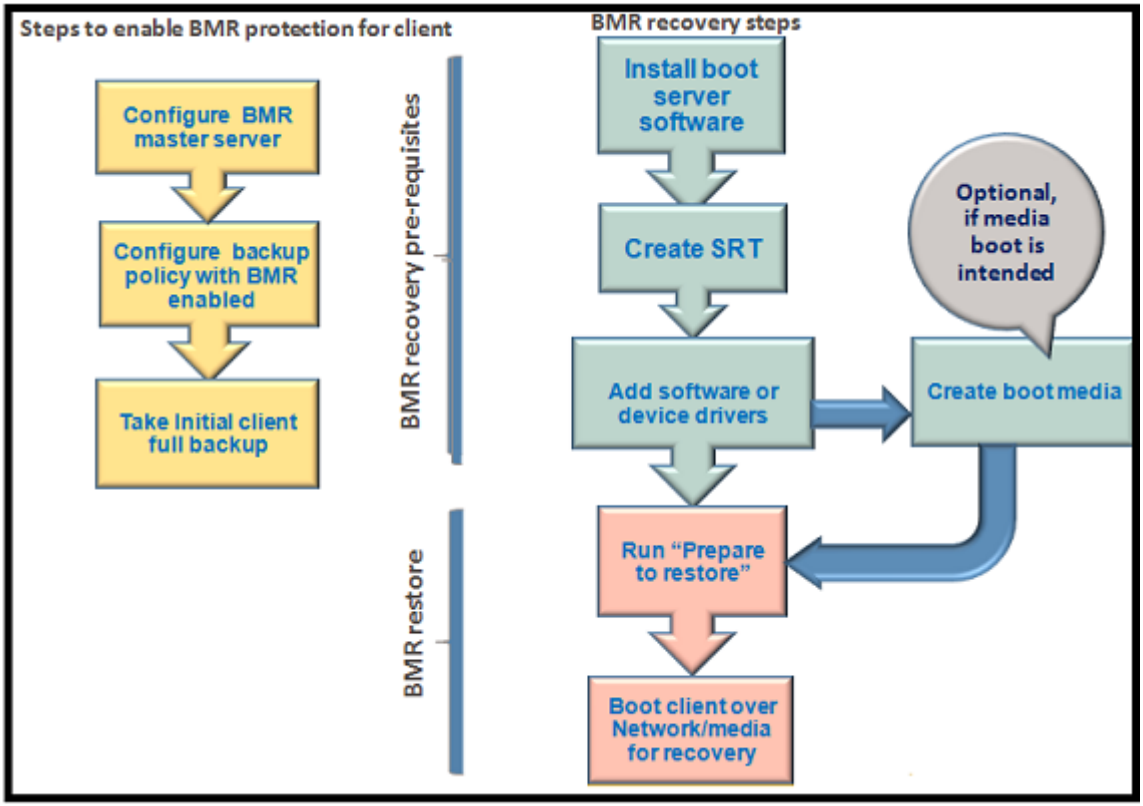
- Client Recovery

  This is the actual client recovery phase, where client computer boots into recovery environment. The client needs to be prepared for recovery by running single command line or single click. BMR supports two recovery methods: Network-based boot and Media-based boot. For details about client recovery process, refer chapter *Restoring clients*. BMR can also be leveraged in NetBackup's Auto Image Replication setup to recover primary domain host into DR Domain.

  For details See "BMR client recovery to other NetBackup Domain using Auto Image Replication" on page 256.

BMR protection phase diagram

Following diagram provides an overview of the BMR process from backup till restore.



For more illustration about downloading Microsoft ADK and creating SRT on an offline boot server, refer Create SRT on online and offline boot server diagram.See "Creating SRT on an offline boot server or host " on page 43.

UEFI-GPT support in BMR

Table 1-2 provides information about UEFI-GPT support in BMR for Linux and Windows operating system.

Table 1-2 Proliferation support for UEFI-GPT in BMR

Operating System	Proliferation Support
Red Hat Enterprise Linux 7.x, 8.x	NetBackup BMR supports the GUID Partition Table (GPT) disk types and the Dissimilar Disk Restore (DDR) functionality similar to the BIOS clients. The supported BMR features on UEFI machine are Self-restore, DDR, and Dissimilar System Recovery (DSR). Dissimilar System Restore support is extended to UEFI clients. For details refer the tech note. https://support.cohesity.com/s/article/article-000034868 The newly created Shared Resource Tree can be used to boot BIOS as well as UEFI machines. In addition the VFAT file system is also supported. **Note:** The support for Linux multi-devices is limited and BMR may not restore the exactly some configurations.
Windows	■ For UEFI, and Legacy BIOS booted machines, NetBackup BMR supports self-restore, Dissimilar Disk Restore (DDR), and Dissimilar System Recovery (DSR) for both Legacy MBR and GUID Partition Table (GPT) disk types. ■ For UEFI systems and BIOS system having GPT disks, NetBackup BMR doesn't support Direct virtual machine (VM) creation (Physical to Virtual). The newly created Shared Resource Tree can be used to boot BIOS as well as UEFI machines. In addition the FAT32 file system is also supported.

Chapter 2

Configuring BMR

This chapter includes the following topics:

About installing BMR software

Bare Metal Restore includes the following software components:

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

Subsequent sections contain instructions for installing BMR.

Prerequisites for Configuring BMR Servers

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

Configuring BMR Servers

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

- See "Configuring BMR Master Server" on page 17.
- See "Configuring BMR Boot Server" on page 18.

Configuring BMR Master Server

After installing NetBackup, setup the BMR master server and create the BMR database.

Bare Metal Restore master server gets installed with NetBackup master server. After the installation you have to configure the Bare Metal Restore master server.

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

In a cluster environment, configure BMR master server on the active node only.

To create the BMR database and setup the BMR master server

1. Log on as the root user on the system on which the NetBackup master server is installed.
2. Run the following command to configure the BMR database:

   ```
   %NB_INSTALL_DIR%/bin/bmrsetupmaster
   ```

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

Note: You need to restart NetBackup services, after you run the `bmrsetupmaster` command on the master server.

Setting up the BMR master server on a Windows system

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

To set up the BMR master server on a Windows system

1. On the Windows BMR master server, select **Programs > Cohesity NetBackup > Bare Metal Restore -- Master Server Setup** from the **Start** menu.
2. Follow the prompts to set up the BMR master server.

   You do not have to enter any information; the wizard performs all the steps required to set up the master server.
3. If you want to set up BMR in a cluster environment, unfreeze the active node after you complete this process.

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

   See the clustering section in the NetBackup in Highly Available Environments Administrator's Guide.

Configuring BMR Boot Server

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

Every NetBackup server includes the NetBackup client software by default. Therefore, you can run a BMR boot server on either a NetBackup server or a client (if BMR supports that platform). Boot servers provide the environment that is required to rebuild a protected client, including resources such as shared resource trees (SRT).

Note: The BMR master server needs to be configured on the NetBackup primary server before the BMR boot server is configured.

About choosing boot server hosts

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

See “Boot server requirements” on page 187.

Prerequisites for boot servers

If network-based BMR recovery is intended then few network services need to be configured on BMR boot server. These configuration settings vary for various platforms.

See “Network services configurations on BMR boot Server” on page 244. for more details.

Setting up a BMR boot server

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

Note: Before you configure a BMR Boot server on a NetBackup host, make sure that the NetBackup host is configured with the NetBackup primary server. Refer to the NetBackup Administrator's Guide for registering the NetBackup client with the NetBackup primary server.

To register a BMR boot server

1. Navigate to the directory where NetBackup is installed.

   UNIX: `/usr/openv/netbackup/bin`

   Windows: `c:\program files\veritas\netbackup\bin`

2. Run the following command on the boot server host:

   ```
   bmrsetupboot -register
   ```

After you run the command, you can see the boot server name in the NetBackup web UI: **Bare Metal Restore > Hosts > Boot Servers**. This command starts the BMR Boot server daemon running.

BMR boot servers in a UNIX cluster

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

- In the clustering application, set up a virtual IP address on the nodes that provide the BMR boot server functionality.
- Install the NetBackup client software on each node. You can register the Bare Metal Restore boot server on each node that has NetBackup client installed. See the NetBackup Installation Guide. The NetBackup client software includes the BMR boot server software (if BMR supports the platform).
- On each node, configure the NetBackup client name to be the name that resolves to the virtual IP address. Use that name for the last `CLIENT_NAME` entry in the `bp.conf` file on the system.
- Set up the boot server on active node.
  See "Setting up a BMR boot server" on page 19.
- Create a cluster application resource that calls the following start and stop scripts for the boot server daemon:

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

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

- When you create SRTs, choose a location on a file system on the shared disk.
- If a boot server fails over and restore tasks are not completed, perform a new prepare-to-restore operation for each incomplete restore task.

BMR boot servers in a Windows cluster

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

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

- In the clustering application, set up a virtual IP address on the nodes that provide the BMR boot server functionality.
- Install the NetBackup client software on each node.
- On each node, do the following:
  - Configure the NetBackup client name to be the name that resolves to the virtual IP address.
  - Start the Backup, Archive, and Restore interface.
  - Enter the NetBackup client name as the client name in the **Specify NetBackup Machines and Policy Type** dialog box.
  - Make the NetBackup client name the current client.
- Install the BMR boot server software on each node. Switch the virtual address to each node before you install the boot server software.
- Create a cluster application resource that calls the start and stop script for the boot server services:

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

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

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

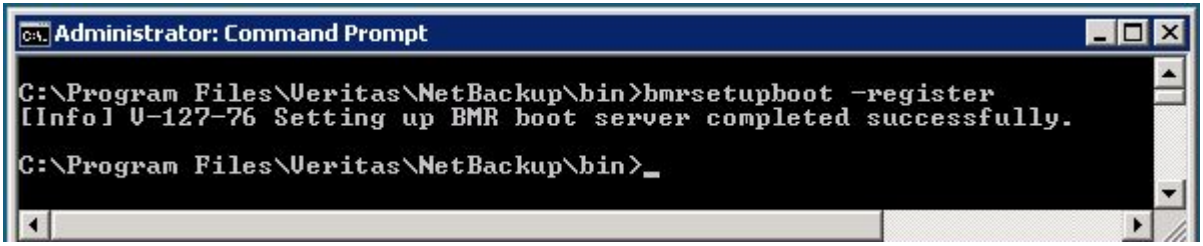
To register a BMR boot server on a Windows system

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

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

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

   The following screen shot shows the registration of **BMR Boot Server**.



Deactivating BMR servers

You do not uninstall BMR components. Rather, you deactivate them. NetBackup BMR master server is bundled with NetBackup master server and BMR boot server is installed with NetBackup client. If you uninstall NetBackup master server and client, BMR master server and boot server are removed from the system. Refer NetBackup Administrator's Guide for information about uninstalling NetBackup.

Deactivating BMR master server

Use the following procedure to de-activate BMR master server and BMR database and delete the BMR license.

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

To deactivate the BMR master server

1. Log on as the root user on the system on which the NetBackup master server is installed.
2. To de-activate BMR Master server, execute the following command:

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

   for example, on a UNIX/Linux system, run

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

   and on Windows master, run

   ```
   c:\program files\veritas\netbackup\bin\bmrsetupmaster -undo -f
   ```

Deactivating BMR boot server

Deactivate a BMR boot server by using the following procedure.

To deactivate a BMR boot server

1. Log on as the root user to the BMR boot server host.
2. Run the following command on BMR boot server to de-register it.

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

   For example on Windows, run

   ```
   c:\program files\veritas\netbackup\bin\bmrsetupboot -deregister
   ```

   On UNIX/Linux run

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

On successful execution of the command, the boot server instance is not visible in NetBackup web UI: **NetBackup web UI > Bare Metal Restore > Hosts > Boot servers**. De-registering command stops the BMR Boot server daemon running.

Note: BMR Boot server deactivation does not remove SRTs hosted by the BMR Boot server. The SRTs will exist in case they need to be imported by another BMR Boot server or the same Boot server if enabled again in the future. On de-registering BMR boot server on windows, BMR PXE and TFTP services will be removed along with BMR boot server service.

Chapter 3

Protecting clients

This chapter includes the following topics:

Prerequisites for protecting clients

Before making configurations that are required to protect BMR clients, it is necessary to install BMR master server.

To know how to set up BMR master server, See “Configuring BMR Master Server” on page 17.

To collect BMR information during backup of client RHEL 8.4 on NetBackup version 9.1.0.1 or later, it is necessary to install net-tools package. After installing this package, it provides netstat and ifconfig commands.

If the net-tools package is not installed, then it gives an error receiving BMR information during the backup of client RHEL 8.4 on NetBackup version 9.1.0.1 or later. For more information, see https://support.cohesity.com/s/.

Backing up BMR clients

To perform client disaster recovery using BMR, the NetBackup backup policy needs to be configured for BMR. At least a full backup is required with BMR-enabled backup policy for the client to be recovered.

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

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

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

Configuring policies to back up BMR clients

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

The following are the requirements for protecting BMR clients:

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

Note: Enabling the attribute 'Collect disaster recovery information for BMR" automatically sets the "Collect true image restore information and with move detection" attribute.

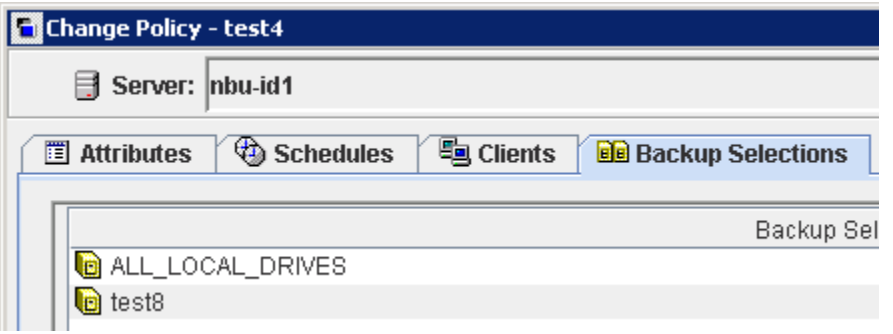
These attributes enable NetBackup to restore only those files present on the system at the time of the backup. Move detection enables NetBackup to restore the files correctly that were moved, renamed, or newly installed. These attributes also ensure that all of the restored files fit in the volumes and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

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

Note: Similar option to enable the BMR backup is also available under the **Policy management** tab, in the NetBackup web UI.

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

  If a client has database or application files to back up using a NetBackup database agent or other policy, you can use an exclude list to exclude them from the policy that specifies `ALL_LOCAL_DRIVES`. In case some files are excluded in the BMR policy, then post BMR recovery the excluded files need to be explicitly recovered.



Note: Even if All_Local_Drives is not selected, minimum OS volumes and in case of Windows system state is required.

- For clustered clients, the most effective backup strategy uses multiple policies. Each node should have its own policy that backs up local file systems. Shared file systems should be backed up by the additional policies that back up the node that currently owns the resources.
- In case of multiple policies configured for the same client for different backup selection, then scheduling all policies to run at the same time will help achieve consistency post recovery.
- NetBackup media servers can be protected as BMR clients. Media servers that back up to their own storage devices (either SCSI-attached or SAN-attached) require special procedures for restores. If you understand these procedures, you can configure NetBackup to minimize the time and effort that the restores require.

  See "About restoring NetBackup media servers" on page 132.

For information about configuring backup policies, see the NetBackup Administrator's Guides.

Using the same client name in multiple policies

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

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

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

About performing complete backups

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

About performing a full backup after a restore

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

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

Ensuring successful backups

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

Table 3-1 Steps to ensuring successful backups

Step	Action	Reference
Step 1	For UNIX clients, configure NetBackup to retry file backups if a file changes during the backup attempt. More information is available on busy file properties.	See the NetBackup Administrator's Guide Volume I.

Table 3-1 Steps to ensuring successful backups *(continued)*

Step	Action	Reference
Step 2	For Windows clients, configure NetBackup to use a **Windows Open File Backup** option. More information is available on **Windows Open File Backup** properties.	See the NetBackup Administrator's Guide Volume I .
Step 3	Examine the NetBackup log files regularly to ensure that any backup errors are corrected promptly. During backup, network or server errors can occur that affect the backup.	

Saving custom files on UNIX or Linux

The following information applies only to UNIX and Linux clients.

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

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

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

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

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

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

See "Enabling or disabling SRT exclusive use" on page 74.

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

Monitoring client backups

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

See "Monitoring backup jobs" on page 238.

BMR related other NetBackup properties

Below mentioned properties are set by default, however, you may need to configure or tune these if required.

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

  The following settings are your options:

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

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

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

Protecting clients with specific use cases

Storage Foundation for Windows Clients

BMR can restore a Storage Foundation for Windows (SFW) Clients both using Legacy Restore method as well as Fast Restore (non-SFW volumes recovery) method. However currently FAST Restore method can ONLY support restoring non-SFW disks ONLY which are not managed by SFW volume manager. The backup configurations required to restore using Legacy Restore method is different than the one used for Fast Restore method.

Bare Metal recovery using Fast Restore:

When using BMR to backup and restore (SFW) using Fast Restore method, you need to perform few additional steps before attempting a backup.

Note: It is advisable to keep the system disk under the control of Windows Disk Manager and not SFW. This way you can recover the system using BMR fast recovery method and then later get back the SFW volumes.

To perform bare metal recovery using fast restore,

1. Configure a DWORD - registry key "BMR_USE_WINDOWS_VOL_MGR" under `HKLM\SOFTWARE\Veritas\NetBackup\BareMetal` with value set as "1" on the SFW client which is to be protected. This is important step and hence validate that the key is set correctly.
2. Perform the BMR backup of the SFW client.
3. Verify that all disks except the system disk are marked as "Restricted" by BMR in the "current" configuration. If you see that the SFW disks are not marked as 'Restricted' then there may be a problem in setting the registry key. BMR does not restore the disks that are marked restricted and they are maintained as it is.

Note: BMR does not restore the disks that are marked as 'Restricted" and these disks are maintained as is.

Chapter 4

Setting up restore environments

This chapter includes the following topics:

Recovery steps

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

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

Table 4-1 Process for setting up restore environment

Step	Action	Related topic
Step 1	Install boot server software	See "Installing boot server software" on page 31.
Step 2	Create shared resource trees	See "Shared resource trees" on page 31.

Table 4-1 Process for setting up restore environment *(continued)*

Step	Action	Related topic
Step 3	Add client specific resources	See "Adding client-specific resources" on page 32.
Step 4	Create boot media	See "When to use boot media" on page 32.
Step 5	Preparing client to restore	See "Preparing client for restoration" on page 33.

Installing boot server software

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

A NetBackup client that is not be registered as a boot server to the BMR master server, or a boot server that is unable to communicate with the BMR master server is considered a **master-less boot server**. Out of all the SRT-related operations, only create SRT, export SRT, and delete SRT operations are allowed in case of master-less boot server, as BMR SRT operations require Microsoft's ADK to be available. User can install ADK on a master-less boot server, create an SRT, and export it. This SRT can be imported on any other registered boot server thereby eliminating the need of ADK installation on those boot servers

Shared resource trees

A shared resource tree (SRT) is system recovery critical software which is a collection of the following:

- Operating system files
- NetBackup client software
- Optionally other software like device drivers, Volume manger, File system managing software which are necessary to rebuild the original system.

More information is available about SRTs and procedures to create and manage SRTs. See chapter *Managing Shared Resource Trees.*

Adding client-specific resources

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

Examples of such resources are as follows:

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

In case of Windows, you can add any restoration required device drivers into the BMR packages pool so they are available to add to the restore configuration.

More information is available about how to add packages to the packages pool and adding software to Windows SRT. For this, refer to the chapter *Managing Windows drivers packages*.

See "Adding software to a Windows SRT" on page 71.

In case of UNIX systems, you can add any required software or device driver using BMR-SRT administration utility.

See "Adding software to a UNIX or Linux SRT" on page 67..

See "About clients and configurations" on page 154.

When to use boot media

The BMR restore process begins by booting the client (using the network boot) from a BMR boot server or from BMR prepared boot media (CD, DVD, or floppy). If you use a network boot to begin the restore, boot media is not required.

If you have minimal network connectivity or have any restriction of not deploying network-based recovery required services (viz. DHCP or TFTP) then Cohesity recommends using the boot media that contains a shared resource tree

---

Note: Once BMR Media SRT is created, BMR bootserver is not required during the recovery.

More information is available about boot media and procedures for creating boot media. Refer chapter *Managing boot media* for details.

See "Managing boot media" on page 77.

Preparing client for restoration

Once a suitable SRT for client recovery is ready, a step “prepare to restore” is to be triggered from NetBackup primary server. This step digests client configuration to be recovered, verifies the resources, and tunes the recovery environment for that client restore.

More information is available on this subject, refer Chapter *Restoring Clients*.

Chapter 5

Shared resource trees

This chapter includes the following topics:

About shared resource trees

A shared resource tree (SRT) is BMR system recovery critical software which is a collection of the following:

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

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

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

Note the following:

- For UNIX and Linux systems: Each client type and operating system version requires its own SRT. For example, Solaris 11 requires a Solaris 11 SRT, AIX 7.1 TL3 requires an AIX 7.1 TL3 SRT, and so on.

- For Windows systems: A single SRT can restore all Windows versions of the same architecture.

For UNIX and Linux systems, you create SRTs on boot servers of the same operating system. The boot server must run the same version or a later version of the operating system that is installed in the SRT. For example, a Solaris 11 SRT must reside on a Solaris 11 or later boot server. For Windows systems, any version of Windows can host the SRT.

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

During a restore, a client accesses the SRT from a boot server over a network, or on a CD or DVD. Although SRTs reside on boot servers, you can copy an SRT to CD media or DVD media, boot the client from that media, then access the SRT on that media. If you are using a BMR Media, you do not require the boot server during recovery.

Depending on the operating system for which an SRT is created, the SRT size requirement can vary from 100 MB to 1 GB of disk space.

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

Pre-requisites for Shared Resource Tree

Following sections describes about the pre-requisites of shared resource trees.

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.

Note: You cannot create Legacy SRTs on a BMR boot server.

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

- Operating system (UNIX and Linux only).

- For Linux SRTs, the Bare Metal Restore third-party products CD. This CD contains the open source products that may not be included in the vendor Linux distribution.

  Note: Cohesity updates the third-party components in 3PPCD to their respective recent releases from time to time. Veritas always recommends using the latest possible version of 3PPCD while creating new SRTs. A Boot Server of NetBackup version 8.3 or later requires version 3.0 of BMR 3PPCD. For NetBackup versions earlier than 8.3, Veritas recommends using version 2.0 of 3PPCD as you are not allowed to use newer version 3.0 of 3PPCD. Similarly, for Boot Servers with NetBackup versions earlier than 8.0, only version 1.0 of 3PPCD could be used. Also, a user is allowed to continue using the existing SRTs created with older versions of 3PPCD. During first time SRT creation BMR keeps the contents of 3PPCD at location /usr/openv/netbackup/baremetal/server/data/media/3PPCD/ when we the user provides the 3PPCD. For subsequent SRT creation we use the contents from this location. If this location is empty due to some reason, bmrsrtadm asks for 3PPCD during SRT creation. After upgrading older boot servers to 8.3, during SRT creation BMR checks the OS version for which SRT is being created, BMR verifies this location contents and cleans the area and asks for version 3.0 of 3PPCD.

  https://support.cohesity.com/s/

- Optional: Other applications or packages (such as Arctera Volume Manager or Arctera File System).
- Optional: Patches, maintenance levels, Maintenance Packs, service packs, fileset, or the drivers that the operating system requires or other software that is installed in the SRT. You must install into the SRT any operating system patches that the NetBackup client software requires. If they are not installed, NetBackup does not function correctly in the temporary restore environment, and the restore may fail.

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

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

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

- Place the installation program in a removable media drive of the boot server. Then provide the path to that removable media drive.
- Copy the contents of the installation program to a local directory. Then provide the path to that local directory.
- Copy the installation program contents to a remote directory, available to the boot server through NFS or network share. Then provide the path to that remote directory or share location.

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

See "Creating an SRT for UNIX or Linux" on page 51.

See "Creating an SRT for Windows" on page 37.

Creating an SRT for Windows

BMR Windows recovery is supported by fast restore method by which Windows SRTs no longer require the user to supply a version of Windows. The SRTs use a pre-installed Windows physical environment on the boot server. For creating the physical environment, Microsoft ADK is required to be installed on the boot server. For information about steps to create SRT, See "Create an SRT" on page 38.

Shared Resource Tree Administration Wizard

This wizard applies only to Windows systems.

Use the Shared Resource Tree Wizard to do the following:

- Create an SRT
- Edit an SRT
- Export an SRT
- Import an SRT
- Copy an SRT
- Delete an SRT
- Create a bootable CD or DVD image
- Add or update packages to SRT
  - Add the NetBackup client software to an SRT
  - Add NetBackup Release Update or Maintenance Pack to an SRT
  - Add NetBackup Language pack

Create an SRT

BMR SRT provides the resources that are needed to boot the client system and begin the restore process. BMR Windows SRT uses Windows Pre-Installation Environment (WinPE) as base recovery environment. In order to create this base WinPE recovery environment, you need to install Microsoft Assessment and Deployment Kit (ADK) version 10 on the host. Microsoft ADK installation is essential while creating new SRT for the first time. There are different options available to setup ADK on BMR boot server host as explained below:

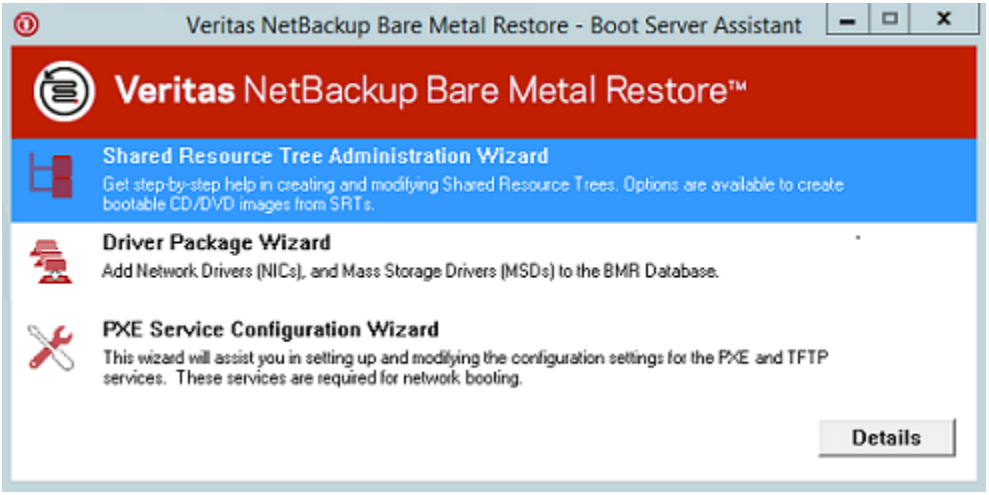
- BMR Shared Resource Tree administration wizard can install it using:
  - Automatic download of ADK and installation
  - Use remotely downloaded ADK installer for creating the SRT
- Manual ADK setup using FULL ADK 10 installable ADK 10 is downloadable (ADKsetup.exe) and can be installed from Microsoft's website https://go.microsoft.com/fwlink/p/?LinkId=526740 directly or an offline installation can be done by downloading entire ADK installer package from the Microsoft's web site.

The approximate size of the ADK setup program is 3GB.

To create an SRT for Windows

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

The Bare Metal Restore Boot Server Assistant appears.

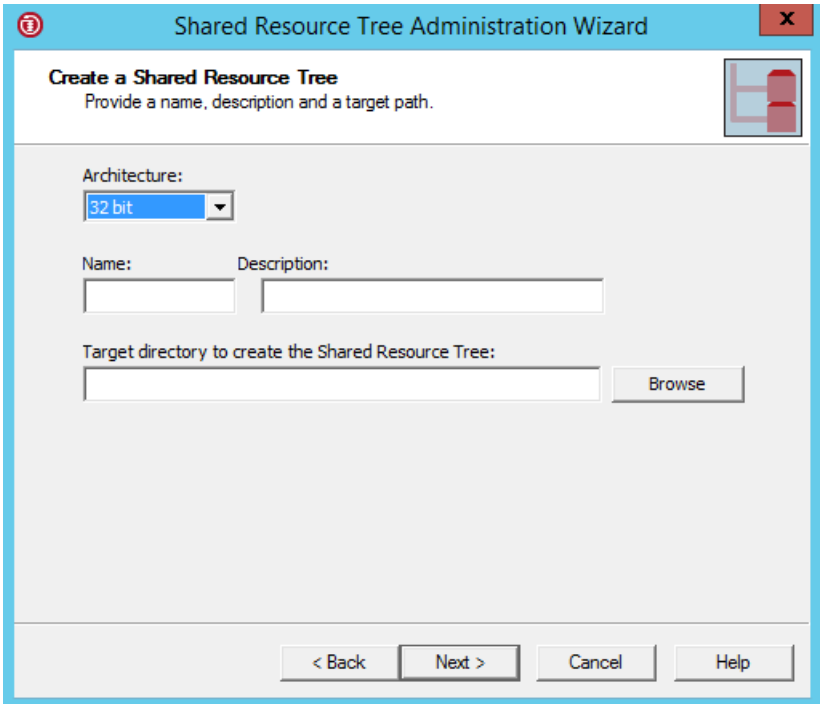


2 Click **Shared Resource Tree Administration Wizard**.

The Shared Resource Tree Administration Wizard appears.

3 Select the type of Shared resource tree as Fast Restore SRT.

4 Follow the prompts to create a shared resource tree. You must provide the following information:



Architecture	Select the architecture from drop-down options.
Name	The name of the SRT is also used for the directory that contains it. Only alphanumeric characters and the underscore (_) character are allowed.
Description	Enter the description of the SRT.
Target Directory	Enter the path or browse the location of target of SRT.

Installing Microsoft Assessment and Deployment Kit (ADK)

NetBackup Bare Metal Restore requires customized Windows Pre-Installation Environment (WinPE) for recovery of clients protected by NetBackup. Installation of Microsoft ADK is essential for creating the customized physical environment for SRT creation.

For installing the Microsoft ADK, following two options are available:

- Automatic downloading and installing the ADK option
- Using the already downloaded ADK on the remote site to install it on the current host

Installing ADK using automatic download and install option

This option downloads and installs Microsoft ADK automatically fromMicrosoft website.

Perform the following steps:

1. Choose the option **Automatically Download and Install** and click **Next**.

   This will initiate the download and installation of ADK automatically. You can observe the process progress the wizard.
2. Specify the path for installation and click **Next**.
3. Customer Experience Improvement Program (CEIP) is optional. Respond and click **Next**.
4. Accept the License Agreement in order to continue.
5. Do not dis-select the pre-selected features for deployment tools and Windows Preinstallation Environment to create the base recovery environment for BMR. These features are essential. Click **Install**.

   The progress bar confirms that Windows ADK installation is complete.
6. Click **Close**.
7. Shared Resource Tree Administration Wizard progress bar will continue with customizing the Recovery Disk Image.

Progress of ADK download and install process

If you select the option for downloading and installing the ADK automatically, BMR performs a pre-check for the install process to begin. This is required in order to check the pre-configuration compliance for developing the physical environment for creating the SRT.

After starting the automatic download and install of ADK, you can observe the progress details and the pre-configuration checks running on the wizard. The stages are:

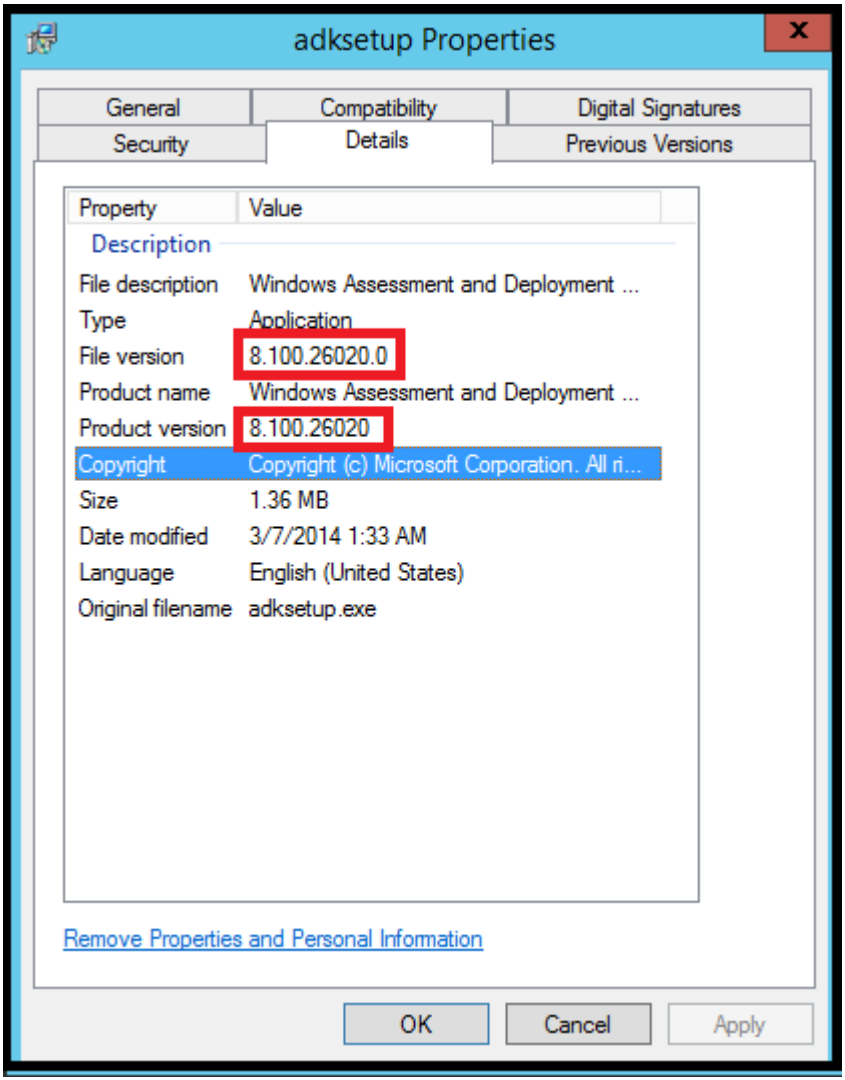
- Downloading and install of ADK
- Creating NetBackup BMR Windows recovery environment
- Cusomizing Symanted recovery disk image

Wait till all the prechecks are completed and then click **Next**.

Using pre-downloaded ADK executable file

In order to use a pre-dowloaded ADK executable file, the file must be downloaded on the host with internet connectivity. Refer Technote21353 for getting stepwise instruction for how to download ADK.

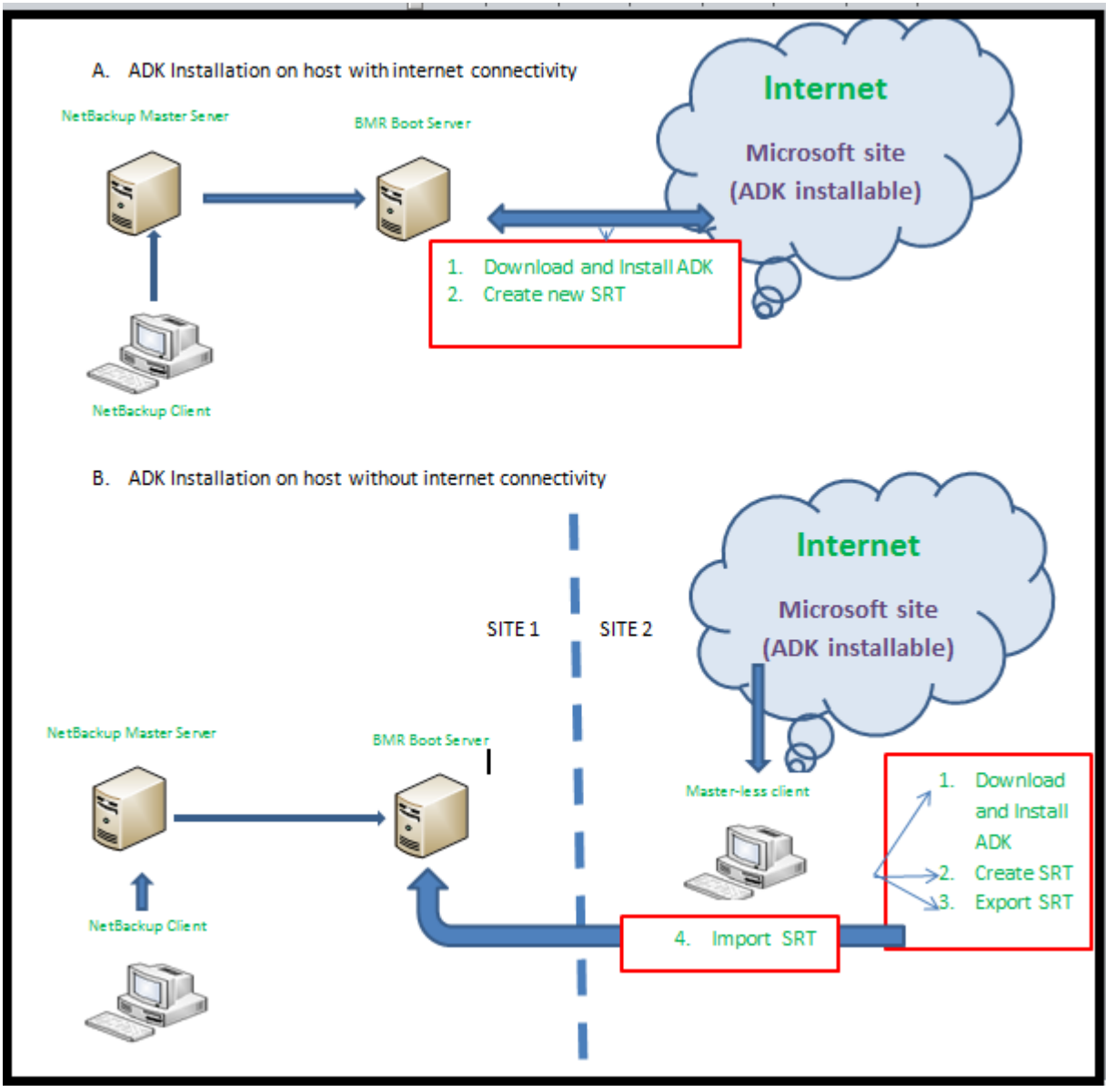
Download **ADKsetup.exe** which is required for installing the Windows ADK from http://www.microsoft.com. The Windows ADK setup program is downloaded directly from the internet by using either the graphical user interface (GUI) or the command-line. Make sure that the BMR boot server remains connected to the internet while ADK setup is running. The ADK setup downloads installation packages from the internet. The time required to complete the ADK setup varies depending on the bandwidth of the internet connection, the performance of the computer, and the Windows ADK features that you select to install.



Creating SRT on an offline boot server or host

A NetBackup client that is not be registered as a boot server to the BMR master server, or a boot server that is unable to communicate with the BMR master server is considered as a master-less or offline boot server. Create, export and delete SRT operations are only allowed in case of master-less boot server, as BMR SRT operations require Microsoft's ADK to be available. In case of unavailability of internet connection on host or boot server, you can install ADK on a temporary boot server, which can be master-less, create a new SRT and export it to the host. This

SRT can be imported on any other registered boot server thereby eliminating the need of ADK installation on those boot servers without internet connectivity. Refer section Importing the SRT autimatically.



SRT automatic import

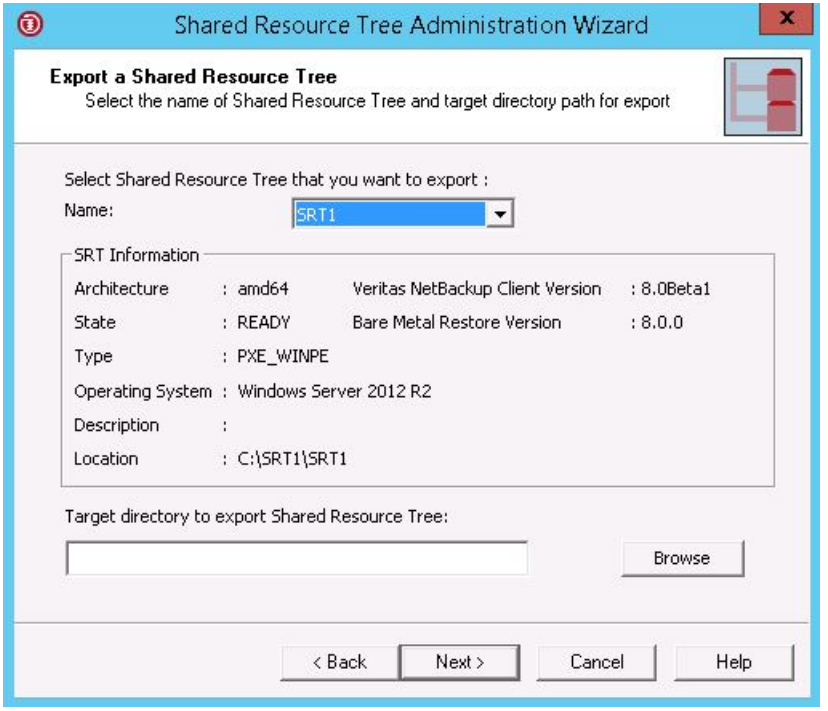
This operation enables auto-import of the Shared Resource Trees created on any client that was not registered as boot server to BMR master server or boot server with no connectivity with master server. Once the boot server is registered or connected back to master server, as we select Shared Resource Tree Administration option from Boot Server Assistant wizard, all the previously created SRT entries will be automatically inserted into BMR master server database. These SRTs are then available for recovery operation.

Note: The duplicate SRTs (SRT created on master-less boot server whose name already exists on master server's database) will not get auto-imported.

Export SRT

This option enables you to export any SRT which is in ready state. Exporting an SRT creates a compressed file of 1 GB size containing ADK executable, SRD files (for both x86 and amd64) and SRT. wim file. This compressed file can be imported at any other boot server.

Note: To be able to export an SRT, a minimum of 1.4 GB additional space is needed on C:\ drive as it acts as a temporary storage till the export process is complete and the SRT is successfully exported to the target location.



Perform the following steps in order to export an SRT:

1. Select an SRT to export.
2. Enter a path to or browse to select the location to create the new exported SRT cab.

Note: CD/ISO based SRTs export is not supported. Before exporting any SRT to network location, make sure that network location is already authenticated and accessible.

Edit an SRT

This panel lets you edit SRT parameters.

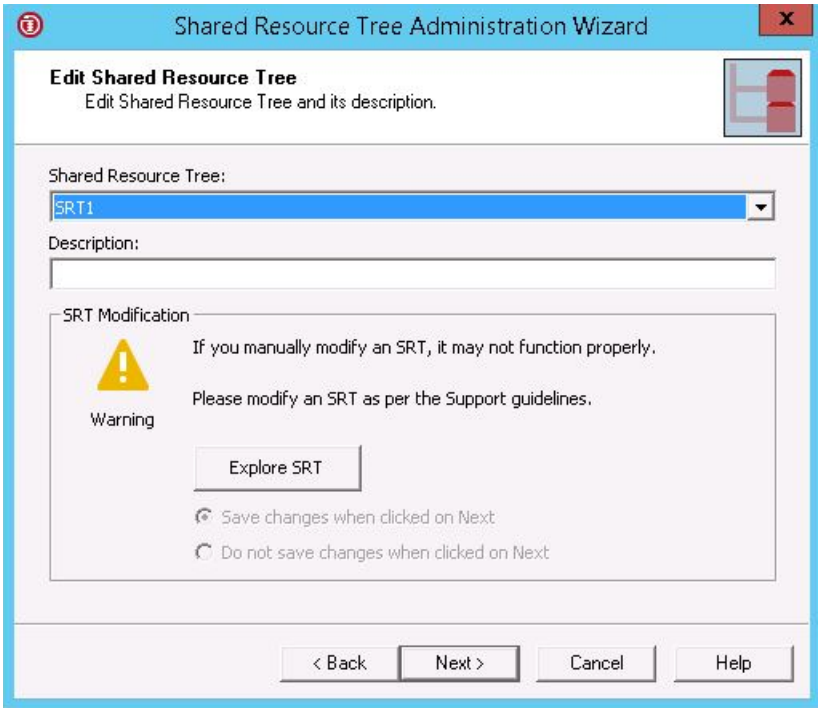
In certain scenarios, you may need to modify the SRT contents. For example, add a new binary to the SRT as part of applying a new release update to the existing BMR version. In such scenarios, you first need to mount the SRT and then modify its contents.

The **Explore SRT** option automatically mounts the selected SRT and shows it in a file explorer view where you can add any new binaries or even modify existing ones.

This option is particularly useful when user would like to apply any engineering binary within the SRT.

If you manually modify an SRT, it may not function properly. In this case, you need to follow the guidelines that Cohesity Support provides with the release update content.

Figure 5-1 Edit a Shared Resource Tree



Select the SRT to modify its parameters:

- Modify the SRT description.
- Modify the contents in the SRT by clicking **Explore SRT**.

After modifying the SRT, click either of the following:

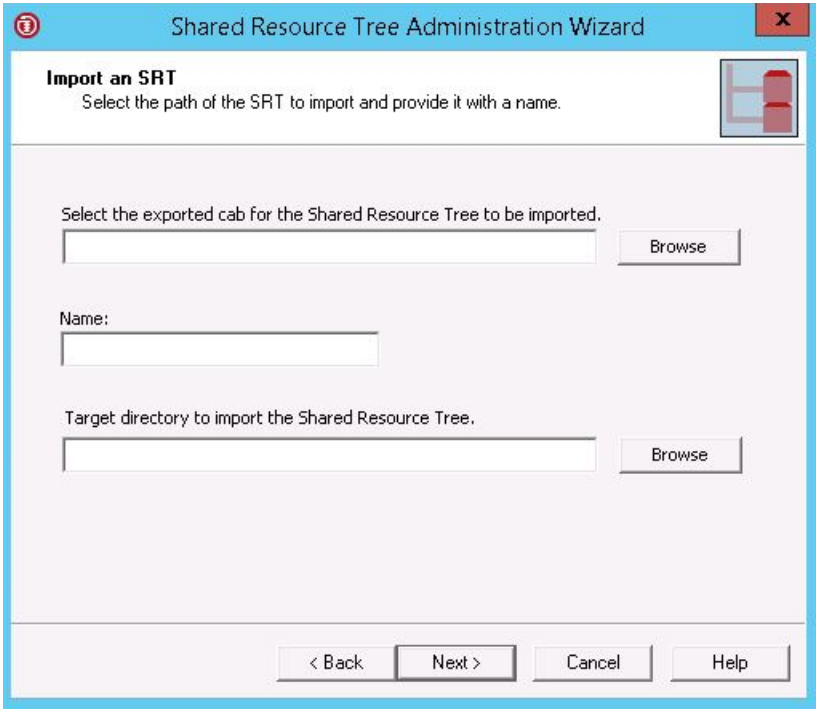
- Click **Save changes when clicked on Next**.
- Click **Do not save changes when clicked on Next**.
  If you select this option and click **Next**, the modifications to the SRT description or content is not saved.

Click **Next** to complete the SRT modification procedure.

Import an SRT

This option lets you import an existing SRT in a form of a compressed executable file. The SRT to be imported from another host should be first exported from the remote host. Refer section Exporting the SRT for the specific steps. After you export an SRT, while importing the SRT to a new location, following operations are observed on the boot server.

- Extract cab contents on the boot server at the specified path.
- Copy Mini-ADK (OSCDIMG.exe)
- Copy SRD files (both x86 and amd64).
- Copy SRT.wim file at specified path.
- Add entry of SRT in master database.
- Modify entry of SRT in local database.



Perform the below steps in order to import an SRT:

1. Select the directory on the boot server where the existing SRT is located, which you want to import.
2. Enter the name for the new SRT.
3. Enter a path to or browse to select the location to import the SRT.

Note: To be able to import an SRT, a minimum of 1.4 GB additional space is needed on C:\ drive as it acts as a temporary storage till the import process is complete and the SRT is successfully imported on the target location.

Copy an SRT

This option enables you to copy an existing SRT from one boot server to other. Copy operation is always preferred over re-creating a new SRT as it is faster.

Perform the below steps in order to copy an SRT:

- Select the SRT to copy.
- Enter a name for the new SRT. The SRT name should not contain more than eight alphanumeric characters.
- Enter a description for the new SRT.
- Enter a path to or browse to select the location to create the new the SRT.

Delete an SRT

Select the SRT to delete, then click **OK** in the confirmation dialog box.

Note: An SRT which is in the mounted state or opened for editing cannot be deleted.

Creating bootable CD or DVD image for Fast Restore SRT

The steps for creating bootable CD/DVD images from Fast Restore SRTs is as follows:

- Select the shared resource tree.
  See "Select an SRT" on page 50.
- Specify the location of ISO and client verification.
  See "Specify a location for the ISO image" on page 50.

The process ends with the **Copy Progress** panel and the **Completing the Shared Resource Tree** panel.

Select an SRT

Select the shared resource tree that you want to turn into a bootable CD or DVD image to be used for the restore.

Specify a location for the ISO image

You need to specify the location for the ISO image.

Enter the path or browse to select the directory in which the ISO image is to be stored. The wizard does not create a CD or a DVD; it creates an image that you must burn onto a CD or a DVD.

If any clients are listed on this page, they are automatically restored when booting this image.

Completing the Shared Resource Tree configuration panel

Click **Finish** to complete the SRT configuration.

Add or update packages to an SRT

Select the resource to add to the shared resource tree:

- Update the NetBackup client software image in an SRT.
  An SRT must contain a NetBackup client image that is the same version as the system or systems to be protected.
- Add Cohesity security services to an SRT.

Add NetBackup Client to an SRT

The steps to add NetBackup client software to the shared resource tree are as follows:

- Select the shared resource tree to which you want to add the client image.
- Enter the path name to the NetBackup client installation image (`NetBackup Client.msi`) or browse to select the image.

An SRT must contain a NetBackup client image that is the same version as the system(s) to be protected.

If the SRT already contains a NetBackup client image, it is replaced.

An SRT without a NetBackup client is in the **Locked** state. **Ready** state indicates a NetBackup client image is installed.

Add NetBackup Security Services to an SRT

A separate installation of NetBackup Security Services in SRT is not required. The security services get installed into an SRT as part of NetBackup client installation. For the SRTs containing an older version of NetBackup client, NetBackup security

service should be installed separately into SRT. If you use NetBackup Access Management to administer access to your NetBackup environment, install the NetBackup Security Services (VxSS) software for NetBackup client older version.

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

You would need to perform following steps to add NetBackup Security Services to an SRT:

- Select the shared resource tree to which you want to add the NetBackup Security Services image.
- Select the version of NetBackup security service.
- Enter the path to the setup file (in `.exe` format) or browse to select the image.

Add NetBackup Release Update or Maintenance Pack to an SRT

Steps for adding NetBackup Release Update or Maintenance Pack to the shared resource tree are as follows

1. Select the shared resource tree to which you want to add the client image.
2. Enter the path name to the NetBackup client installation image (Release Update.msi) or browse to select the image.

   An SRT must contain the base NetBackup client image for that particular version before you apply the relevant Release Update or Maintenance Pack.

   If the SRT already contains the NetBackup Release Update, the current file is replaced with the new one.

Add NetBackup Language Pack

Steps for adding NetBackup Language Pack software to the shared resource tree are as follows:

1. Select the shared resource tree to which you want to add the client image.
2. Enter the path name to the NetBackup Client installation image (Language Pack.msi) or browse to select the image.

   If the SRT already contains a NetBackup Language Pack, it is replaced.

Creating an SRT for UNIX or Linux

To create an SRT for UNIX or Linux OS client you need to use the `bmrsrtadm` command line.

To know the procedure of creating each client OS-specific SRT type, see the following:.

- See “ Creating an AIX SRT” on page 52.
- See “Creating an HP-UX SRT” on page 55.
- See “Creating a Solaris SRT” on page 58.
- See “Creating a Linux SRT” on page 62.

Creating an AIX SRT

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

- The operating system software
- NetBackup client software

To create an AIX SRT

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

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

2. Run the following command:

   ```
   ./bmrsrtadm
   ```

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

4 Complete the command prompts as indicated in following table.

`Enter the name of the SRT to create`	The name of the SRT that is also used for the directory that contains it. Only alphanumeric characters and underscore (_) characters are allowed.
`Enter the description of the new SRT`	A description of the SRT.
`Enter desired OS level of AIX`	Enter the levels you can create based on the operating system version of the boot server.
`Enter desired Architecture(32/64)`	Enter 64-bit AIX operating system. **Note:** During the NetBackup client installation into SRT step, `bmrsrtadm` gives the appropriate error message if there is any incompatibility between SRT OS architecture type and NetBackup client version.
`Enter the directory in which to place the new SRT`	The path to the directory in which to create the SRT. The root of the SRT (called the SRT path) is the path name to the SRT location, which includes the SRT name. The default is either /export/srt or the directory where an SRT was last created successfully. The directory must already exist.
`Source of AIX install images`	Enter the name of the device where the operating system installation program is inserted or enter the path to the installation image. After you enter the device name or host:/path, the operating system is installed into the SRT.
`Enter the source of the NetBackup install images.` `Specify a device name or an NFS path (host:/path form), or a local directory`	Enter the device name where the NetBackup client software installation program is inserted or enter the path to the installation image. After you enter the device name or path, the NetBackup client installation procedure installs the client software into the SRT.
`Do you want to continue? [y,n] (y)`	Enter **y**.

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

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

More information is available about how to add other software.

See "Adding software to a shared resource tree" on page 66.

Creating an HP-UX SRT

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

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

To create an HP-UX SRT

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

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

2. Enter the following command:

   ```
   ./bmrsrtadm
   ```

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

4 Complete the command prompts as indicated in following table.

`Enter the name of the SRT to create`	The name of the SRT also is used for the directory that contains it. Only alphanumeric characters and the underscore (_) character are allowed.
`Enter the description of the new SRT`	A description of the SRT.
`SRT OS level`	The levels you can create based on the operating system version of the boot server.
`Enter desired Architecture(32/64)`	Enter 64-bit HP-UX operating system. **Note:** During the NetBackup client installation into SRT step, `bmrsrtadm` gives the appropriate error message if there is any incompatibility between SRT OS architecture type and NetBackup client version.
`Enter the directory in which to place the new SRT`	The path to the directory in which to create the SRT. The root of the SRT (called the SRT path) is the path name to the SRT location, which includes the SRT name. The default is either /export/srt or the directory where an SRT was last created successfully. The directory must exist.

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

`The following patches are required for this SRT: patch_list`
`These patches can be found on an HPE support plus media, or they can be downloaded from the HPE web site.`
`Location (device or path) of the media that contains patch_list:`
	If your version of Ignite requires a patch, you are prompted to provide the path to the specific patch that the version requires.
	Note: To create SRT for HP-UX 11.11 PARISC, a new patch **PHCO_36006** is required. This patch is available in HP-UX 11.11 'Dec_2009_11i_GoldPack' patch bundle. You need to download this patch bundle and then install the patch PHCO_36006 by providing the location of Dec_2009_11i_GoldPack.

`Location (device or path) of the Veritas NetBackup install media`	Enter the name of the device where the NetBackup client software installation media is inserted or enter the path to the installation image. After you enter the device name or path, the NetBackup client installation procedure installs the client software into the SRT.
`Do you want to continue? [y,n] (y) y`	Enter `y`.
`Do you want to install the NetBackup client software for this client? [y,n] (y)`	Enter `y`.
`Enter the name of the NetBackup server:`	Enter any non-blank value. The server name is replaced at restore time with the correct values for the BMR client being restored.
`Would you like to use` *`servername`* `as the configured name of the NetBackup client? [y,n] (y)`	Accept the default or enter any nonblank value. The client name is replaced at restore time with the correct values for the BMR client being restored.

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

More information is available about how to add other software.

See "Adding software to a shared resource tree" on page 66.

Creating a Solaris SRT

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

- Operating system software
- NetBackup Client software

You may want to consult the following additional information:

- See "About installing patches and packages into Solaris SRTs" on page 70.

To create a Solaris SRT

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

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

2. Enter the following command:

   ```
   ./bmrsrtadm
   ```

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

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

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

Note: SRT creation requires developer studio 12.6 runtime patches in SRT. The patches can be downloaded from https://www.oracle.com

Enter the local diretory path containing the patches extracted from OracleDeveloperStudio12.6-solaris-<platform>-pkg.tar.bz2:

Make sure that the ISO path is provided when prompted and not the mounted location.

Follow the instructions mentioned in the article to the extract patch file (with tar.bz2 extension).

Provide the following path:

/<extractedPatchDir>/OracleDeveloperStudio12.6-solaris-<platform>-pkg/patches/system folder

After you enter the device name or path, the operating system is installed into the SRT.

`Enter a [hostname:]/pathname containing NetBackup client software`	Enter the name of the device in which the NetBackup software installation media is inserted or enter the path to the installation program (named `install`). After you enter the device name or path, the NetBackup installation procedure installs the client software into the SRT.
`Do you want to continue? [y,n] (y) y`	Enter `y`.
`Do you want to install the NetBackup client software for this client? [y,n] (y)`	Enter `y`.
`Enter the name of the NetBackup server:`	Enter any nonblank value. The server name is replaced at restore time with the correct values for the BMR client being restored.
`Would you like to use` *`servername`* `as the configured name of the NetBackup client? [y,n] (y)`	Accept the default or enter any nonblank value. The client name is replaced at restore time with the correct values for the BMR client being restored.

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

More information is available about how to add other software.

See "Adding software to a shared resource tree" on page 66.

Creating a Linux SRT

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

- The operating system software.
- BMR third-party products, the open source products that may not be included in the vendor Linux distribution. Cohesity updates the third-party components in 3PPCD to their respective recent releases. For more information, refer to the following tech-article
  https://support.cohesity.com/s/
- NetBackup client software.

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

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

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

The BMR third-party products CD is distributed as an ISO file system image. You can download the image and use it as the source image or write it to CD media.

To create a Linux SRT

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

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

2. Enter the following command:

   ```
   ./bmrsrtadm
   ```

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

4 Complete the command prompts as indicated in following table.

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

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

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

`The following media is required:`
`NetBackup x.x Client`
`Please load the media now.`
`Load media from:`
	Enter the name of the device in which the NetBackup client software installation media is inserted or enter the path to the installation image.
	After you enter the device name or path, the NetBackup client installation procedure installs the client software into the SRT.

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

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

More information is available about how to add other software.

See "Adding software to a shared resource tree" on page 66.

Managing shared resource trees

You can import, copy or delete the existing SRTs and can also add softwares into an SRT.

Adding software to a shared resource tree

Install additional software into an existing SRT only if it is required during a restore. Additional software may include an operating system patch or fileset that NetBackup client software requires. The software in an SRT is not installed on the restored system. It only brings the protected system to a state from which the original files can be restored. Therefore, you do not need to install the following: patches,

maintenance levels, maintenance packs, service packs, fileset, or drivers into an SRT that are in a protected system.

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

More information is available on the following tasks:

- See "Adding software to a UNIX or Linux SRT" on page 67.
- See "Adding software to a Windows SRT" on page 71.

Adding software to a UNIX or Linux SRT

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

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

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

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

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

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

To add software to a UNIX or Linux SRT

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

   /usr/openv/netbackup/bin

2. Enter the following command:

   ```
   ./bmrsrtadm
   ```

3. When you are prompted, select the option to modify an existing shared resource tree.

4 Enter the name of the SRT to modify.

5 Select intended installation option.

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

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

- See "About adding NetBackup Maintenance Packs" on page 68.
- See "About adding Arctera Volume Manager and Arctera File System" on page 68.
- See "About adding Veritas Security Services" on page 69.
- See "About adding other software" on page 69.

About adding NetBackup Maintenance Packs

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

When you select the install option of Cohesity Maintenance pack, you are prompted for the location of the installation program or image as follows::

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

Enter the full path to the location of the installation program or image.

About adding Arctera Volume Manager and Arctera File System

The following information does not apply to Linux systems.

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

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

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

software to the copies. To copy an existing SRT usually is faster than to create an SRT.

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

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

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

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

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

For more information about operating system dependencies for VxVM and VxFS, see OSCL matrix on https://support.cohesity.com/s/article/article-100040093

About adding Veritas Security Services

Bare Metal Restore version 11.2 does not require separate installation of Veritas Security Services in SRT. Veritas Security Services gets installed into SRT along with NetBackup client installation. For the SRTs containing an older version of NetBackup client, Veritas Security should be installed separately into SRT.

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

About adding other software

Use only the specific options to add software to an SRT.

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

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

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

See "About installing patches and packages into Solaris SRTs" on page 70.

See "Installing device drivers into Linux SRTs" on page 70.

About installing patches and packages into Solaris SRTs

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

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

Installing device drivers into Linux SRTs

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

To install device drivers into Linux SRTs

1. Select **Modify an existing SRT** option under the main menu and provide name of the SRT to be modified.
2. Choose the option **Install additional patches/drivers**.

   The following appears:

```
The following additional packages are available to install:
     1. Install/update kernel drivers.
     2. Install a Linux Update/Service Pack.
     3. None of the above, leave unchanged.

Enter your selection [3] :
```

   Select the appropriate option.

Choose option 1 to add additional Linux kernel drivers (.o, .ko) files into the SRT. This option can be used to add the drivers which are not present into the Linux installation media by default and need to be loaded during BMR restoration.

Adding software to a Windows SRT

You can install the following into an existing Windows SRT:

- NetBackup client software
- NetBackup Security Services

To add software to a Windows SRT

1. On the **Start** menu on the Windows BMR boot server that hosts the SRT, click **Programs > Cohesity NetBackup > Bare Metal Restore Boot Server Assistant**.
2. In the **Bare Metal Restore Boot Server Assistant**, click **Shared Resource Tree Administration Wizard**.
3. In the Shared Resource Tree Administration Wizard, click **Next** on the **Welcome** panel.
4. Select the option to update an SRT.
   - 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.
     See "Add NetBackup Client to an SRT " on page 50.
   - Add Cohesity Security Services to an SRT.
     See "Add NetBackup Security Services to an SRT" on page 50.
5. Follow the prompts to add software to the shared resource tree.

   The Shared Resource Tree Wizard help pages provide additional information.

Importing a shared resource tree

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

See "Importing an SRT on Windows" on page 72.

Importing an SRT on UNIX and Linux

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

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

To import an SRT on UNIX and Linux

1. Enter the following command:

   ```
   ./bmrsrtadm
   ```

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

Importing an SRT on Windows

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

Note: In NetBackup 7.6.1.2 and later versions, Windows Boot Servers do not support importing SRTs of versions 6.X , 6.5.X, and 7.6.

Starting Windows 7.6.1.2, Windows Boot Servers do not support import of old Legacy SRT.

Copying a shared resource tree

You can create a new SRT by copying another SRT.

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

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

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

See “Copying an SRT on UNIX and Linux” on page 72.

See “Copying an SRT on Windows” on page 73.

Copying an SRT on UNIX and Linux

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

To copy an SRT on UNIX and Linux

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

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

2. Enter the following command:

   ```
   ./bmrsrtadm
   ```

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

Copying an SRT on Windows

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

See “Copy an SRT ” on page 49.

Deleting a shared resource tree

You can delete an SRT by using the `bmrsrtadm` command (UNIX and Linux boot servers) or Shared Resource Tree Administration Wizard (Windows boot servers).

An SRT that is allocated to a restore task or being modified cannot be deleted.

Deleting an SRT on UNIX and Linux

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

To delete an SRT on UNIX and Linux

1. Change to the following directory on the boot server where the SRT resides:

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

2. Run the following command:

   ```
   ./bmrsrtadm
   ```

3. When you are prompted, select the option to delete an existing shared resource tree.
4. When you are prompted, type the name of the SRT and press **Enter**.
5. When you are asked if you want to delete the SRT, enter **y** to delete the SRT.

   If the SRT is locked, this operation fails.

   See "Breaking a stale shared resource tree lock" on page 76.

Deleting an SRT on Windows

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

See "Delete an SRT" on page 49.

Enabling or disabling SRT exclusive use

The following information applies only to UNIX and Linux clients.

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

Enable exclusive use before you do any of the following:

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

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

You may want to consult the following additional information:

See "Saving custom files on UNIX or Linux" on page 27.

To enable or disable SRT exclusive use

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

   `/opt/openv/netbackup/bin`

2. Enter the following command:

   `./bmrsrtadm`

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

Repairing a damaged shared resource tree

The following information applies only to UNIX and Linux boot servers.

If BMR places an SRT into a **DAMAGED** state, it may be possible to repair it to return it to a **READY** state. If an SRT is marked **DAMAGED** because a previous `bmrsrtadm` command is interrupted, recovery is likely. If you are unsure why an SRT was marked **DAMAGED**, delete it and create a new one from scratch.

SRT states appear in the **Bare Metal Restore > Resources > Shared resources trees** on the left of the NetBackup web UI.

To repair a damaged share resource tree

1. Change to the following directory on the boot server on which the SRT resides:

   `/usr/openv/netbackup/bin`

2. Run the following command:

   `./bmrsrtadm`

3. Enter the number of the option to modify an existing shared resource tree.

4. When you are asked for the name of an SRT, enter the name of the damaged SRT.
5. When you are asked if you want to continue, enter **y**.

   The `bmrsrtadm` program attempts to repair the SRT. The program guides you through installation of any missing SRT components.

   If repair is successful, the `bmrsrtadm` modify menu appears. When you quit the program, the SRT is in a **READY** state.

Breaking a stale shared resource tree lock

The following information applies only to UNIX and Linux boot servers.

An SRT in the `LOCKED_READ` or `LOCKED_WRITE` state is busy and most operations are not allowed. To manage a locked SRT, you should wait for the process using the SRT to finish and release the lock before you proceed. (The one exception is that you can allocate an SRT in a `LOCKED_READ` state to a restore task.)

In rare cases, an SRT may be left with a stale lock. For example, if a boot server crashes or is rebooted in the middle of an SRT operation, the SRT may be left locked. If you are sure that an SRT lock is stale, you can break the lock.

SRT states are displayed in the Bare Metal Restore > Resources > Shared resources tree view of the NetBackup web UI.

To break a stale SRT lock

1. Change to the following directory on the boot server on which the SRT resides:

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

2. Run the following command:

   ```
   ./bmrsrtadm
   ```

3. When you are asked for a select, provide the number of the option to modify the Shared Resource. The following appears:

   ```
   Enter the name of an existing SRT :
   ```

4 When you are asked for the name of an existing SRT, enter the name of the locked SRT and press **Enter**.

Warning: Do not attempt to break an SRT lock unless you are positive that the SRT is stale. If you break the lock of an SRT while it is in use, it may become corrupted.

5 When you are asked if you are sure that you want to break the lock, enter **y** to break the lock.

The stale lock is broken.

The `bmrsrtadm` command modify menu appears.

When you quit the program, the SRT is in a **READY** state.

Managing boot media

Boot media is used to boot a client and provide the shared resource tree or the resources to mount a shared resource tree. The boot media contains a small run-time environment that includes a kernel, a RAM file system, libraries, and programs. The client system firmware boots the kernel from the media. This boot media also contains a shared resource tree.

If you use media to boot the client system, you must use BMR to prepare the appropriate boot media. You can prepare boot media at any time before the restore. However, a prerequisite is that the shared resource tree for the protected system must exist.

Boot media is created from the resources that are stored in an SRT.

About the supported boot media on Windows

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

You can boot BMR clients only with the following options on Windows platform:

- Network boot
- CD/DVD Media boot

Note: Floppy-based restore is not supported on Windows platform because of the elimination of PC-DOS.

About writing a CD or DVD

The size of the media boot image that BMR produces depends on several factors. The structure of the installation program can change from one release to another and from one type of media (CD) to another (DVD). Therefore, sizes of the final images that are produced may be different under seemingly identical conditions.

The size of the media boot image that BMR produces depends on the following:

- The optional software packages on the SRT
- The operating system version
- The install media type used (where applicable) during media boot image creation.

In all cases, if the final media boot image that BMR produces fits on a CD, burn the image to a CD or a DVD. However, if the final image cannot fit on a CD, you must burn a DVD.

CD/DVD media must be bootable by the system for which you create it. To determine the correct way to create a bootable CD/DVD for the specific system, see the instructions that are provided with your CD/DVD writing software.

In addition, consider the following:

- The CD/DVD image that is created for AIX, Linux, and Solaris uses ISO-9660 format. HP-UX uses a binary format that is different from ISO.
- BMR does not contain CD/DVD writing software.

  Burn the CD/DVD image onto a disk using CD/DVD writing software that supports the following:

  - ISO-format images for AIX, Linux, and Solaris
  - Binary images for HP-UX

  The procedures for writing CDs/DVDs vary between applications; refer to the documentation for procedures.
- The CD/DVD writing software may require that ISO-format or binary CD/DVD image files end in a .iso extension. If necessary, you can add a .iso extension to the CD/DVD image before you write it.
- If the BMR boot server does not have CD/DVD writing hardware and software, transfer the CD/DVD image to a system that does. Ensure that the CD/DVD image file transmits as a binary file and transfers without errors; corrupted CD/DVD image files produce unpredictable results.
- For the CD/DVD media that includes an SRT, the name of the SRT appears as the content of the root directory on the CD/DVD.
- Label the CD/DVD for easy identification.

Include the following information.

- The client name (Windows clients)
- The NetBackup version that is used
- The operating system of the SRT that is installed
- Any extra software installed

- BMR does not use the CD/DVD image file after it is created. Therefore, you can move, rename, or delete the image file after you write the CD/DVD.

Creating boot media for UNIX and Linux

On UNIX and Linux systems, use the `bmrsrtadm` command to create a bootable CD/DVD image that contains an SRT. After you create the CD/DVD image, you must use CD/DVD writing software to burn the image onto a CD/DVD.

This process copies an existing SRT to the CD/DVD media; therefore, an SRT that supports the client must exist.

The following is the required information:

- The name of the SRT you want to use.
- The name to use for the SRT on the CD/DVD.
- The path to a directory that has enough free space to store the CD/DVD image.

To create boot media for UNIX and Linux

1. On Solaris systems only, use the following command to verify that the `vold` process is not running on the boot server where the SRT resides:

   ```
   # ps -ef | grep vold
   ```

   If it is running, do the following:

   - To eject any CD/DVD that may be loaded, run the following command

     ```
     # eject
     ```

   - To stop the `vold` process, run the following command

     ```
     # /etc/init.d/volmgt stop
     ```

2. On the boot server on which the SRT resides, change to the following directory:

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

3 Run the following command:

```
./bmrsrtadm
```

4 When you are prompted, select the option to create a new CD/DVD image-based shared resource tree.

5 Continue by referring to the information about the operating system.

See "About boot media for AIX" on page 80.

See "About boot media for HP-UX" on page 80.

See "About boot media for Linux" on page 81.

See "About boot media for Solaris" on page 81.

About boot media for AIX

You must have the AIX installation program that created the SRT that you want to use to create the boot media. (You must have it even if you created the SRT from a network copy of the media.) You must enter the device name that contains the installation program.

The directory for the CD/DVD image should not be a direct prefix of the directory that contains the SRT you intend to use.

For example, you can use the following for SRT `/export/srt/aix433esm`:

- Do not specify `/`, `/export`, or `/export/srt` for the location.
- You can specify `/export/srt/mb` because it is not a direct prefix of the SRT path.

About boot media for HP-UX

HP-UX uses a binary format that is different from ISO. The CD/DVD image file is a binary image of the CD/DVD and does not contain an extension. However, you can add an `.iso` extension to the CD/DVD image if your CD/DVD writing software requires it.

The CD/DVD recording programs that are known to work for HP-UX images are as follows:

- Sony CD/DVD Extreme - Add an `.iso` extension to the image file name and use the **Global Image** or **Other Image** option from the **File** menu options.
- Nero - Add an `.iso` extension to the image file name, and use the **Burn Image to Disk** option.

Note: The Roxio Easy CD/DVD Creator recording program does not work for HP-UX images.

About boot media for Linux

For Linux, the `bmrsrtadm` command creates a bootable ISO image file by using the name of the SRT with an `.iso` extension. Any standard CD/DVD writing software can be used to write media from this file.

About boot media for Solaris

You must have the Solaris installation media (Software 1 of 2) that created the SRT you copy to the CD/DVD. You must enter the device name that contains the installation media.

After you enter the information about the SRT, the following information appears:

- If Arctera Volume Manager (VxVM) is installed on the BMR boot server, the following appears:

  ```
  What do you want to use for temporary space?
  Select one of the following options:
      1. Use a disk group.
      2. Use a raw partition.
  Enter your selection (1-2) [1] :
  ```

  Enter `1` or `2`. Then enter the name of the disk group or the device file for the raw partition. If you use a raw partition for temporary storage, you are prompted to continue.

- If Arctera Volume Manager (VxVM) is not installed on the BMR boot server, the following appears:

  ```
  Enter the name of a partition of size 103040 or more blocks
  ```

  Enter the name of the device file for the raw partition. Then respond to the next prompt if you want to continue.

After the CD/DVD image is created, restart the `vold` process (`/etc/init.d/volmgt start`) if you stopped it before running the command `bmrsrtadm`.

Creating boot media for a Windows client

Windows systems may create a bootable ISO image which can be burned to either a CD or DVD.

To create boot media for a Windows client

1. On the Windows BMR boot server, select **Programs > Cohesity NetBackup > Bare Metal Restore Boot Server Assistant** from the Windows **Start** menu.

   The **Bare Metal Restore Boot Server Assistant** screen appears.

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

3. Select the option for **Create a Bootable CD/DVD** from a Shared Resource Tree.

4. Follow the prompts to create the boot media.

Chapter 6

Restoring clients

This chapter includes the following topics:

BMR restore process

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

Table 6-1 Restore types

Restore type	Procedures
To restore to the same client and use the most recent backup	See "About restoring BMR clients using network boot" on page 93. See "About restoring BMR clients using media boot" on page 106.
To restore to a specific point in time	See "About restoring to a specific point in time" on page 119.
To restore a client in which the disks are different	See "About restoring to dissimilar disks" on page 122.
To restore to a new target system (only on Windows systems)	See "Restoring to a dissimilar system" on page 127.
To restore a NetBackup media server	See "About restoring NetBackup media servers" on page 132.
To restore a BMR boot server	See "About restoring BMR boot servers" on page 135.
To customize the restore process	See "About external procedures" on page 137.

Other information is available.

See "Preparing a client for restore" on page 86.

See "BMR disk recovery behavior" on page 88.

See "About SAN (storage area network) support" on page 146.

See "Port usage during restores" on page 150.

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

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

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

Figure 6-1 shows a standard network restore.

Figure 6-1 Network restore

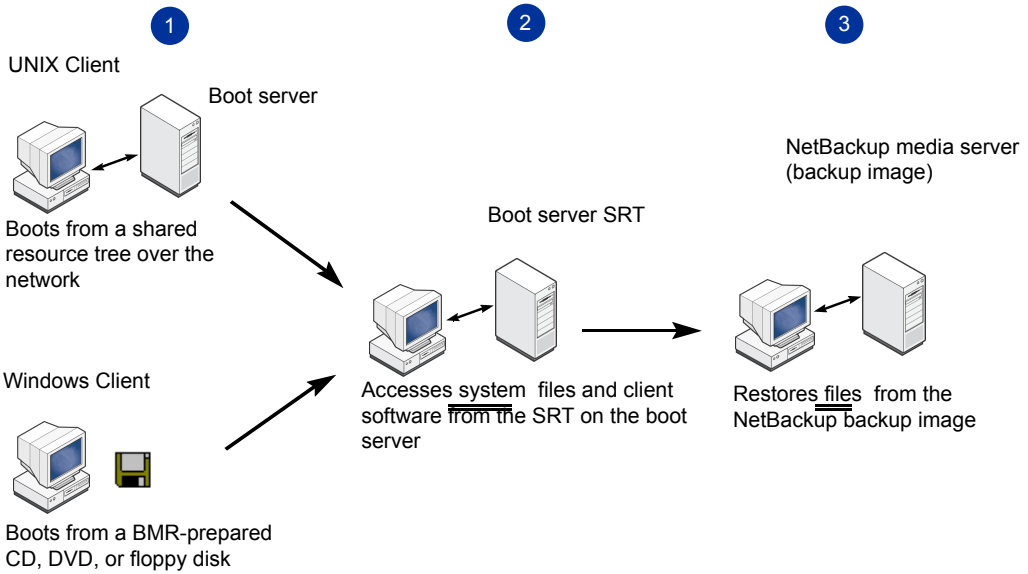
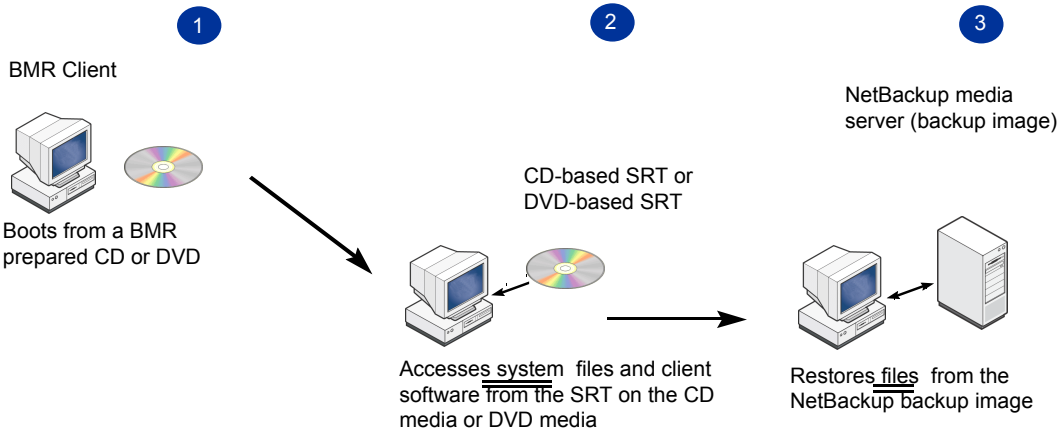


Figure 6-2 shows a media restore.

Figure 6-2 Media restore



Preparing a client for restore

Review the secure communication compatibility matrix for BMR for NetBackup 8.1.1 and later releases before you proceed with the prepare to restore operation.

See "Secure communication compatibility matrices for BMR for NetBackup 8.1.1 and later releases" on page 258.

Before you restore a client, you must prepare to restore (PTR) the client.

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

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

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

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

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

For more information on commands, refer to the *NetBackup Commands Reference Guide*.

To prepare a client for restore using the `bmrprep` command

1. Login as an administrator.
2. Run the `bpnbat` command.
3. Run the `bmrprep` command to initiate a prepare to restore operation.

   When you run the `bmrprep` command, validation checks are performed pertaining to the different parameters such as SRT version, configuration version, and so on.

   - If the validation checks for prepare to restore are successful, then the client is marked for automatic recovery. This automatic recovery is by default valid for 48 hours. Master server authenticity is validated automatically and a host-ID based certificate is automatically issued to this client during the automatic recovery process.
     Use the `nbhostmgmt` command to verify whether the client is marked for automatic recovery.
     For more information about the automatic recovery and the host-ID based certificate, refer to the *NetBackup Security and Encryption Guide*
     https://support.cohesity.com/s/article/article-100040135
   - If the validation checks fail, appropriate error messages are displayed. Follow the instructions that are provided in the message.
     For more information, See "Error messages for prepare to restore, prepare to discover, and the `bmrprep` command with reference to secure communication in BMR" on page 207.

The client is ready for restore.

To prepare a client for restore using the NetBackup web UI

1. In the NetBackup web UI, expand **Bare Metal Restore > Hosts > Bare Metal Restore clients**.
2. Select a client or a client configuration.
3. Select **Actions > Prepare to Restore**.
4. In the **Prepare to Restore Client** dialog box, select the appropriate values for the restore.

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

   If some other PTR options are selected, See "BMR disk recovery behavior" on page 88.

5 Click **OK**.

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

When you click **Prepare to Restore**, validation checks are performed pertaining to the different parameters such as SRT version, configuration version, and so on.

- If the validation checks for prepare to restore are successful, then the client is marked for automatic recovery. This automatic recovery is by default valid for 48 hours. Master server authenticity is validated automatically and a host-ID based certificate is automatically issued to this client during the automatic recovery process.
  Use the `nbhostmgmt` command to verify whether the client is marked for automatic recovery.
  For more information about the automatic recovery and the host-ID based certificate, refer to the *NetBackup Security and Encryption Guide*
  https://support.cohesity.com/s/article/article-100040135
  https://support.cohesity.com/s/article/article-100040135
- If the validation checks fail, appropriate error messages are displayed. Follow the instructions that are provided in the message.
  For more information, See "Error messages for prepare to restore, prepare to discover, and the `bmrprep` command with reference to secure communication in BMR" on page 207.

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

The client is listed in the **Bare Metal Restore Tasks** in **Queued** state. The Prepare-To-Restore step may take few minutes to complete.

To clean up the restore configuration

1 In the NetBackup web UI, click **Bare Metal Restore > BMR Tasks**.

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

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

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

BMR disk recovery behavior

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

- To restore a disk means that BMR formats the disk and restore files to it. No attempt is made to retain any data on the disk.

- To import a disk means that BMR tries to reuse the volumes on it (that is, mount the file systems automatically after restore). BMR tries to reuse rather than format the disk and restore files to it.

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

- **Restore system disks/volumes only**.
  - On AIX and HP-UX, the root volume groups (`rootvg` and `vg00`) are restored.
  - On Solaris, all disks that have any of the root file systems (`/`, `/swap`, `/var`, `/usr`) are restored.
  - On Windows, all disks that have `%SystemRoot%`, `%SystemBoot%`, and `%TEMP%` are restored. On Active Directory servers, BMR also restores the disks that contain the Active Directory system, database, and log files.
  - On Linux, all disks that have `/`, `usr/`, `/usr/local`, `/var`, `/opt`, `/tmp`, and `/boot` are restored.
- **Make available volumes on non-restored disks after the system is restored**. If you select this option, BMR imports the disks. Otherwise, the action depends on the disk class processing with prepare-to-restore options.

The following are the disk classes:

- System disks contain the operating system files that are required to boot the system.
- Nonsystem disks are all other disks, as follows:
  - Restorable disks are visible in the temporary restore environment and therefore can be restored.
  - Nonrestorable disks are not visible in the temporary restore environment and therefore cannot be restored. Typically these are SAN devices. You may not know that these disks cannot be restored until you attempt a restore. If these disks are required for a restore, you are forced to do a dissimilar disk restore (DDR).
  - Shared disks are shared with another system using clustering software. The client may not control them during or after the restore.
  - Missing disks may or may not have been used and are no longer attached to the system. These disks are in the restore configuration. More information is available about the actions to perform for missing disks.
    See "BMR disk class processing with prepare-to-restore options" on page 90.

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

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

BMR disk processing with prepare-to-restore options

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

Note the following about the restore options column:

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

Table 6-2 BMR disk actions

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

BMR disk class processing with prepare-to-restore options

Table 6-3 describes the actions that BMR performs for system disks.

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

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

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

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

Table 6-3 Actions for system disks

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

Table 6-4 Actions for nonsystem disks

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

Import actions for operating systems or volume managers

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

Note the following regarding import actions:

- HP-UX logical volume manager is a virtual auto import. An HP system can have VxVM managed root disks and some LVM managed disks. In a system only restore, the LVM database (the `/etc/lvmtab` file) is restored. Without any action required by BMR, these disks and their volumes are available. If entries remain in the `/etc/fstab` file for the file systems, those file systems are available.
- During a merge on Solaris systems or a merge on VxVM, BMR may remove entries in the `/etc/fstab` or `/etc/vfstab` files by commenting them out.
- Veritas Volume Manager is an auto import. VxVM has the ability (a disk group option) to import disk groups automatically. If there are entries in the `/etc/fstab` and the `/etc/vfstab` files, the file systems are available without BMR having to take action.
- Note the following for Windows imports:
  - Without import, only the drive letters that were recreated are assigned after restore.
  - With import, the drive letters assigned to volumes on Trusted disks are assigned to the same location after the restore. If the volume does not exist or has moved, you must edit the Mount Devices registry key.

Table 6-5 Import actions

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

About restoring BMR clients using network boot

Note: Review the secure communication compatibility support matrix for BMR table to know more about the supported master, boot server, client, and SRT versions for Linux, Windows, Solaris, AIX, and HP-UX environments. See "Secure communication compatibility matrices for BMR for NetBackup 8.1.1 and later releases" on page 258.

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

Note: If NetBackup access control management is used in your environment, you must provide the appropriate credentials when prompted so that NetBackup can restore the client files. To restore BMR Windows or UNIX client, you MUST perform `bpnbat -addmachine` on master server before restoring the client.

Use the `bpnbat -ShowMachines` command on the master server to view the name of the added machine.

To restore using media boot requires that you first create bootable media.	Refer sections on creating boot media.
Before you do a standard restore, you must run the prepare to restore operation using the current, saved configuration.	See "Preparing a client for restore" on page 86.
The procedure for restoring the client system depends on the manufacturer and mode.	See "Restoring an AIX client with network boot" on page 94. See "Restoring a Solaris client with network boot" on page 103. See "Restoring a HP-UX client with network boot" on page 97. See "Restoring a Linux client with network boot" on page 100. See "Restoring a Windows client with network boot" on page 104.

Other information about restoring clients is available.	See "About external procedures" on page 137. See "About performing complete backups" on page 26. See "About performing a full backup after a restore" on page 26. See "Ensuring successful backups" on page 26.

Restoring an AIX client with network boot

Note: Review the secure communication compatibility support matrix for BMR table to know more about the supported master, boot server, client, and SRT versions for Linux, Windows, Solaris, AIX, and HP-UX environments. See "Secure communication compatibility matrices for BMR for NetBackup 8.1.1 and later releases" on page 258.

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

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

AIX system restore requires certain information and resources.

The information to be configured in the firmware varies according to architecture, but can include the following:

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

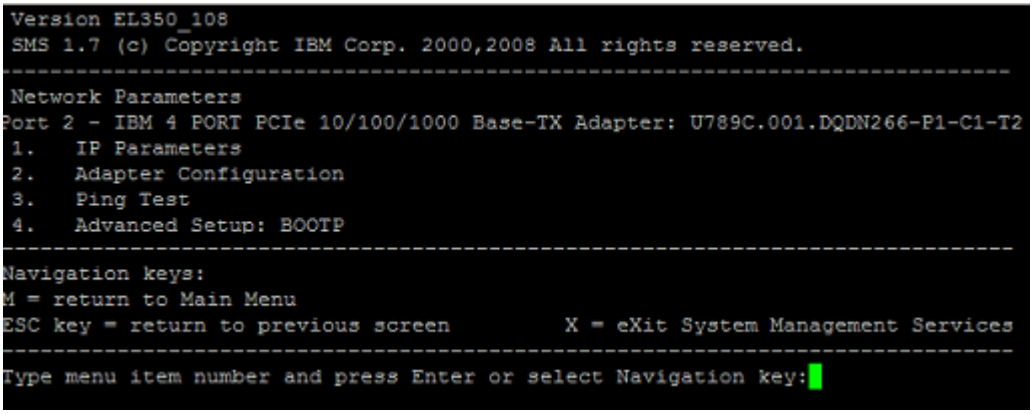
Here is sample screenshot showing the required entities configured in the target hardware firmware so that it can be BMR restored automatically upon a network boot.

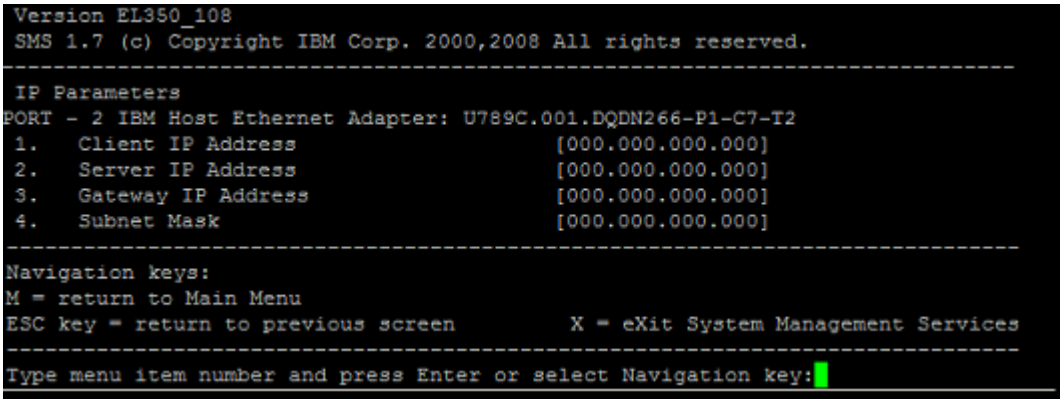
Figure 6-3 Sample AIX firmware settings

```
Version EL350_108
SMS 1.7 (c) Copyright IBM Corp. 2000,2008 All rights reserved.
-------------------------------------------------------------------------------
Main Menu
1.   Select Language
2.   Setup Remote IPL (Initial Program Load)
3.   Change SCSI Settings
4.   Select Console
5.   Select Boot Options
-------------------------------------------------------------------------------
Navigation Keys:

                                          X = eXit System Management Services
-------------------------------------------------------------------------------
Type menu item number and press Enter or select Navigation key:
```

```
Version EL350_108
SMS 1.7 (c) Copyright IBM Corp. 2000,2008 All rights reserved.
-------------------------------------------------------------------------------
NIC Adapters
     Device                          Location Code                Hardware
                                                                  Address
1.   PORT - 1 IBM Host Ethernet Ada  U789C.001.DQDN266-P1-C7-T1   00215e48b8d0
2.   PORT - 2 IBM Host Ethernet Ada  U789C.001.DQDN266-P1-C7-T2   00215e48b8d1
3.   Port 1 - IBM 4 PORT PCIe 10/10  U789C.001.DQDN266-P1-C1-T1   00145ee791d8
4.   Port 2 - IBM 4 PORT PCIe 10/10  U789C.001.DQDN266-P1-C1-T2   00145ee791d9
5.   Port 1 - IBM 4 PORT PCIe 10/10  U789C.001.DQDN266-P1-C1-T3   00145ee791da
6.   Port 2 - IBM 4 PORT PCIe 10/10  U789C.001.DQDN266-P1-C1-T4   00145ee791db
-------------------------------------------------------------------------------
Navigation keys:
M = return to Main Menu
ESC key = return to previous screen         X = eXit System Management Services
-------------------------------------------------------------------------------
Type menu item number and press Enter or select Navigation key:
```

```
Version EL350_108
SMS 1.7 (c) Copyright IBM Corp. 2000,2008 All rights reserved.
-------------------------------------------------------------------------------
Select Internet Protocol Version.

1.   IPv4 - Address Format 123.231.111.222
2.   IPv6 - Address Format 1234:5678:90ab:cdef:1234:5678:90ab:cdef
-------------------------------------------------------------------------------
Navigation keys:
M = return to Main Menu
ESC key = return to previous screen         X = eXit System Management Services
-------------------------------------------------------------------------------
Type menu item number and press Enter or select Navigation key:1
```





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

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

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

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

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

To restore an AIX client with network boot

1. Prepare to restore the client.

   See “Preparing a client for restore” on page 86.

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

   Due to the automatic recovery parameter set during prepare to restore, the restore operation attempts to retrieve the host-ID based certificate and validate the Certificate Authority (CA) certificate. This recovery is time bound. For more information about the automatic recovery during prepare to restore, See “Preparing a client for restore” on page 86.

   Note: If you abort the restore operation or if the restore operation fails, either run the prepare to restore operation again to restart the automatic recovery or manually set the **Security > Host mappings > Hosts > Menu button > Allow auto reissue certificate** option using the **NetBackup web UI** or command-line interface.

   For more information about manually setting the *Allow Auto Reissue Certificate* option, see *Allowing automatic reissue of a certificate* section within the *NetBackup Security and Encryption Guide*

   https://support.cohesity.com/s/article/article-100040135

   The restore begins.

   After a successful completion of restore, the host ID-based certificate is copied on the client that is restored. The automatic recovery parameter is reset. For more information about the automatic recovery, See “Preparing a client for restore” on page 86.

Restoring a HP-UX client with network boot

Note: Review the secure communication compatibility support matrix for BMR table to know more about the supported master, boot server, client, and SRT versions for Linux, Windows, Solaris, AIX, and HP-UX environments. See “Secure communication compatibility matrices for BMR for NetBackup 8.1.1 and later releases” on page 258.

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

HP-UX system restore requires certain information and resources.

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

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

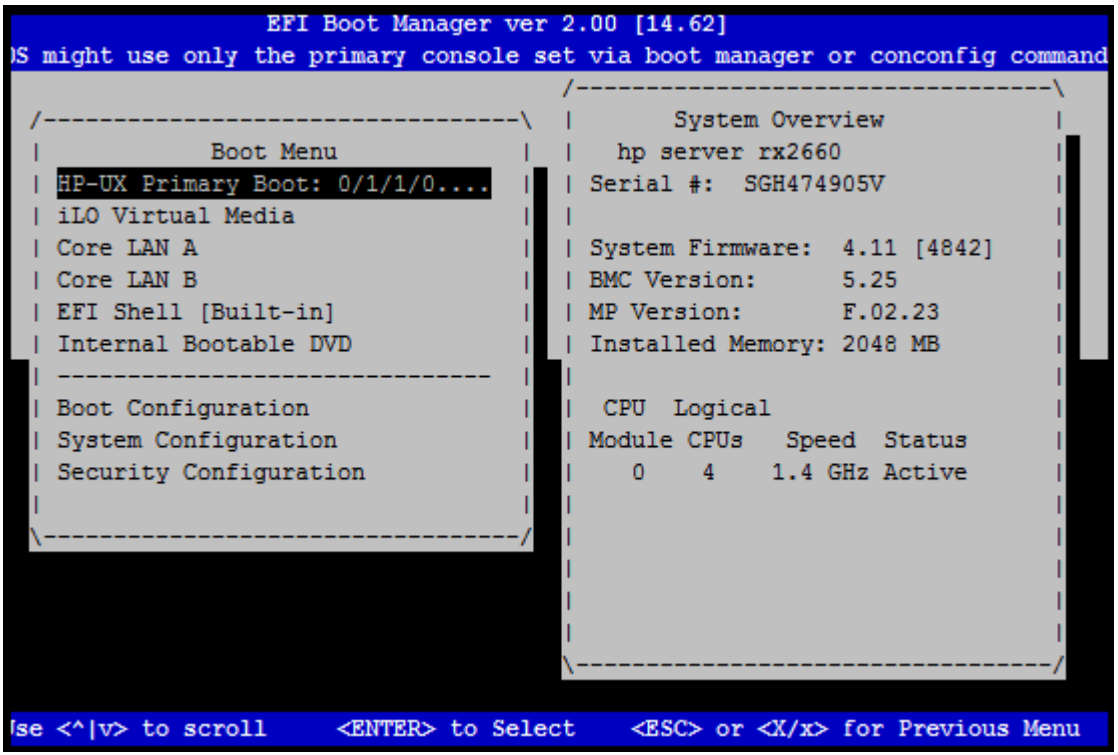
After you perform the network boot procedure, the remainder of the restore process is automatic and requires no manual intervention. After the restore finishes and the client reboots itself, it is completely restored.

To restore a HP-UX IA client with network boot

1. Prepare to restore the client.

   See "Preparing a client for restore" on page 86.

2. Boot the client to restore.



3. If the client is a workstation, select the operating system language by number. For example, US English is 61.
4. After you enter the language choice, press **Enter** twice to select and confirm the choice. The HP-UX Ignite menu opens.
5. Use the arrow key to scroll to **Run a Recovery Shell**. Wait while the DHCP search occurs and until the **Network Configuration** menu opens. If you interrupt a DHCP search, the BMR restore may fail.
6. Answer the following prompts:
   - `Hostname:`

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

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

The system boots from the network.

Due to the automatic recovery parameter set during prepare to restore, the restore operation attempts to retrieve the host-ID based certificate and validate the Certificate Authority (CA) certificate. This recovery is time bound. For more information about the automatic recovery during prepare to restore, See "Preparing a client for restore" on page 86.

Note: If you abort the restore operation or if the restore operation fails, either run the prepare to restore operation again to restart the automatic recovery or manually set the **Security > Host mappings > Hosts > Menu button > Allow auto reissue certificate** option using the **NetBackup web UI** or command-line interface.

For more information about manually setting the *Allow Auto Reissue Certificate* option, see *Allowing automatic reissue of a certificate* section within the *NetBackup Security and Encryption Guide*

https://support.cohesity.com/s/article/article-100040135

8 The restore begins.

After a successful completion of restore, the host ID-based certificate is copied on the client that is restored. The automatic recovery parameter is reset. For more information about the automatic recovery, See "Preparing a client for restore" on page 86.

Restoring a Linux client with network boot

Note: Review the secure communication compatibility support matrix for BMR table to know more about the supported master, boot server, client, and SRT versions for Linux, Windows, Solaris, AIX, and HP-UX environments. See "Secure communication compatibility matrices for BMR for NetBackup 8.1.1 and later releases" on page 258.

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

To network boot Linux clients, BMR requires the following:

- PXE
- DHCP
- TFTP
- NFS

During the prepare-to-restore operation all the information is gathered that is required for a Linux network boot. For Linux client network based recovery, you need to make sure above listed services are configured on the BMR boot server and are running. You need to require to do any client specific settings in these services configuration files. BMR handles the required network boot services configuration for the selected client during prepare-to-restore operation. To know more on the required network services configuration,

See "Network services configurations on BMR boot Server" on page 244.

After the prepare-to-restore, boot the client to start the restore.

To network boot a Linux client

1. Prepare to restore the client.

   See "Preparing a client for restore" on page 86.

2. Ensure that no other DHCP service except the one running on BMR Boot server is running in the same subnet. Otherwise the client DHCP boot request may go to un-intended DHCP server and PXE network boot may fail.

   Note: This is the limitation with PXE, DHCP boot protocols where first DHCP reply failure stops network boot process. Hence recommendation is to keep only Linux DHCP service on the boot server running.

3. Boot the client to restore.

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

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

Due to the automatic recovery parameter set during prepare to restore, the restore operation attempts to retrieve the host-ID based certificate and validate the Certificate Authority (CA) certificate. This recovery is time bound. For more information about the automatic recovery during prepare to restore, See "Preparing a client for restore" on page 86.

Note: If you abort the restore operation or if the restore operation fails, either run the prepare to restore operation again to restart the automatic recovery or manually set the **Security > Host mappings > Hosts > Menu button > Allow auto reissue certificate** option using the **NetBackup web UI** or command-line interface.

For more information about manually setting the *Allow Auto Reissue Certificate* option, see *Allowing automatic reissue of a certificate* section within the *NetBackup Security and Encryption Guide*

https://support.cohesity.com/s/article/article-100040135

---

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

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

6 Upon successful client recovery, BMR automatically cleans up any network boot settings added for the client in DHCP configuration during prepare-to-restore operation.

After a successful completion of restore, the host ID-based certificate is copied on the client that is restored. The automatic recovery parameter is reset. For more information about the automatic recovery, See "Preparing a client for restore" on page 86.

Restoring a Solaris client with network boot

Note: Review the secure communication compatibility support matrix for BMR table to know more about the supported master, boot server, client, and SRT versions for Linux, Windows, Solaris, AIX, and HP-UX environments. See "Secure communication compatibility matrices for BMR for NetBackup 8.1.1 and later releases" on page 258.

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

To network boot Solaris clients, BMR requires the following:

- `PXE` (In case of Solaris-x64 platform based client recovery)
- `DHCP`
- `TFTP`
- NFS

To know more on the required network services configuration,

See "Network services configurations on BMR boot Server" on page 244.

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

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

To restore a Solaris client with network boot

1. Prepare to restore the client.

   See "Preparing a client for restore" on page 86.

2. Ensure that no other DHCP service except the one running on BMR Solaris Boot server is running in the same subnet. Otherwise the client DHCP boot request goes to un-intended DHCP server and network boot may fail.

   Note: This is a limitation with DHCP, PXE boot protocols themselves where first DHCP reply failure stops network boot process. Hence recommendation is to keep only Solaris DHCP service on the boot server running.

3 Boot the client to restore.

4 Terminate the boot process by using the **#.**command to return to the `sc>` prompt and send break command from `sc>`prompt to get OK prompt.

5 Start the network boot by entering the following command

`(net[id] is the device that points to the BMR boot server): boot net[id]` where [id] is 1,2,3 interface cards.

6 Start the network boot by entering the following command (*net[id]* is the device that points to the BMR boot server):`boot net[id]` where id is 1,2,3 interface cards.

Due to the automatic recovery parameter set during prepare to restore, the restore operation attempts to retrieve the host-ID based certificate and validate the Certificate Authority (CA) certificate. This recovery is time bound. For more information about the automatic recovery during prepare to restore, See "Preparing a client for restore" on page 86.

Note: If you abort the restore operation or if the restore operation fails, either run the prepare to restore operation again to restart the automatic recovery or manually set the **Security > Host mappings > Hosts > Menu button > Allow auto reissue certificate** option using the **NetBackup web UI** or command-line interface.

For more information about manually setting the *Allow Auto Reissue Certificate* option, see *Allowing automatic reissue of a certificate* section within the *NetBackup Security and Encryption Guide*

https://support.cohesity.com/s/article/article-100040135

After a successful completion of restore, the host ID-based certificate is copied on the client that is restored. The automatic recovery parameter is reset. For more information about the automatic recovery, See "Preparing a client for restore" on page 86.

Restoring a Windows client with network boot

Note: Review the secure communication compatibility support matrix for BMR table to know more about the supported master, boot server, client, and SRT versions for Linux, Windows, Solaris, AIX, and HP-UX environments. See "Secure communication compatibility matrices for BMR for NetBackup 8.1.1 and later releases" on page 258.

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

Windows systems network boot uses the PXE protocol. The BMR boot server provides and manages the PXE network services, but a DHCP service is required in the environment. A DHCP service can exist on the same Boot server or anywhere in the subnet.

To restore a Windows client with network boot

1. Prepare to restore the client.

   See "Preparing a client for restore" on page 86.

2. Ensure that PXE and TFTP services configuration on BMR Boot server is done once.

   If BMR PXE configuration is not done ever on the boot server then run **PXE Service Configuration Wizard** available in **BMR Boot server assistant** which can be located in the **Start** menu on the Windows BMR boot server.

   For this, click **Programs** >**NetBackup web UI** > **Windows > Veritas netbackup > BMR Boot Server Assistant**. This BMR PXE service configuration needs to be done only once for a Windows boot server. If the DHCP server location changes later then this wizard needs to be run again.

   Note: Any other non-BMR PXE or TFTP service running on the same BMR Boot server cannot be used for BMR recovery. Make sure to stop these services while client network boots for recovery. Otherwise the client PXE boot request goes to un-intended server and PXE network boot may fail. This is a limitation with PXE, DHCP boot protocols, Cohesity recommendation is to keep only correct PXE, DHCP, TFTP servers running while booting client for network based recovery.

3. Make sure BMR PXE and TFTP services are up and running.
4. Boot the client to restore.

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

Due to the automatic recovery parameter set during prepare to restore, the restore operation attempts to retrieve the host-ID based certificate and validate the Certificate Authority (CA) certificate. This recovery is time bound. For more information about the automatic recovery during prepare to restore, See "Preparing a client for restore" on page 86.

Note: If you abort the restore operation or if the restore operation fails, either run the prepare to restore operation again to restart the automatic recovery or manually set the **Security > Host mappings > Hosts > Menu button > Allow auto reissue certificate** option using the **NetBackup web UI** or command-line interface.

For more information about manually setting the *Allow Auto Reissue Certificate* option, see *Allowing automatic reissue of a certificate* section within the *NetBackup Security and Encryption Guide*

https://support.cohesity.com/s/article/article-100040135

---

6 When you are prompted, press the **Function 12** key and the system boots and the restore begins.

After a successful completion of restore, the host ID-based certificate is copied on the client that is restored. The automatic recovery parameter is reset. For more information about the automatic recovery, See "Preparing a client for restore" on page 86.

About restoring BMR clients using media boot

Note: Review the secure communication compatibility support matrix for BMR table to know more about the supported master, boot server, client, and SRT versions for Linux, Windows, Solaris, AIX, and HP-UX environments. See "Secure communication compatibility matrices for BMR for NetBackup 8.1.1 and later releases" on page 258.

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

To restore using media boot requires that you first create bootable media.	Refer sections on creating boot media.
Before you do a standard restore, you must run the prepare to restore operation using the current, saved configuration.	See "Preparing a client for restore" on page 86.
The procedure for restoring the client system depends on the manufacturer and mode.	See "Restoring an AIX client with media boot" on page 107. See "Restoring a HP-UX client with media boot" on page 109. See "Restoring a Linux client with media boot" on page 111. See "Restoring a Solaris client with media boot" on page 113. See "Restoring a Windows client with media boot" on page 115.
Other information about restoring clients is available.	See "About external procedures" on page 137. See "About performing complete backups" on page 26. See "About performing a full backup after a restore" on page 26. See "Ensuring successful backups" on page 26.

Restoring an AIX client with media boot

Note: Review the secure communication compatibility support matrix for BMR table to know more about the supported master, boot server, client, and SRT versions for Linux, Windows, Solaris, AIX, and HP-UX environments. See "Secure communication compatibility matrices for BMR for NetBackup 8.1.1 and later releases" on page 258.

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

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

To restore an AIX client with media boot

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

   See "Preparing a client for restore" on page 86.

2. Boot the client from the boot media you created. For instructions on how to boot from a CD or from a DVD, see the IBM hardware documentation.

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

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

   Due to the automatic recovery parameter set during prepare to restore, the restore operation attempts to retrieve the host-ID based certificate and validate the Certificate Authority (CA) certificate. This recovery is time bound. For more information about the automatic recovery during prepare to restore, See "Preparing a client for restore" on page 86.

   The restore begins.

Note: If you abort the restore operation or if the restore operation fails, either run the prepare to restore operation again to restart the automatic recovery or manually set the **Security > Host mappings > Hosts > Menu button > Allow auto reissue certificate** option using the **NetBackup web UI** or command-line interface.

For more information about manually setting the *Allow Auto Reissue Certificate* option, see *Allowing automatic reissue of a certificate* section within the *NetBackup Security and Encryption Guide*

https://support.cohesity.com/s/article/article-100040135

After a successful completion of restore, the host ID-based certificate is copied on the client that is restored. The automatic recovery parameter is reset. For more information about the automatic recovery, See "Preparing a client for restore" on page 86.

Restoring a HP-UX client with media boot

Note: Review the secure communication compatibility support matrix for BMR table to know more about the supported master, boot server, client, and SRT versions for Linux, Windows, Solaris, AIX, and HP-UX environments. See "Secure communication compatibility matrices for BMR for NetBackup 8.1.1 and later releases" on page 258.

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

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

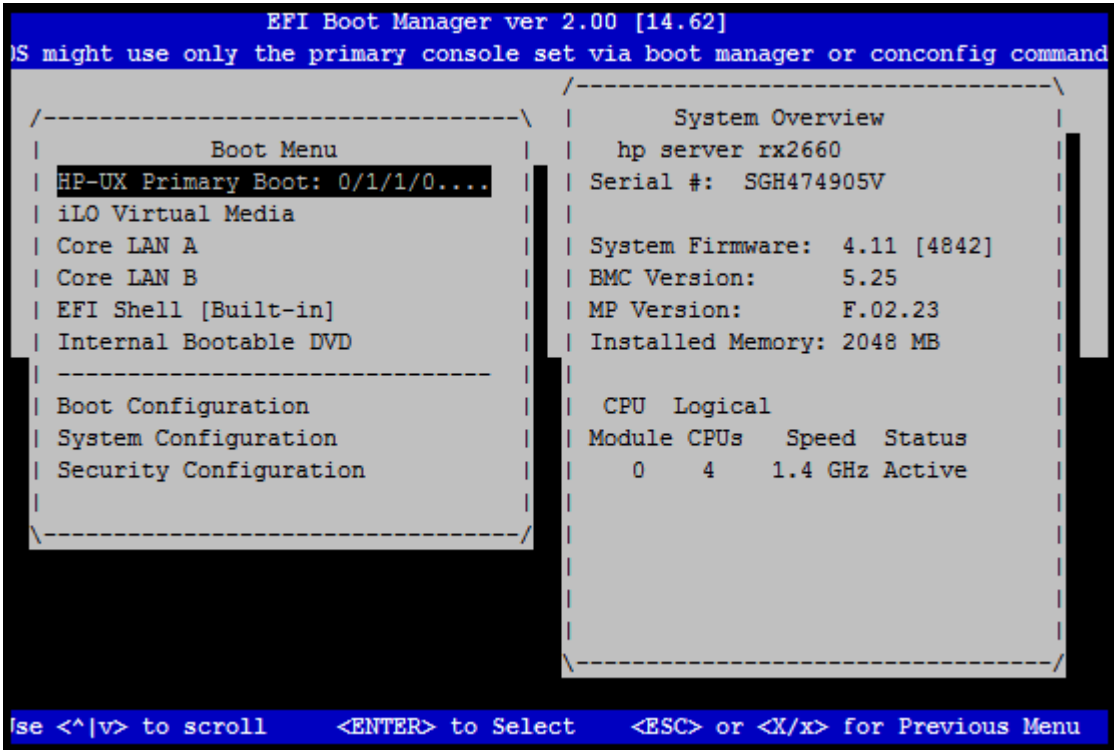
To restore a HP-UX IA client with media boot

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

   See "Preparing a client for restore" on page 86.

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

3 Boot the client to restore.



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

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

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

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

7 Enter the following information when prompted:

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

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

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

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

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

Due to the automatic recovery parameter set during prepare to restore, the restore operation attempts to retrieve the host-ID based certificate and validate the Certificate Authority (CA) certificate. This recovery is time bound. For more information about the automatic recovery during prepare to restore, See "Preparing a client for restore" on page 86.

The restore begins.

Note: If you abort the restore operation or if the restore operation fails, either run the prepare to restore operation again to restart the automatic recovery or manually set the **Security > Host mappings > Hosts > Menu button > Allow auto reissue certificate** option using the **NetBackup web UI** or command-line interface.

For more information about manually setting the *Allow Auto Reissue Certificate* option, see *Allowing automatic reissue of a certificate* section within the *NetBackup Security and Encryption Guide*

https://support.cohesity.com/s/article/article-100040135

After a successful completion of restore, the host ID-based certificate is copied on the client that is restored. The automatic recovery parameter is reset. For more information about the automatic recovery, See "Preparing a client for restore" on page 86.

Restoring a Linux client with media boot

Note: Review the secure communication compatibility support matrix for BMR table to know more about the supported master, boot server, client, and SRT versions for Linux, Windows, Solaris, AIX, and HP-UX environments. See "Secure communication compatibility matrices for BMR for NetBackup 8.1.1 and later releases" on page 258.

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

Use the following procedure for Linux clients.

To restore a Linux client with media boot

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

   See "Preparing a client for restore" on page 86.

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

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

3. Boot the client to restore.

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

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

   Due to the automatic recovery parameter set during prepare to restore, the restore operation attempts to retrieve the host-ID based certificate and validate the Certificate Authority (CA) certificate. This recovery is time bound. For more information about the automatic recovery during prepare to restore, See "Preparing a client for restore" on page 86.

   The restore begins.

Note: If you abort the restore operation or if the restore operation fails, either run the prepare to restore operation again to restart the automatic recovery or manually set the **Security > Host mappings > Hosts > Menu button > Allow auto reissue certificate** option using the **NetBackup web UI** or command-line interface.

For more information about manually setting the *Allow Auto Reissue Certificate* option, see *Allowing automatic reissue of a certificate* section within the *NetBackup Security and Encryption Guide*

https://support.cohesity.com/s/article/article-100040135

After a successful completion of restore, the host ID-based certificate is copied on the client that is restored. The automatic recovery parameter is reset. For more information about the automatic recovery, See "Preparing a client for restore" on page 86.

Restoring a Solaris client with media boot

Note: Review the secure communication compatibility support matrix for BMR table to know more about the supported master, boot server, client, and SRT versions for Linux, Windows, Solaris, AIX, and HP-UX environments. See "Secure communication compatibility matrices for BMR for NetBackup 8.1.1 and later releases" on page 258.

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

Use the following procedure for Solaris clients.

To restore a Solaris client with media boot

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

   See "Preparing a client for restore" on page 86.
2. Insert the bootable CD or bootable DVD into the CD-ROM drive.
3. Boot the client to restore.
4. Terminate the boot process by pressing command `#.` to return to the `sc>` prompt and send break command from `sc>` prompt to get OK prompt.

5 Enter the following command:

```
boot cdrom
```

The Solaris OS Installation prompts you for network identification.

6 Enter the network identification.

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

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

Due to the automatic recovery parameter set during prepare to restore, the restore operation attempts to retrieve the host-ID based certificate and validate the Certificate Authority (CA) certificate. This recovery is time bound. For more information about the automatic recovery during prepare to restore, See "Preparing a client for restore" on page 86.

After you enter the required information, the restore begins.

Note: If you abort the restore operation or if the restore operation fails, either run the prepare to restore operation again to restart the automatic recovery or manually set the **Security > Host mappings > Hosts > Menu button > Allow auto reissue certificate** option using the **NetBackup web UI** or command-line interface.

For more information about manually setting the *Allow Auto Reissue Certificate* option, see *Allowing automatic reissue of a certificate* section within the *NetBackup Security and Encryption Guide*

https://support.cohesity.com/s/article/article-100040135

After a successful completion of restore, the host ID-based certificate is copied on the client that is restored. The automatic recovery parameter is reset. For more information about the automatic recovery, See "Preparing a client for restore" on page 86.

Restoring a Windows client with media boot

Note: Review the secure communication compatibility support matrix for BMR table to know more about the supported master, boot server, client, and SRT versions for Linux, Windows, Solaris, AIX, and HP-UX environments. See "Secure communication compatibility matrices for BMR for NetBackup 8.1.1 and later releases" on page 258.

Note: If NetBackup access management is used in your environment, you must provide the appropriate credentials when prompted so that NetBackup can restore the client files. To restore BMR Windows client, you MUST perform `bpnbat -addmachine` on master server before restoring the client.

Use the `bpnbat -ShowMachines` command on the master server to view the name of the added machine.

To media boot a Windows client, do the following.

To restore a Windows client with media boot

1. Prepare to restore the client.

   See "Preparing a client for restore" on page 86.

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

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

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

Due to the automatic recovery parameter set during prepare to restore, the restore operation attempts to retrieve the host-ID based certificate and validate the Certificate Authority (CA) certificate. This recovery is time bound. For more information about the automatic recovery during prepare to restore, See "Preparing a client for restore" on page 86.

Note: If you abort the restore operation or if the restore operation fails, either run the prepare to restore operation again to restart the automatic recovery or manually set the **Security > Host mappings > Hosts > Menu button > Allow auto reissue certificate** option using the **NetBackup web UI** or command-line interface.

For more information about manually setting the *Allow Auto Reissue Certificate* option, see *Allowing automatic reissue of a certificate* section within the *NetBackup Security and Encryption Guide*

https://support.cohesity.com/s/article/article-100040135

---

4 Boot the client to restore.

The following message appears:

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

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

After a successful completion of restore, the host ID-based certificate is copied on the client that is restored. The automatic recovery parameter is reset. For more information about the automatic recovery, See "Preparing a client for restore" on page 86.

Generic BMR Restore

NetBackup Bare Metal Restore (BMR) provides a feature to restore a Windows client without performing Prepare to Restore (PTR) operation. This feature is referred to as **Generic BMR Restore**.

To restore a Windows client using Generic BMR

1. Boot the client using Windows SRT. After you boot the client using Windows SRT, on the screen that appears, as shown in the figure, press any key to proceed to the **Veritas System Recovery Disk** wizard.
2. On the **Veritas System Recovery Disk** wizard, click **Generic BMR Restore**
3. On the screen that appears, as shown in the figure, enter the following network details:
   - IP Address
   - Netmask
   - Gateway
   - NetBackup master server IP address
   - NetBackup master server name

   Then click **Contact Master Server**.
4. Validate and confirm if the selected primary server with which the client intends to establish a communication is a trusted server.

   Click **Yes**, if you trust the primary server.

   For more information on how to validate the Certificate Authority (CA) hash certificate, refer to the *Finding and communicating the fingerprint of a CA certificate* section in the *NetBackup Security and Encryption Guide*

   https://support.cohesity.com/s/article/article-100040135
5. Enter the **Reissue** token and then click **OK**.

   Use the **Certificate Management** node on **NetBackup** web UI to generate click on the left **Host mappings > Hosts > Menu button > Generate reissue token**.

   For more information on how to generate a reissue type of authorization token, refer to the *Creating a reissue token* section in the *NetBackup web UI Help or the NetBackup Security and Encryption Guide*.

   https://support.cohesity.com/s/article/article-100040135

6 From the client configuration drop-down list, select the client configuration that you want to restore and click **Restore Client**.

Note: The list displays configurations of only that particular client with which the provided reissue token is associated.

Select **Show all configurations** if you want to view a list of all the configurations that are associated with the client for which you have provided reissue token.

7 The restore begins with no further user intervention required.

8 After a successful completion of restore, the host ID-based certificate is copied on the client that is restored.

Generic Discovery of Hardware

NetBackup Bare Metal Restore (BMR) provides a feature to discover a Windows client without performing Prepare to Discover (PTD) operation. This feature is referred to as **Generic Discovery of Hardware**.

To discover a Windows client using Generic Discovery

1 Boot the client using Windows SRT. After you boot the client using Windows SRT, on the screen that appears, as shown in the figure, press any key to proceed to the **Veritas System Recovery Disk** wizard.

2 On the **Veritas System Recovery Disk** wizard, click **Generic Discovery of Hardware**.

3 Provide the details of the configuration.

(Optional) Select the **Save a discovered configuration locally** check box, if you want to save the discovered configuration on your local system. The discovered configuration is saved in the XML format.

4 Click **Do Discover**.

If you have selected **Save a discovered configuration locally** check box and then clicked **Do Discover**, the discovery continues without any further user intervention required.

5 If you do not select the **Save a discovered configuration locally** check box and click **Do Discover**, on the screen that appears, you must enter the following network details:

- IP Address
- Netmask

- Gateway
- NetBackup master server IP address
- NetBackup master server name

6 Click **Contact Master Server**, after you have entered all the details mentioned in Step 5.

7 (Conditional to Step 5 and 6)Validate and confirm if the selected primary server with which the client intends to establish a communication is a trusted server.

Click **Yes**, if you trust the primary server.

For more information on how to validate the Certificate Authority (CA) hash certificate, refer to the *Finding and communicating the fingerprint of a CA certificate* section in the *NetBackup Security and Encryption Guide*

https://support.cohesity.com/s/article/article-100040135

8 (Conditional to step 5 and 6) Click on the left **Host mappings > Hosts > Menu button > Generate reissue token** and then click **OK**

Use the **Certificate Management** node on **NetBackup** web UI to generate click on the left **Host mappings > Hosts > Menu button > Generate reissue token**.

For more information on how to generate a reissue type of authorization token, refer to the *Creating a reissue token* section in the *NetBackup web UI Help or the NetBackup Security and Encryption Guide*.

https://support.cohesity.com/s/article/article-100040135

9 Click **OK**. Discovery completes with no further user intervention required.

After a successful discovery, the discovered configuration is listed under **Bare Metal Restore > Resources > Discovered configurationsBare Metal Restore > Resources > Discovered configurations** on the **NetBackup** web UI.

About restoring to a specific point in time

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

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

About the point in time restore process

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

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

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

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

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

Creating a point in time restore configuration

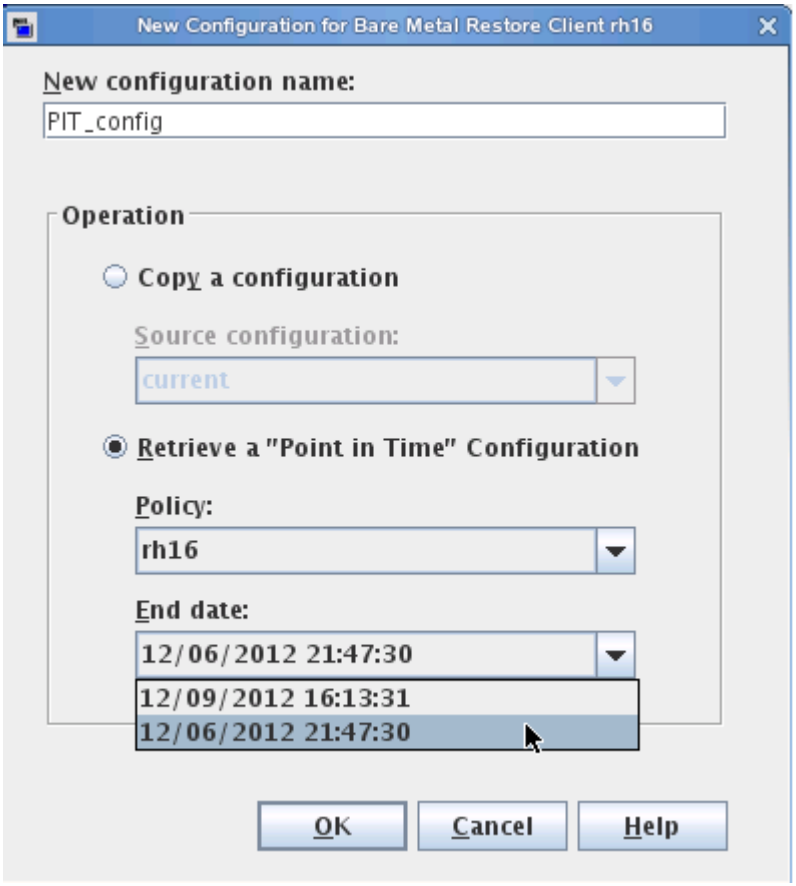
The following procedure creates the restore configuration for a point in time restore for any client type. Then follow the standard restore procedures for the client.

To create a point in time restore configuration

1. In the NetBackup web UI, expand **Bare Metal Restore > Hosts > Bare Metal Restore Clients** .
2. In the **All Bare Metal Restore Clients** pane, right-click the saved configuration for the client (the configuration labeled current), then select **New** from the shortcut menu.

3 In the **New Configuration** dialog box, enter a name for the new configuration.

Below is a sample screenshot showing creation of Point-In-Time configuration for recovery.



4 Click **Retrieve from NetBackup**.

5 Select the **Policy** and **End Date** for the restore.

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

6 Click **OK**.

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

7 Restore the client.

See "About restoring BMR clients using network boot" on page 93.

See "About restoring BMR clients using media boot" on page 106.

About restoring to dissimilar disks

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

About the dissimilar disk restore process

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

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

Mapping occurs as follows:

- Before the restore: You can create a configuration you can edit (an editable restore configuration) and initialize that configuration with the new disk layouts. Then map the original volume configuration to the new disks. After you finish mapping, you restore the client using the restore configuration.
  - Layouts of the new disks on the client, which is necessary, for example, when you perform a discovery operation.
  - Whether another protected client has the same disks.
- During the restore: You perform a standard restore and BMR detects that the disks are different. BMR enters DDR mode and creates an editable restore configuration so you can map the disks.
  - For UNIX and Linux clients, use the BMR disk mapping utility in the NetBackup web UI on the master server.
  - For Windows clients, you can map on the client during recovery or on the master server using the BMR disk mapping utility in the NetBackup web UI.

You should use dissimilar disk restore in the following circumstances:

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

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

Creating a restore configuration for DDR

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

In case of Windows client recovery, you do not have to create a DDR configuration before you begin the restore. You can begin a restore and perform disk mapping during the restore itself. BMR windows recovery opens disk mapping GUI automatically in case it fails to map original disks to the disks available during recovery time. While in case of UNIX/Linux client case, if disks matching fails then recovery process goes into target hardware discovery mode.

See "Restoring a client to dissimilar disks" on page 124.

Table 6-6 To create a restore configuration

Step	Task	Procedure
Step 1	Discover the configuration of the new disks.	See "Discovering a configuration" on page 156.
Step 2	Create an editable restore configuration by copying the current configuration.	See "Copying a configuration" on page 155.
Step 3	Open the **Change Configuration** dialog box for the restore configuration.	See "Modifying a configuration" on page 159.

Table 6-6 To create a restore configuration *(continued)*

Step	Task	Procedure
Step 4	Initialize the restore configuration with the disk information from the discovered configuration and then map the original volume configuration to the new disks.	See "About Volumes properties" on page 173.
Step 5	After you finish mapping, perform the DDR restore procedure.	See "Restoring a client to dissimilar disks" on page 124.

Restoring a client to dissimilar disks

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

Note the following for UNIX and Linux DDR:

- Shared disks in a cluster are marked restricted.
- Unused VxVM disks on Solaris clients are marked restricted and should remain restricted.
- You cannot map Linux LVM volume groups with the physical volumes that were created on top of multi devices with the same configuration. The physical volumes are mapped to either disks or partitions but not to a multi device.

Table 6-7 To perform a dissimilar disk restore

Step	Task	Procedure
Step 1	Prepare to restore the client.	If you prepared a restore configuration in advance, select that configuration during the prepare operation. See "Preparing a client for restore" on page 86.

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

Step	Task	Procedure
Step 2	Begin the restore by booting the client using either network boot or media boot.	If you use a configuration where the protected system's volume configuration is already mapped to the new disks, the restore proceeds as a standard restore. No intervention is required. If BMR detects that the disks are different and are not already mapped, BMR enters DDR mode. In case of Windows, you can map volumes to recovery time disks at this point by using auto popped-up BMR configuration mapping GUI. See "BMR restore process" on page 84.
Step 3	Save the editable restore configuration.	Non-editable configuration only. If you use a configuration that cannot be edited, BMR creates an editable restore configuration. It copies the current configuration and prompts you to enter a name for it, as follows: `Current configuration name for restore is 'current'. Please enter the name for a new editable configuration:`

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

Step	Task	Procedure
Step 4	Save the discovered configuration.	To obtain the layouts of the new disks, BMR discovers the hardware of the client. BMR prompts you for a name for the discovered configuration, as follows: `Please enter the name for a new discovered configuration:` BMR saves the discovered configuration. Later, you import the disk layouts from this discovered configuration into the restore configuration by using **Initialize** option on BMR configuration mapping GUI (as described in step-6).
Step 5	Open the **Change Configuration**	After the discovered configuration is saved, in the NetBackup web UI on the master server, on the left click **Bare Metal Restore > Hosts > Bare Metal Restore Clients** for the restore configuration. See "Modifying a configuration" on page 159.
Step 6	Initialize the restore configuration.	Initialize the restore configuration with the new disk layout from the discovered configuration. And then map the original volume configuration to the new disks. See "About Volumes properties" on page 173.

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

Step	Task	Procedure
Step 7	Prepare to restore and then restore the client, using the edited restore configuration.	See "Preparing a client for restore" on page 86. See "About restoring BMR clients using network boot" on page 93. See "About restoring BMR clients using media boot" on page 106.
Step 8	If the disk mapping in the restore configuration is incomplete, BMR enters DDR mode again so you can continue to map volumes to disks.	See "About Volumes properties" on page 173.

Restoring to a dissimilar system

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

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

Table 6-8 Dissimilar system restore overview

Step	Task	Procedure
Step 1	Learn about dissimilar system restore.	See "About dissimilar system restore" on page 128.
Step 2	Discover the configuration of the target system.	See "About discovering the configuration of the new system" on page 129.
Step 3	Create a configuration to use for the restore.	See "Creating an editable DSR configuration" on page 129.
Step 4	Add NIC drivers and the MSD drivers to the restore configuration system.	See "About adding NIC and MSD drivers" on page 129.
Step 5	Change the network interfaces and network identities in the restore configuration.	See "About changing network interfaces" on page 130.

Table 6-8 Dissimilar system restore overview *(continued)*

Step	Task	Procedure
Step 6	Map disks in the restore configuration.	See "About mapping disks in the restore configuration" on page 131.
Step 7	Create boot media.	See "About creating boot media" on page 131.
Step 8	Restore the client.	See "About restoring the client" on page 131.
Step 9	Complete the DSR changes at the first logon to the restored system.	See "Logging on for the first time after system restore" on page 132.

About dissimilar system restore

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

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

A DSR is useful in the following situations:

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

Use DSR when any of the following conditions apply:

- The target system has a disk controller that the protected system does not have.
- The target system has a network card that the protected system does not have.
- The target system requires a different hardware abstraction layer (HAL) or kernel than the protected system.

- The target system has different TCP/IP settings than the protected system has. (Only TCP/IP properties are restored. Other networking properties, such as Internetwork Packet Exchange (IPX), are not restored and must be configured after the restore.)

About discovering the configuration of the new system

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

See "Discovering a configuration" on page 156.

Creating an editable DSR configuration

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

Table 6-9 Process for creating an editable DSR configuration

Step	Action	Related topic
Step 1	Create the DSR configuration by copying an existing configuration of the protected client. For example, to restore client `protected` to system `target`, create a configuration named `dsr_to_target` by copying the current configuration of client `protected`.	See "Copying a configuration" on page 155.
Step 2	After you create the DSR configuration, open the **Change Configuration** dialog box to modify the configuration as described in the following sections.	See "Client configuration properties" on page 161.

About adding NIC and MSD drivers

This section is applicable only for Windows operating system.

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

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

See "Discovering a configuration" on page 156.

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

See "Devices and drivers properties" on page 163.

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

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

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

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

About changing network interfaces

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

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

See "Discovering a configuration" on page 156.

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

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

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

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

See "Network interfaces properties" on page 167.

About mapping disks in the restore configuration

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

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

See "Discovering a configuration" on page 156.

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

- Import the disk layouts from that configuration.
- Map disks before the restore.

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

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

More information is available about dissimilar disk restore.

See "About restoring to dissimilar disks" on page 122.

During the recovery of a Windows client, if the BMR recovery process detects a vendor partition on the disk of the target system where the client operating system is being recovered, BMR prompts the user with an option to preserve the detected vendor partition.

About creating boot media

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

See "Managing boot media" on page 77.

About restoring the client

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

See "About restoring BMR clients using network boot" on page 93.

See "About restoring BMR clients using media boot" on page 106.

Logging on for the first time after system restore

This section is applicable only for Windows operating system.

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

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

To logon for the first time after system restore, perform the following actions, depending on which wizard or message screen appears:

- In the **Digital Signature Not Found** panel, click **Yes** or **Continue**.
- In the **Found New Hardware Wizard** panel, click **Cancel**.
- In the **New drivers are installed, do you want to reboot?** panel, click **No**.

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

About restoring NetBackup media servers

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

The following options exist for restoring NetBackup media servers:

- If you back up a media server to a different media server, restore the protected media server as you restore any protected client.
  See "About restoring BMR clients using network boot" on page 93.
  See "About restoring BMR clients using media boot" on page 106.
- A media server can back up its own data using SCSI-attached storage devices or SAN-attached storage devices. If this is true for you, use BMR to restore the media server by first configuring NetBackup to use an alternate media server.

More information is available.

See "About configuring an alternate media server" on page 132.

See "Restoring the media server" on page 134.

About configuring an alternate media server

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

You must do one of the following:

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

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

More information is available.

See "Overriding the original media server manually" on page 134.

See "Enabling automatic media server failover to an alternate server" on page 133.

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

See the NetBackup Web UI Administrator's Guide.

Enabling automatic media server failover to an alternate server

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

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

To enable automatic failover to an alternate server

1. Open the **Restore failover** host properties for the primary server.
2. Add an entry in the **Alternate restore failover machines** list; name the media server and failover restore servers.
3. Stop and restart the NetBackup Request Manager daemon or service on the primary server.

Overriding the original media server manually

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

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

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

To override the original server for manual restores

1. Open the **General server** host properties for the primary server.
2. Add an entry in the **Media host override** list; name the original backup server and the restore server.
3. Stop and restart the NetBackup Request Manager daemon or service on the master server.

Restoring the media server

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

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

Table 6-10 Restore media server process

Step	Task	Procedure
Step 1	Create a restore configuration.	See "Copying a configuration" on page 155.
Step 2	Add an alternate media server as a host.	See "Modifying a configuration" on page 159. See "Hosts properties" on page 166.
Step 3	After you create and modify the restore configuration, perform a standard restore.	See "About restoring BMR clients using network boot" on page 93. See "About restoring BMR clients using media boot" on page 106.

About restoring BMR boot servers

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

If a boot server is installed on the same system as the NetBackup master server, you cannot protect it as a BMR client. You can recover the NetBackup catalogs (which include the BMR databases) on the NetBackup master server. However, you must reinstall the NetBackup and BMR software on the master server.

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

About restoring AWS RHEL and Windows VM clients

Bare Metal Recovery (BMR) facilitates the backup and recovery of AWS virtual machines running on the RHEL and Windows operating system platform.

For more details about BMR supported RHEL and Windows OS platform, refer to the BMR SCL.

This feature is particularly useful in AWS Local Zones where snapshot functions are not available.

In the NetBackup web UI, a new option is now visible in the configuration for BMR clients running RHEL and Wondows EC2 on AWS virtual machines. This option is Restore to Cloud.

Development requirements

NetBackup primary server can reside either on-premises or on AWS EC2. NetBackup RHEL and / or Windows client(s) and media server must be configured on AWS EC2. NetBackup Snapshot Manager (NBSM) must be installed and configured alongside the NetBackup Primary Server. Additionally, AWS VM(s) intended for protection must already be discovered by NBSM.

BMR backup for AWS RHEL VM

The BMR backup process captures required instance details alongside the standard BMR backup data.

BMR AWS RHEL and Windows VM restore prerequisites

- Restoring an AWS virtual machine backup does not require a Shared Resource Tree (SRT), eliminating the need for a boot server.
- Instead, it requires an Amazon Machine Image (AMI) of the same OS version as the backup. For windows restores, it requires AMI of version Windows 2019 server or later. This AMI must have the NetBackup client installed but without certificates.
- A script available on the download center accepts inputs such as the base AMI and the path to the NetBackup client installer. This script creates the necessary AMI for restoration.
- Additionally, the script requires inputs for a key file (.pem file containing a public-private key pair) and a key name, which are used during the creation of the target virtual machine.

To restore a BMR AWS virtual machine

1. Utilize the instance data collected during the BMR backup and user inputs, a new virtual machine is instantiated from the specified AMI ID.
2. The disks of appropriate size and type, as captured in the BMR backup, are attached to the target virtual machine created in step 1.
3. The NetBackup CA certificate and host certificates are retrieved and installed on the target virtual machine.
4. The restore operation is initiated on the target virtual machine.
5. After completion of the BMR restore on the target virtual machine, the AMI OS boot disk is switched with the restored boot disk from the BMR operation.

Note: Users can select the option **Restore with original IP and hostname**, if the original instance has been deleted, and both the IP address and hostname are available to be assigned to the target virtual machine.

Limitations and considerations

- If the user does not select the **Restore with original IP and hostname** option, the backup of the source virtual machine may be restored with a different IP and hostname. As a result, the restored client will adopt a new identity and will not be configured under any policy.
- The user must configure the restored client in the required policies to ensure protection and backups.

About external procedures

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

The following are the external procedure types:

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

Client-specific procedures take precedence over operating system procedures.

External procedures start only if you do one of the following:

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

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

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

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

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

External procedure points and names

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

`prediscover`	Before discovery of hardware is reported to the BMR server (UNIX clients only).
`preformat`	Before disks are formatted and partitioned. On Windows systems, the preformat takes place after the system drive is formatted but before any nonsystem drives are formatted.
`prerestore`	Before files begin to restore.

`postrestore`	After files are restored.
`first boot`	After the restore is complete and at the first boot of a restored client. On Windows systems, the first boot external procedure operates as the first user to log on after a client is restored.

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

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

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

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

About managing external procedures

Use the `bmrepadm` command to do the following:

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

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

```
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 Reference Guide.

Specifying external procedures

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

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

To specify external procedures,

- Select **Run External Procedures** in a **Prepare To Discover** or **Prepare to Restore Client** dialog box.
  See "Discovering a configuration" on page 156.
  See "Preparing a client for restore" on page 86.
- Alternatively, use the bmrprep command -runep option to specify external procedures.

About external procedure data transfer

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

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

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

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

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

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

- On UNIX and Linux clients: /usr/openv/NetBackup/bin

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

For more information about the `bmrc` command, see the NetBackup Commands Reference Guide.

About interaction with external procedures

UNIX and Linux systems	You can enter commands and interact with an external procedure during restore time. To do so, start the `bmrShell` function from within the external procedure script. The `bmrShell` function allows input from the default console keyboard and outputs to the console monitor. You can also use redirection to send output to the screen from an external procedure by redirecting output to the special device. To do so, use `/dev/console` (as in `echo "Hello World" >> /dev/console`). On UNIX and Linux systems, the `bmrShell` is not available during first boot.
Windows systems	You can enter commands and interact with an external procedure during restore time. To do so, start the Windows command interpreter `cmd` from within the external procedure script. On Windows systems, the limited restore environment may not contain DLLs or the same version of DLLs that were used with the original client system. Use `bmrc` to transfer these DLLs during the restore to the `C:\BMR\WINNT\SYSTEM32` directory. Alternatively, add the location of that DLL to the path environment variable.

External procedure logging examples

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

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

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

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

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

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

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

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

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

The following is the log entry from the previous command:

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

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

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

For more information about the `bmrc` command, see the NetBackup Commands Reference Guide.

External procedure operational states

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

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

Pre-format External Procedure	An external procedure runs during the preformat phase.
Pre-restore External Procedure	An external procedure runs during the prerestore phase.

About external procedure exit codes

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

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

About external procedure error handling

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

For UNIX and Linux restores, the following menu appears:

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

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

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

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

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

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

About external procedure environment variables

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

UNIX and Linux environment variables

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

Table 6-11 UNIX and Linux environment variables

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

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

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

AIX environment variables

```
$BMR_BOSINST_DATA      $MNT
$RC_CONFIG             $ROUTES
```

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

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

HP-UX environment variables

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

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

Solaris environment variables

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

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

Windows environment variables

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

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

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

About SAN (storage area network) support

Bare Metal Restore (BMR) can restore a system that is attached to a Storage Area Network (SAN). On Windows, AIX, Linux, Solaris, and HP-UX systems, if the host bus adapter (HBA) drivers are available, BMR automatically restores the SAN-attached volumes.

Note: During BMR recovery, user can either avail BMR DDR (dissimilar disk restore) support where user may want to restore operating system on the same SAN LUNs to make the machine SAN bootable again or the user can move operating system volumes on local disk so that machine is bootable from the local disk. Same logic is applicable while restoring machine having local disk-based systems. Using DDR, user can map operating system volumes to SAN LUN and can make restored machine SAN bootable.

See "Restoring Solaris SAN-attached volumes if they are left unmapped" on page 147.

See "About SANs and dissimilar system restores on Windows clients" on page 147.

Restoring Solaris SAN-attached volumes if they are left unmapped

The following information applies only to Solaris clients.

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

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

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

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

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

About SANs and dissimilar system restores on Windows clients

The following information applies only to Windows clients.

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

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

More information is available on adding drivers.

See “About adding NIC and MSD drivers” on page 129.

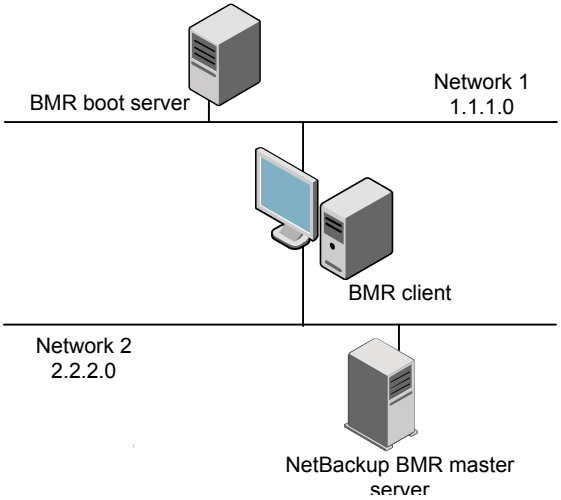
About multiple network interface support

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

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

Figure 6-4 illustrates a configuration that can occur with multihomed clients. For this configuration, specify the network interface for Network 1 when you network boot the client.

Figure 6-4 Simple multihomed example



About client configuration using gateways

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

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

Table 6-12 Network gateways

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

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

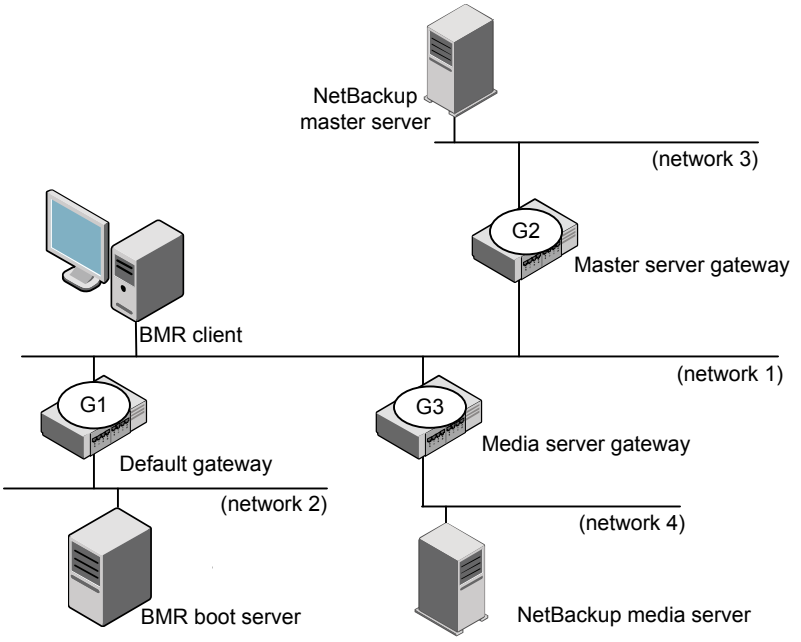
For network boots, specify the following:

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

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

Figure 6-5 shows how gateways can be used during a BMR client restore.

Figure 6-5 Gateway example



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

Port usage during restores

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

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

Table 6-13 Port usage during restores

Service	Port	UNIX	Linux	Windows
`bootp/DHCP`	67, 68	X	X	X
`ping`			X	
`lockd`	Unreserved	X	X	
`mountd`	Unreserved	X	X	
`nfsd`	2049	X	X	
`portmapper`	111	X	X	
`rpcbind`		X (for `bootparam` on Solaris only)		
`statd`	Unreserved	X	X	
`tftp`	69	X	X	X
`vnetd`	13724	X	X	X
`bpcd`	13782	X	X	X
Windows File Sharing	445			X

Chapter 7

Managing Windows drivers packages

This chapter includes the following topics:

About Windows drivers packages

Windows packages are network interface card (NIC) drivers and mass storage device (MSD) drivers. Packages are stored in the BMR database on the NetBackup master server. The packages pool comprises of the packages that are stored in the database. The packages pool is the common pool of packages that can be added to restore configurations.

Packages may be required when you restore to a different system, in which case you add packages to the restore configuration. If the **Packages** window does not contain a driver that is required for a dissimilar system restore, add it to Bare Metal Restore. Do not add it to the restore configuration if a driver is on the Windows installation media that created the SRT.

If a package required for a dissimilar system restore already appears in the **Packages** window, add it to the restore configuration.

See “Client configuration properties” on page 161.

See “Devices and drivers properties” on page 163.

Adding a Windows driver package

Add a package, as follows:

- Use the Driver Package Wizard on any Windows boot server to add a network interface card (NIC) driver or mass storage device (MSD) driver.
- Alternatively, install NetBackup client software on the target system and perform a full BMR backup. The drivers are saved in that client's configuration and available for use during a dissimilar system restore.

Before you can add a package, you must have the installation files for the package. Obtain the files from the vendor's web site, the installation program that is provided with the NIC device or MSD device, or another BMR Windows client in your environment.

Note: You can add only NIC and MSD drivers. All other types of drivers (audio, video, modem, and so on) must be installed on the system after the restore is complete.

See "Finding the correct driver if Windows is already installed" on page 152.

To add a driver package by using the Driver Package Wizard

1. On the **Start** menu on any Windows boot server, click **Programs > Cohesity NetBackup > Bare Metal Restore Boot Server Assistant**.
2. In the Bare Metal Restore Boot Server Assistant, click **Driver Package Wizard**.
3. In the Driver Package Wizard, step through the prompts as follows to add the software package:
   - Path to the installation files for the package
   - Description of the package
   - Version of Windows that the package can be used with
   - The specific driver from the package installation files (installation files may include more than one driver)

Finding the correct driver if Windows is already installed

A driver information file (`.inf` or `txtsetup.oem`) may contain information about more than one driver. Therefore, when you add a mass storage device (MSD) or network interface card (NIC) driver, you may have to select from more than one option.

The devices should be documented in the materials that come with the computer. If not, contact the manufacturer for the driver option.

Alternatively, use the following procedure to determine the correct name for the driver if Windows is installed.

To find the correct driver if Windows is already installed

1. On the computer that contains the mass storage device adapter, open the Windows device manager.
2. Expand the category for the adapter (for example, network adapters).
3. Note the device name that appears here. The option name in the `.inf` file should be the same or similar to this device name.

Deleting a Windows driver package

The following procedure deletes a driver package.

Warning: Do not delete any drivers that are required for a restore.

To delete a Windows driver package

1. In the NetBackup web UI on the NetBackup master server, click **Bare Metal Restore > Resources > Packages**.
2. In the details pane, right-click the driver you want to delete.
3. Select **Delete** on the shortcut menu.
4. In the confirmation panel, click **Yes**.

   The selected package is deleted.

Chapter 8

Managing clients and configurations

This chapter includes the following topics:

About clients and configurations

Logically, a BMR client is a collection of configurations. A configuration is a collection of information about the system to be used as a template to rebuild a protected system.

It includes the following:

- Number of disk drives
- Volume information
- File system information
- Number and type of network adapters
- Network properties

- Drivers
- Other system software components.

Most BMR operations are performed on configurations.

When a BMR protected client is backed up, the configuration of the client is saved and named current. Every time a client is backed up, the new saved configuration replaces the previously saved configuration.

The saved, current configuration is read-only. Use the current configuration to restore the original protected system to its state at the most recent backup (a standard or a self restore).

To restore to a different point in time, to different disks, or to a different system, create a restore configuration by copying a current configuration. Then modify the restore configuration.

Copying a configuration

Copy a configuration so that you can do the following:

- Restore a client to a state that was saved in a backup before the last backup.
  See "About restoring to a specific point in time" on page 119.
- Restore a client in which the disks have changed.
  See "About restoring to dissimilar disks" on page 122.
- Restore a Windows client to a different system.
  See "Restoring to a dissimilar system" on page 127.
- Restore a client to the same hardware but with different network properties.

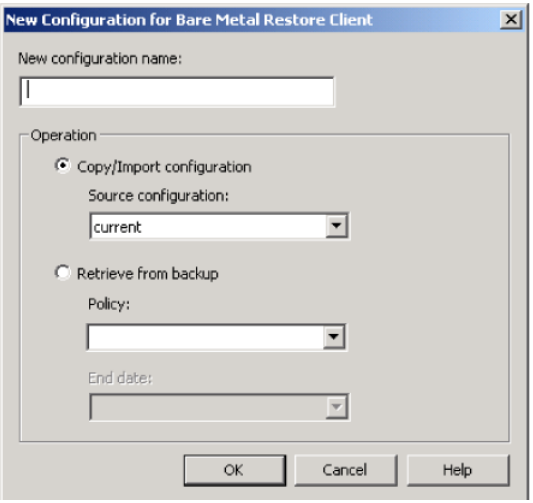
A copied configuration that is used for a restore is called a restore configuration.

After you create the restore configuration, modify it so it matches the target hardware properties.

To copy a configuration

1. In the NetBackup web UI, click **Bare Metal Restore > Hosts > Bare Metal Restore Clients**.
2. In the **All Bare Metal Restore Clients** tree pane, expand the view of the client that contains the configuration you want to copy.
3. Right-click the configuration you want to copy.

4 On the shortcut menu, select **New**.



5 On the **New Configuration for Bare Metal Restore Client** dialog box, complete the fields.

6 Click **OK**.

7 If necessary, modify the configuration.

See "Modifying a configuration" on page 159.

Discovering a configuration

Review the secure communication compatibility matrix for BMR before you proceed with the prepare-to-discover operation.

See "Secure communication compatibility matrices for BMR for NetBackup 8.1.1 and later releases" on page 258.

You can discover the configuration of a new system; the system does not have to be a NetBackup client. A discovered configuration contains the hardware and the software information of a host.

Hardware discovery is mainly required when you recover a client to a different target system than the original. The target system differs from the original in the hardware details like the NIC (network interface card) and disk details. BMR needs to understand those details before restore begins. Therefore user needs to perform hardware discovery of target hardware using BMR prepare-to-discover operation and map original client configuration with the discovered configuration.

When you discover a configuration, BMR adds it to the discovered configurations pool. The elements of the configuration (such as disk layout) can then be used when you perform operations such as dissimilar disk restore.

When the discovery operation ends, the following changes appear on the client, and the configuration appears in the **Discovered Configurations** view:

- AIX clients display B55 on the LED display.
- HP-UX, Linux, and Solaris clients display the following message:
  `The Bare Metal Restore hardware discovery boot has concluded.`
- Windows clients display a pop-up box stating that the discovery is finished and that you can click **OK** to restart the system.

For more information regarding on commands, refer to the *NetBackup Command Reference Guide*

https://support.cohesity.com/s/article/article-100040135

For more information about the automatic recovery or discovery and the host-ID based certificate, refer to the *NetBackup Security and Encryption Guide*.

To discover a configuration using the `bmrprep` command

1. Logon as an administrator.
2. Run the `bpnbat` command.
3. Run the `bmrprep` command to initiate a prepare-to-discover operation.

   When you run the `bmrprep` command, validation checks are performed. These checks pertain to the different parameters such as SRT version, configuration version, etc.

   - If the validation checks for prepare to discover are successful, then the client is marked for automatic discovery. This automatic discovery is by default valid for 48 hours. The primary server authenticity is validated automatically; a host-ID based certificate is automatically issued to this client during the automatic discovery process.
     Use the `nbhostmgmt` command to verify whether the client is marked for automatic discovery.
   - If the validation checks fail, appropriate error messages are displayed. Follow the instructions that are provided in the message.
     For more information, See "Error messages for prepare to restore, prepare to discover, and the `bmrprep` command with reference to secure communication in BMR" on page 207.

The client is ready for discovery.

To discover a configuration using the NetBackup web UI

1. On the left click **Bare Metal Restore > Hosts > Bare Metal Restore clients**
2. Complete the fields and enter data as necessary.

   If you select a client in the **Hosts > Bare Metal Restore Clients** view, the values for that client are included in the dialog box.

   Note: If a client is the target of a dissimilar disk restore (DDR) and VxVM manages the protected client's disks, specify an SRT with VxVM installed.

3. Click **OK**.

   When you click **Prepare to Discover**, validation checks are performed. These checks pertain to the different parameters such as SRT version, configuration version, etc.

   - If the validation checks are successful, then the client is marked for automatic discovery. This automatic discovery is by default valid for 48 hours. The primary server authenticity is validated automatically; a host-ID based certificate is automatically issued to this client during the automatic discovery process.

     The client is ready for discovery.

     Use the `nbhostmgmt` command to verify whether the client is marked for automatic discovery.

     For more information about the automatic recovery or discovery and the host-ID based certificate, refer to the *NetBackup Security and Encryption Guide*
   - If the validation checks fail, appropriate error messages are displayed. Follow the instructions that are provided in the message.

     For more information, See "Error messages for prepare to restore, prepare to discover, and the `bmrprep` command with reference to secure communication in BMR" on page 207.

4. Boot the client to start the hardware discovery operation.

   If you use media boot, when BMR prompts for the client name, enter it as it appears in the **Tasks** view from the prepare-to-discover operation.

   Target system discovery is done automatically and you receive a notification upon discovery completion. Upon successful discovery operation, you can see the discovered configuration with the given name under **Bare Metal Restore Management** > **Resources** > **Discovered Configurations** menu.

Note: If you stop the discovery operation or if the discovery operation fails, either run the prepare-to-discover operation again to restart the automatic discovery or manually set the **Security > Host mappings > Hosts > Menu button > Allow auto reissue certificate** option using the **NetBackup web UI** or command-line interface.

For more information about manually setting the *Allow Auto Reissue Certificate* option, see *Allowing automatic reissue of a certificate* section within the *NetBackup Security and Encryption Guide*

https://support.cohesity.com/s/article/article-100040135

Modifying a configuration

Modify a configuration so you can do the following:

- Restore a client to a state that was saved in a backup before the last backup.
  See "About restoring to a specific point in time" on page 119.
- Restore a client in which the disks have changed.
  See "About restoring to dissimilar disks" on page 122.
- Restore a Windows client to a different system.
  See "Restoring to a dissimilar system" on page 127.
- Restore a client to the same hardware but different network properties.
- Restore a client by skipping intended non-OS data volumes or disks.
- Make client SAN bootable by mapping its OS volumes onto SAN LUNs.

You cannot modify the configuration named current; you must create a configuration you can edit.

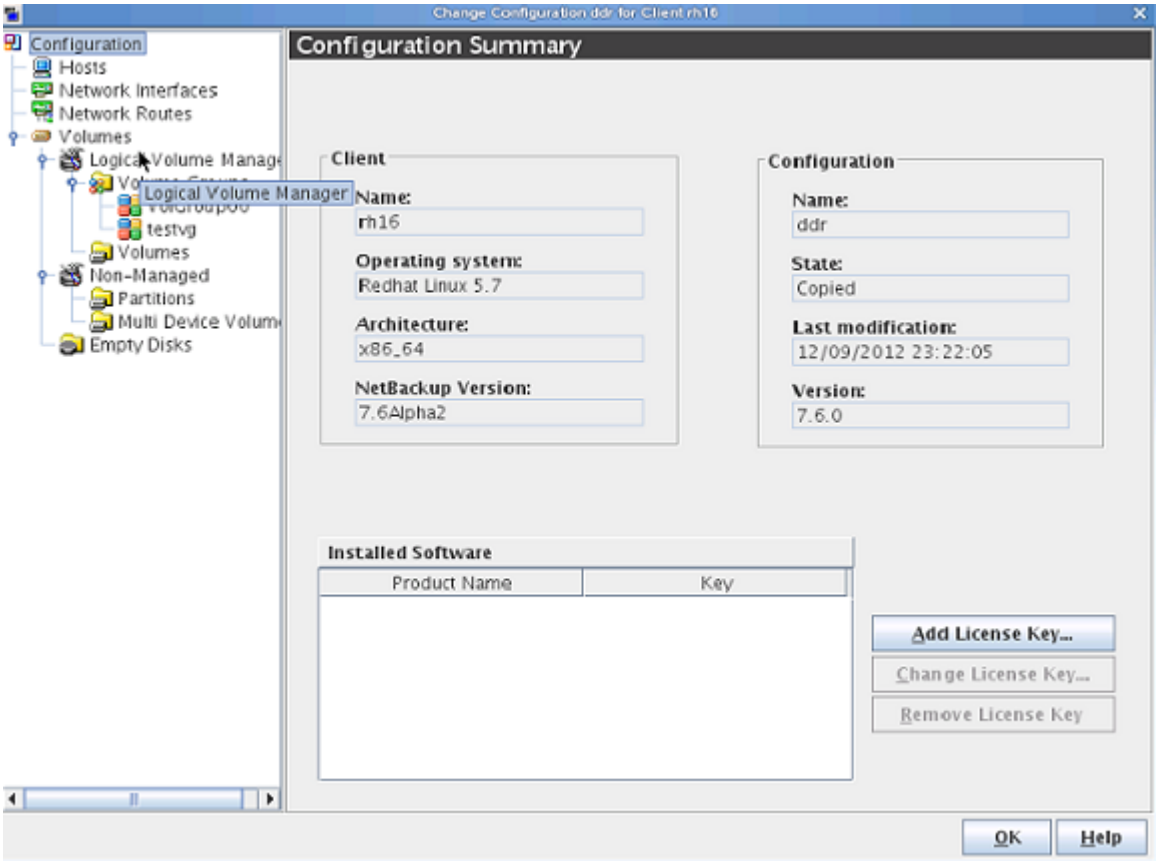
See "Copying a configuration" on page 155.

To modify a configuration

1. In the NetBackup web UI, click **Bare Metal Restore > Hosts > Bare Metal Restore Clients**.
2. In the **All Bare Metal Restore Clients** pane, expand the view of the client that contains the configuration you want to modify.
3. Right-click the configuration you want to modify.
4. On the shortcut menu, select **Change**.
5. In the **Change Configuration** dialog box, modify properties as needed.

   See "Client configuration properties" on page 161.

Figure 8-1 Change Configuration dialog box



Deleting a configuration

You cannot delete a current configuration as it is read-only. Only custom created configurations can be deleted.

To delete a configuration

1. In the NetBackup web UI, click **Bare Metal Restore > Hosts > Bare Metal Restore Clients**.
2. In the **All Bare Metal Restore Clients** pane, expand the view of the client that contains the configuration you want to delete.
3. Right-click the configuration you want to delete.
4. Click **Delete** > **Yes**.

Deleting a client

When you delete a client, it removes only the client and its BMR configurations from the BMR database. It does not remove the NetBackup software on the client, nor remove it from NetBackup, nor delete the backups of the client.

You can delete a client but not remove it from the NetBackup policy that backs it up. If you do, the client is reregistered with BMR the next time it is backed up and appears in the Bare Metal Restore Clients view. (The NetBackup policy that backs it up is the policy that collects BMR information.)

To delete a client

1. In the NetBackup web UI, click **Bare Metal Restore > Hosts > Bare Metal Restore clients**.
2. Right-click the client you want to delete.
3. On the shortcut menu, select **Delete**.
4. In the confirmation dialog box, click **Yes**.

Client configuration properties

Use the **Change Configuration** dialog box to map the attributes of the client configuration on the protected system to the restore configuration. Map the configurations to enable point-in-time restore, dissimilar disk restore, or dissimilar system restore.

The **Change Configuration** dialog box contains multiple property sheets.

See “Configuration Summary properties” on page 161.

See “Devices and drivers properties” on page 163.

See “Hosts properties” on page 166.

See “Network interfaces properties” on page 167.

See “Network routes properties” on page 171.

See “About Volumes properties” on page 173.

Configuration Summary properties

Use **Configuration Summary** property sheet of the **Change Configuration** dialog box to do the following:

- View a summary of the configuration.

- Change a license key for software on the protected system that requires a license key.
- Determine the components of the restore configuration so you can select a shared resource tree that has the appropriate software for the restore.

Figure 8-2 Configuration Summary

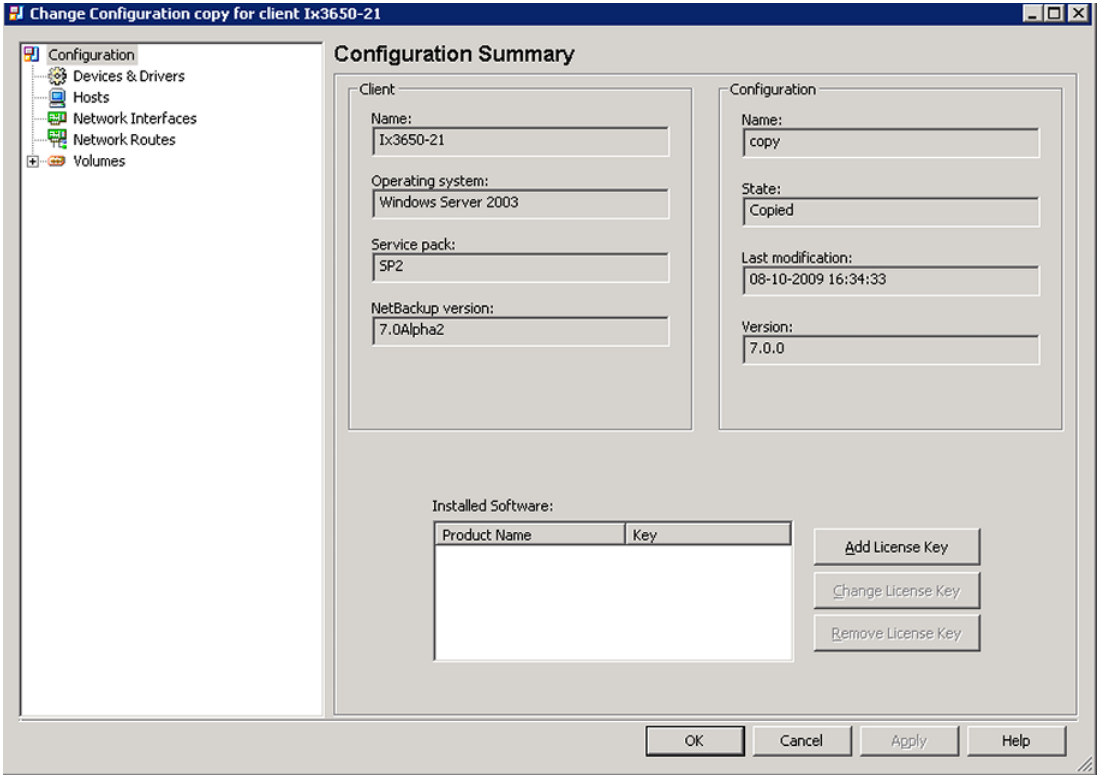


Table 8-1 describes the actions you can initiate regarding license keys.

Table 8-1 License key actions

Action	Description
Add License Key	Opens a dialog box in which you can add the license key for the selected software.
Change License Key	Opens a dialog box in which you can change the license key for the selected software.
Remove License Key	Deletes the selected license key.

Table 8-2 describes the client fields that are displayed in the dialog box.

Table 8-2 Client items

Field	Description
Name	The name of the client.
Operating system	The operating system of the client.
Service pack	(Windows clients only.) The service pack version on the client.
Architecture	(UNIX and Linux clients only.) The architecture of the client.
NetBackup version	The NetBackup software version on the client.
Veritas Volume Manager version	The version of Arctera Volume Manager or Storage Foundation for Windows (if any).

Table 8-3 describes the configuration fields that are displayed in the dialog box.

Table 8-3 Configuration fields

Field	Description
Name	The name of the configuration.
State	The state of the configuration. Saved indicates a configuration that cannot be edited. Copied indicates that the configuration can be edited.
Last modification	The date and time when the configuration was last modified.
Version	The version of the configuration.

Devices and drivers properties

This section is applicable only for the Windows operating system.

The **Devices & Drivers** property sheet applies only to Microsoft Windows clients. The Device Drivers mapping changes are required when a Windows client is restored to a different hardware than the original system, and target hardware has different mass storage device (MSD) drivers or network interface card (NIC).

Use the **Devices & Drivers** property sheet of the **Change Configuration** dialog box to perform the following actions:

- Initialize the devices in this configuration from a new hardware configuration that is discovered or from another client's configuration.

- Automatically select the correct mass storage device (MSD) drivers and network interface card (NIC) drivers for the listed devices.
- Manually add MSD and NIC drivers to the configuration.

You can also specify whether to use only BMR discovered drivers.

Figure 8-3 Devices & Drivers dialog box

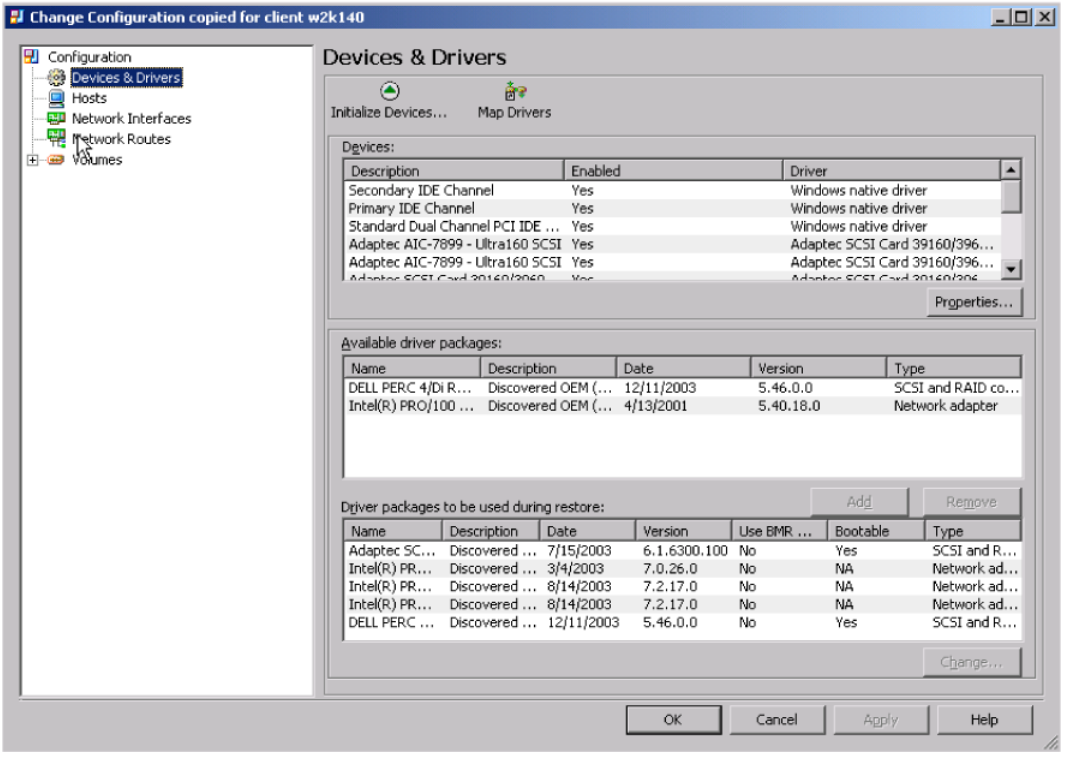


Table 8-4 describes the options available and the actions they initiate.

Table 8-4 Device and driver options

Option	Action
Initialize Devices...	Prompts you for another configuration from which to import the devices. You may select a discovered configuration or one from another client. The initialize operation updates the Drivers packages to be used during restore window to include the necessary drivers for this hardware.

Table 8-4 Device and driver options *(continued)*

Option	Action
Map Drivers	Automatically matches drivers to devices without drivers. If drivers are added to BMR after the last initialize operation, repeat this action. Sometimes, it may be useful to override the driver that is selected automatically by using the **Add** option to select a specific driver manually. Devices without a driver are identified in the **Devices** window by **No matching driver** in the **Enabled** column. These devices are not available during the restore.
Add	Moves the selected driver from the **Available driver packages** window to the **Driver packages to be used during restore** window.
Remove	Moves the selected driver from **Driver packages to be used during restore** window to the **Available driver packages** window.
Change	Lets you change the following attributes of the selected driver: ■ The **Force installation of this driver instead of Windows supplied or newer driver** check box controls whether the selected driver is to be used forcefully. ■ For MSD drivers, the **Bootable driver to be used during text mode portion of the installation** option only applies to Windows legacy restore method. It determines if the driver is used during the installation phase of the Windows legacy restore. It has no effect for a Fast Windows Restore.

Force installation of this driver instead of Windows supplied or newer driver

When BMR saves third-party drivers from a protected system, the driver signing is lost. (Third-party drivers are those that are not part of the Windows distribution.) During the BMR restore, the installation process installs the standard drivers into the temporary repair environment because the drivers from the protected system are unsigned.

You can edit the configuration so that the discovered drivers are forcefully installed onto the temporary repair environment rather than the standard Windows drivers. This option also helps to select particular driver version.

To use discovered Windows drivers during a restore

1. In the **Devices & Drivers** property sheet, select the desired driver from the list of drivers in the bottom window, and click **Change**.
2. Select the **Force installation of this driver instead of Windows supplied or newer driver** check box.
3. Click **OK**.

Hosts properties

Use the **Hosts** property sheet of the **Change Configuration** dialog box to add, remove, or change the attributes of any host that has a role in the restore process.

You can change attributes so you can restore on a network with a different configuration, such as at a disaster recovery site.

Figure 8-4 Hosts property sheet

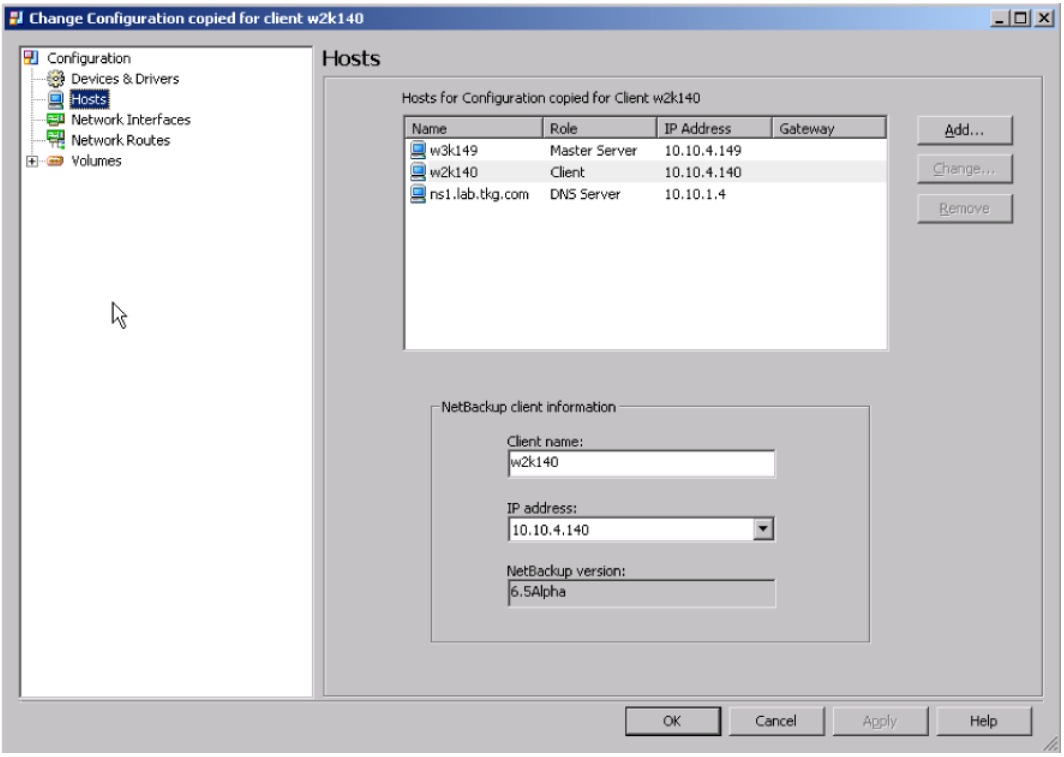


Table 8-5 describes the actions you can initiate from the property sheet.

Table 8-5 Hosts mapping actions

Action	Description
Add	Opens a dialog box in which you can add a new host, specify its role, and enter its IP address and gateway.
Change	Opens a dialog box in which you can change properties for the selected host.
Remove	Removes the selected host. If you don't want to remove the host, click **Cancel** to exit the **Change Configuration** dialog box without applying the changes.

Table 8-6 describes the **Client Information** fields in the **Hosts** property sheet.

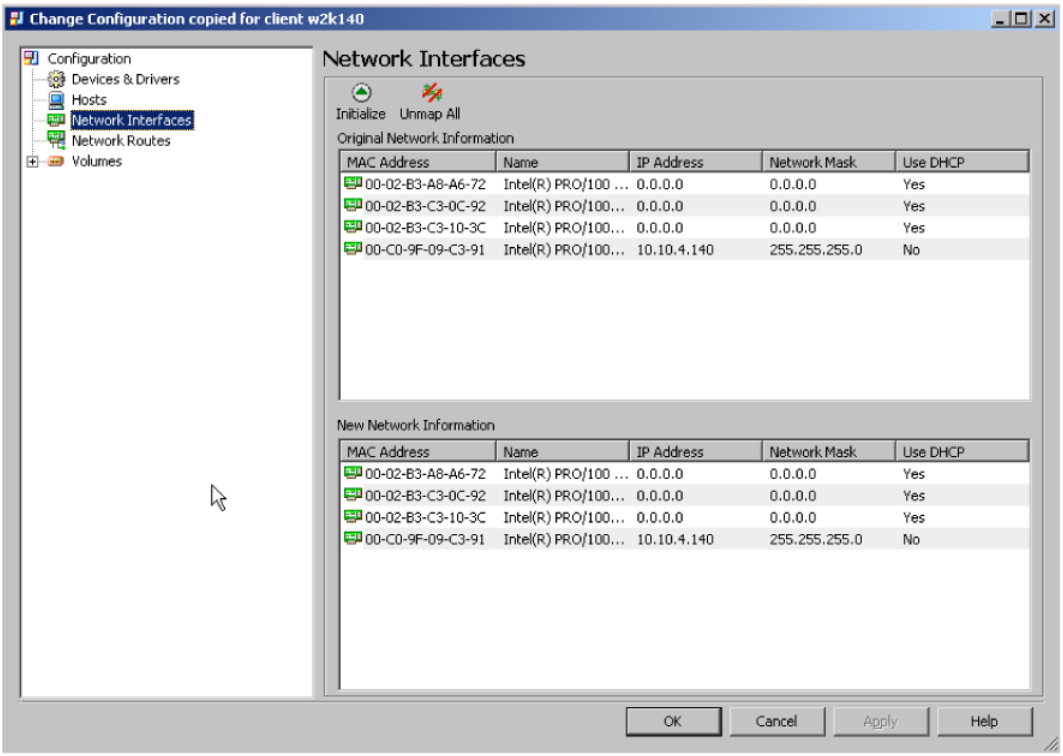
Table 8-6 NetBackup Client Information fields in Hosts dialog box

Field	Description
Client Name	The name by which NetBackup knows the client. The specified client name must match the client name in the NetBackup policy that backs up the client.
IP address	The IP address of the client. All IP addresses defined in the network interfaces are in the drop-down list.
NetBackup version	The NetBackup software version on the client.

Network interfaces properties

Use the **Network Interfaces** property sheet of the **Change Configuration** dialog box to add or remove interfaces or change the network identity that is associated with an interface.

Figure 8-5 Network interfaces property sheet



The **Original Network Information** is read-only. The **New Network Information** shows the values that are used for the restore. If the configuration was not edited, the top panes and bottom panes show the same information.

Table 8-7 describes the actions you can initiate from the dialog box.

Table 8-7 Network interface mapping actions

Action	Description
Initialize	Opens a dialog box from which you can select a configuration to import. Only the hardware information from the configuration is imported, not the network identity. The interfaces from the imported configuration replace the interfaces in the **New Network Information** window.

Table 8-7 Network interface mapping actions *(continued)*

Action	Description
Unmap All	Unmaps all mapped interfaces in the **New Network Information** window and changes all interfaces in the **Original Network Information** window to Unmapped. The unmapping removes the name, IP addresses, network masks, gateways, and DHCP and bootable attributes. MAC addresses are not removed.
Map	Right-click an interface in the **Original Network Information** window and select **Map** from the shortcut menu. In the **Map Interface** dialog box, select an interface in which to map the IP address, netmask, and domain name from the source network card. The MAC address of the original interface is not mapped to the target interface.
Unmap	Right-click an interface in the **New Network Information** window and select **Unmap** from the shortcut menu. The unmapping of an interface removes the name, IP addresses, network masks, and DHCP and bootable attributes. MAC addresses are not removed.
Change	Right-click an interface in the **New Network Information** window and select **Change** from the shortcut menu.

Importing and mapping network interfaces

If you restore to a dissimilar system and you save the target system's configuration by backing up the target system, you can do the following:

- Import the network interface card (NIC) information from the target system into the restore configuration.
- Map the network identify from the NICs in the original configuration to the NICs in the restore configuration.

To import and map interfaces

1. Click **Initialize**.
2. In the **Import configuration** dialog box, select the client configuration to import.
3. Click **OK**.

   The network hardware information is imported into the **New Network Information** window and replaces the interfaces that were in the window. The network identity (IPs, routes, and so on) is not imported.

4 Right-click an interface in the **Original Network Information** window and select **Map** from the shortcut menu.

5 In the **Map or Change Interface** dialog box, select an interface from the **Map to Interface** drop-down list.

6 Click **OK**.

The IP address, netmask, and fully qualified domain name are applied to that interface on the restored system.

Changing network interfaces manually

If you restore to a dissimilar system and do not discover or save the target system's configuration, you can manually change original configuration interface properties for a restore.

You must first determine the MAC addresses of the NICs in the target system.

To change an interface manually

1 Right-click an interface in the **New Network Information** window and select **Change** from the shortcut menu.

2 In the **Map or change interface** dialog box, select **Use DHCP** (if using DHCP). Because this action is an interface change, the dialog box includes the **Hardware MAC Address** field.

Go to step 5.

3 Select a row of attributes in the **Attributes for Network Interface** window and click **Change**.

4 In the **Add Network Identity** dialog box, enter the IP address, netmask, and fully qualified domain name from the interface on the protected system.

Then click **OK**.

5 Enter the hardware MAC address of the NIC in the target system.

6 Click **OK**.

The MAC address and network identity are changed. The name of the interface is not changed, but it does not affect the restore.

Specifying the UNIX and Linux boot interface

UNIX and Linux clients must use a single network interface to boot from and to restore through. The **Bootable** column in the **Network Interfaces** dialog box shows the interface that is configured as the boot interface. If your restore configuration includes more than one network interface, you can specify which one to use for the restore.

Table 8-8 helps you to determine the correct interface.

Table 8-8 Bootable network interfaces

Platform or hardware type	Bootable network interface(s)
AIX	Integrated Ethernet, Ethernet card, or token ring Note the following about the network interfaces on AIX: ■ Only chrp hardware is supported. ■ Booting the RS/6000 from a network adapter requires support in the system firmware.
HP-UX	Integrated Ethernet only
Linux	Any Ethernet device
Solaris	Any Ethernet device

To specify the UNIX and Linux boot interface

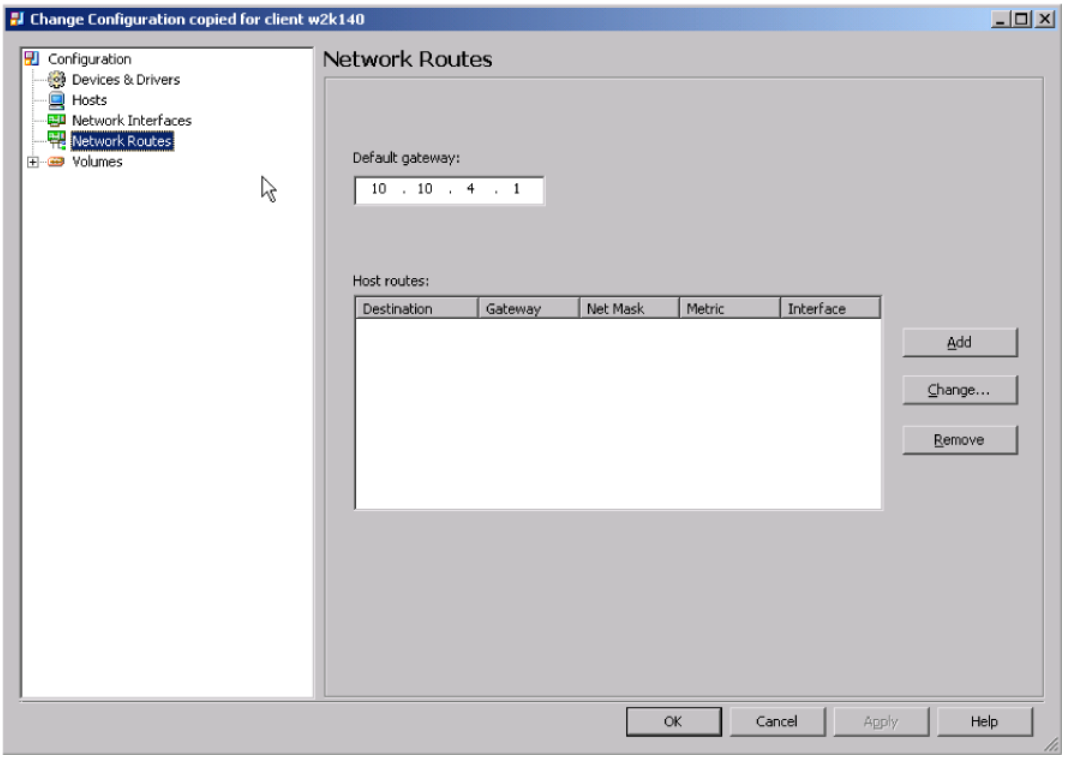
1. In the **New Network Information** window of the **Network Interfaces** property sheet, right-click the interface that you want to use as the boot interface.
2. Select **Change** from the shortcut menu.
3. In the **Map or Change Interface** dialog box, click **Bootable**.
4. Click **OK**.

Note: In case target hardware is booted using different network Interface for recovery than the one shown as Bootable in BMR client configuration, then recovery may fail

Network routes properties

Use the **Network Routes** property sheet of the **Change Configuration** dialog box to add a network route to use during the restore.

Figure 8-6 Network routes property sheet



You may need to add a route if an existing route in the configuration is not sufficient to reach the NetBackup or BMR servers. This situation can occur during disaster recovery at a different location when you move servers from one subnet to another. It also can occur when any routers that intervene are changed.

For example, client 10.10.5.12 and NetBackup master server 10.10.6.23 have a router (10.10.5.254) between them because they are on different subnets. When you prepare to restore, the restore process configures the route to the NetBackup master server as 10.10.5.254, and the restore is successful. However, if the IP address of the router between them changes, the client may not be able to reach the master server. The client cannot reach the server because the configuration does not include the correct route to it. Therefore, you must add a network route to the master server before you perform the prepare-to-restore operation.

BMR attempts to reach hosts in the following order:

- Host routes (specified on the **Hosts** property sheet)
- Network routes that are specified on this property sheet

- The default route that is specified on this property sheet

Table 8-9 describes the fields and options in the property sheet.

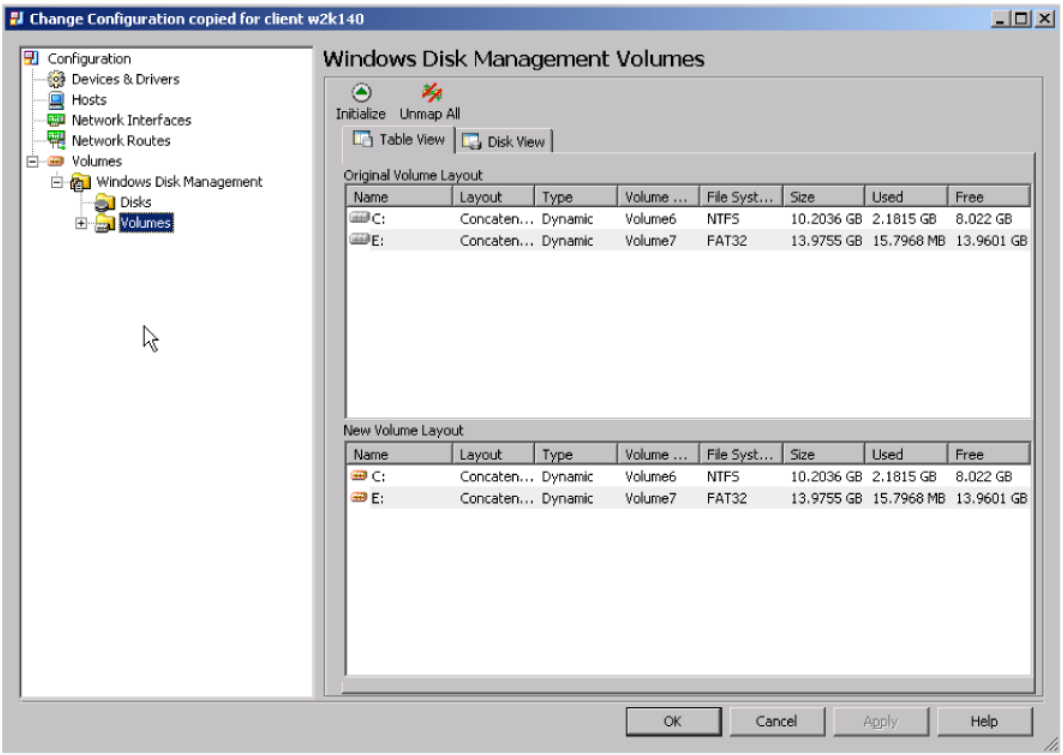
Table 8-9 Network routes mapping fields

Action	Description
Default gateway	The gateway to use if no other route reaches a host.
Add	Opens a dialog box in which you can enter the properties for a new network route.
Change	Opens a dialog box in which you can change the properties for the selected route.
Remove	Removes the selected route.

About Volumes properties

Use the **Volumes** property sheet of the **Change Configuration** dialog box to map the volume configuration from the protected client to the new disks of the restore configuration.

Figure 8-7 Volumes property sheet



You can perform the following operations for mapping volumes and for changing configurations:

- Change the disks that make up a disk group.
- Control the file systems that are restored.
- Control the logical volumes that are created.
- Change the attributes of either a file system, a logical volume, or a disk.
- Restrict a disk to prevent it from being used as a target for mapping.
- Make a discovered disk available for mapping (remove restriction).

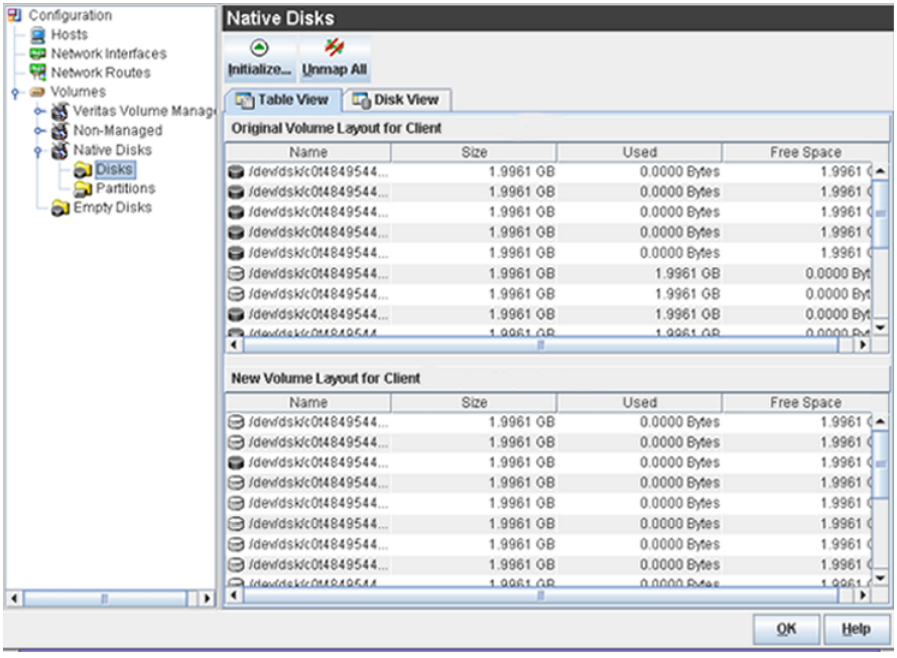
Given enough space on the target disk, you can map all the logical volumes and their file systems. Or you can map specific logical volumes and file systems. You do not have to restore all your logical volumes and file systems.

Primary partitions and simple volumes require only one disk. Striped, mirror, and RAID-5 volumes require multiple disks.

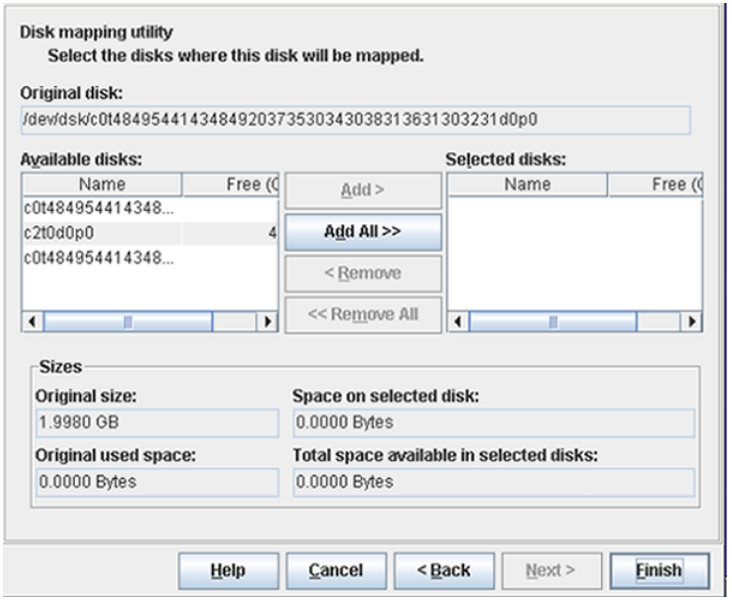
About Native Disk Objects

This section is applicable only for UNIX systems.

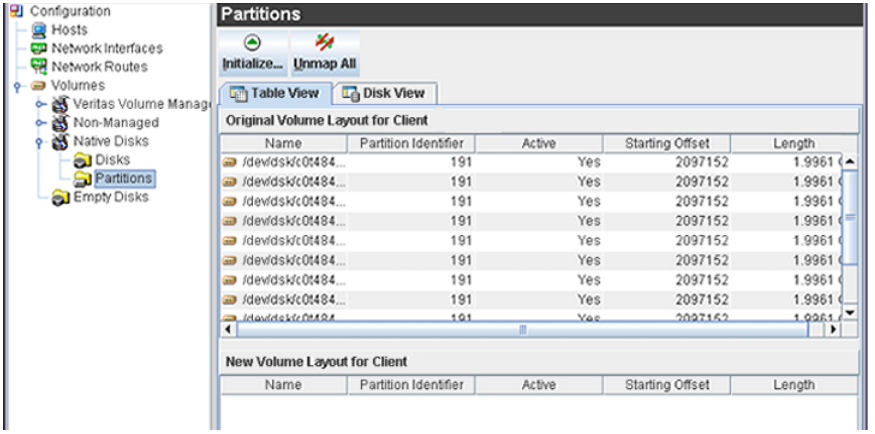
A new **Native Disk** node appears under the **Volumes** node in the **Change Configuration** dialog box. The following example shows information about the Native disks that are available with the total size, used space, and free space.



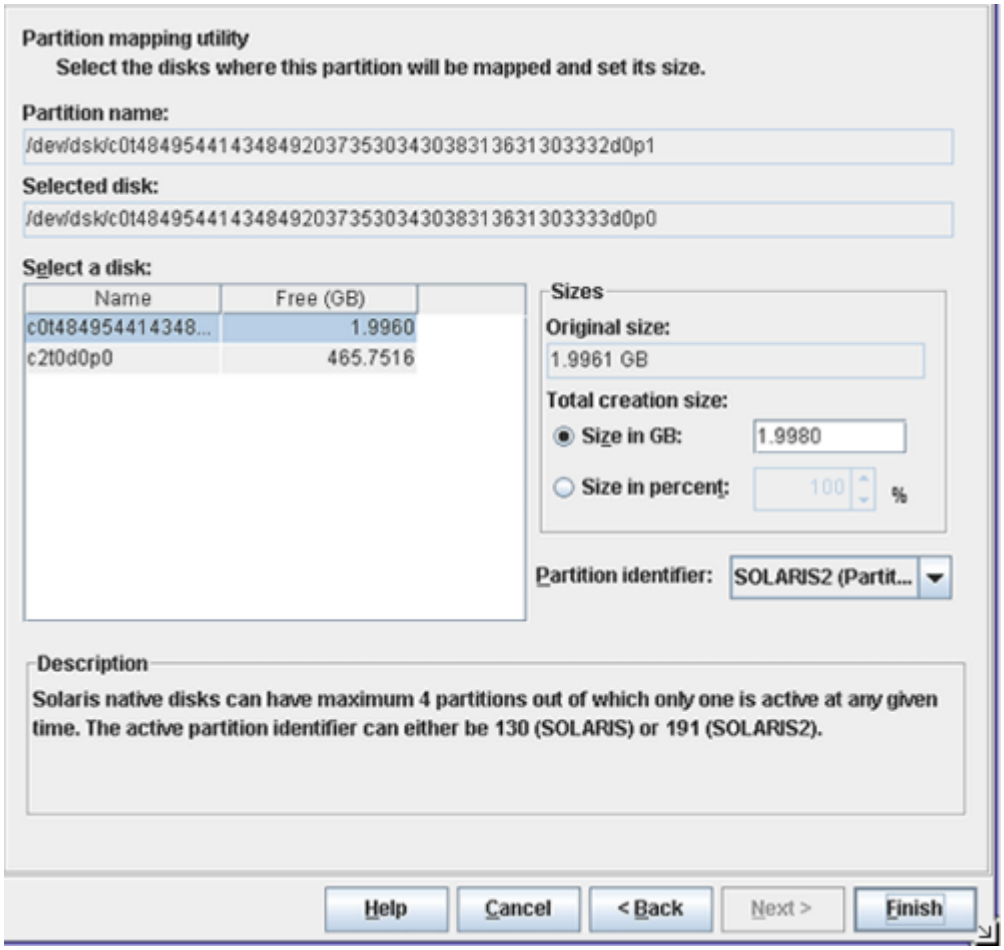
You can map the Solaris Native disk resource by using the disk mapping wizard. To map a disk using the mapping wizard, right-click a volume in the list and click **map**. The following is an example of Disk Mapping Wizard.



A **Partition** node appears under the **Native Disks** node. The following example shows the information regarding the partition name, partition state, partition length (size).



You can map the partition by using the mapping wizard. Right-click the Volume to launch the mapping wizard. You can map the source partition to destination disk and specify the percentage space of the destination disk to use for creating the partition.



About mapping and unmapping volumes

The wizard that appears for mapping volumes depends on what you select to map. These wizards guide you through the mapping process.

The mapping is saved between sessions, so you can stop mapping and then resume later. (If you map during a dissimilar disk restore process and you click **OK** to close the **Change Configuration** dialog box, the DDR restore process continues.)

If an element is mapped or unmapped, all the elements that are contained in it are mapped or unmapped.

The main options are as follows:

Initialize	Opens a dialog box where you can select a configuration to import into the **New Volume Layout** window. Only the disk information from the configuration is imported. Use this option to initialize the configuration with the layout of the new disks so you can begin mapping.
Unmap All	Removes all mapped elements in the **New Volume Layout** and changes all elements in the **Original Volume Layout** window to **Unmapped.**

Note: The mapping wizards do not let you reduce the size of a volume or partition to less than the required space to restore files.

The following notes apply to UNIX and Linux DDR:

- Shared disks in a cluster are marked restricted.
- Unused VxVM disks on Solaris clients are marked restricted.
- You cannot map Linux LVM volume groups with the physical volumes that are created on top of multi-devices with the same configuration. The physical volumes are mapped to either disks or partitions but not a multi device.

The following notes apply to Windows DDR:

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

Table 8-10 describe possible volume mapping actions.

Table 8-10 Volume mapping actions

Action	Description
Initialize	Opens a dialog box from which you can select a configuration to import into the **New Volume Layout** window. Only the disk information from the configuration is imported.
Fast Map	Evaluates the original configuration and maps source disks to disks in the target configuration that have the necessary attributes.
Unmap All	Removes all mapped elements in the target configuration and changes all elements in the original configuration to **Unmapped**.

Table 8-10 Volume mapping actions *(continued)*

Action	Description
Map	Right-click an element in the **Table View of the Original Volume Layout** window and select **Map** from the shortcut menu. The mapping wizard starts for the selected element (except main element Disk Group, Disks, Volumes, Volume Sets, and so on).
Map Volume	Right-click a volume in the **Disk View of the Original Volume Layout** window and select **Map Volume** from the shortcut menu. The mapping wizard starts for the selected element.
Map Volume Group	Right-click a volume group in the **Disk View of the Original Volume Layout** window and select **Map Volume Group** from the shortcut menu. The mapping wizard starts for the selected element.
Map Disk	Right-click a disk in the **Disk View of the Original Volume Layout** window and select **Map Disk** from the shortcut menu. The mapping wizard starts for the selected element.
Map Disk Group	Right-click a disk group in the **Disk View of the Original Volume Layout** window and select **Map Disk Group** from the shortcut menu. The mapping wizard starts for the selected element.
Restrict	(Veritas Cluster Server only.) Right-click an element in the **Original Volume Layout** window and select **Restrict** from the shortcut menu.
Remove Restriction	(Veritas Cluster Server only.) Right-click an element in the **New Volume Layout** window and select **Restrict** from the shortcut menu to map the disk.

Mapping volumes

Use the following procedures to map volumes from the protected client to the restore configuration.

To initiate mapping for individual elements

1. In the **Table View** or **Disk View**, right-click the element in the **Original Volume Layout** window.
2. Choose the appropriate map option on the shortcut menu (the map options are context-sensitive).

   The Mapping Wizard starts with one of the following contexts, as appropriate:

Map	The Mapping Wizard starts for the selected element (except main element disk groups, disks, volumes, volume groups, and so on).
Map Volume	The Volume Mapping Wizard appears.
Map Volume Group	The Volume Group Mapping Wizard appears.
Map Disk	If the element is a disk in a disk group or a volume group, the disk group or volume group wizard appears. Then the volume mapping wizard for each volume appears (the required properties are set). The Disk Mapping Wizard appears if the element is as follows: ■ A disk that is not in a disk group ■ Not part of a volume group (AIX) ■ None of its volumes span other disks (mirrors, stripes). Then all the volumes and the file systems are populated into the target disk. The mapped state is set for both source elements and target elements (disks, volumes, and file systems)
Map Disk Group	The Disk Group Mapping Wizard appears.

To unmap an element

1. In the **Table** View or **Disk** View, right-click the element you want to unmap in the **New Volume Layout** window.
2. Click the unmap option on the shortcut menu. The unmap options are context-sensitive and include **Unmap**, **Unmap Disk**, **Unmap Volume**, and others.

   The element is unmapped, and the values of used and free space change accordingly.

To change the system volume size on Windows

1. In the **Table** View or **Disk** View, right-click the volume in the **New Volume Layout** window.
2. Click **Change Size** on the shortcut menu.
3. In the **Windows System Volume Size Change** dialog box, change the size of the volume.
4. Change the size of the volume.

To restrict a disk or remove restriction

1. In the **Table** View or **Disk** View, right-click the disk in the **New Volume Layout** window.
2. Click either **Restrict** or **Remove Restriction** on the shortcut menu to specify the following:
   - **Restrict** prevents a disk to be used as a target for mapping. Also, it is not formatted, and the volume groups or volumes on it are not created or restored.
   - **Remove Restriction** removes the restriction so the disk can be used as a target. If the disk is mapped, it is formatted and its volumes and volume groups are created and restored.

To promote a disk to dynamic on Windows

1. In the **Table** View or **Disk** View, right-click the disk in the **New Volume Layout** window.
2. Click **Promote to Dynamic** on the shortcut menu.

To add or remove a Windows system mirror

1. If the disk is a basic disk, promote it to a dynamic disk
2. In the **Table** View or **Disk** View, right-click the element in the **New Volume Layout** window.
3. Click either **Add Mirror** or **Remove Mirror** on the shortcut menu.
4. If you add a mirror, in the **Windows Add Mirror to System Volume** dialog box, select the disk to use for the mirror.
5. If you add a mirror, select the disk to use for the mirror.

Volumes views

The tree view (the left pane) shows the elements that are part of the disk layout. The elements in the tree change depending on the operating system of the client and the volume managers that are enabled. The tree view filters the details pane on the right. Select an element to display its attributes in the right pane and to filter other elements so they do not appear in the details pane.

The following indicators show an element's state throughout the mapping process:

Unmapped	The element is not mapped into the new configuration.
Mapped	The element is mapped into the new configuration.

Restricted	The disk is or was shared or manually restricted and cannot be used.

The details pane on the right contains the following views:

- The **Table View** shows the elements in an ordered list.
- The **Disk View** shows how every disk is organized. A colored bar indicates the type of storage layout. For extended partitions, the primary partition color appears in the top color bar and the extended color in a bottom bar. For soft partitions, the top bar shows the underlying volume or slice on which the soft partition was created.
- The **Pool View** shows how every file system and volume of ZFS pool is organized.
- The **Original Volume Layout** (the top window) shows the volume layout and the source elements (disks, disk groups, or volumes) in the original system. The amount of space that is used and the size of the disk appears. To view the properties for an element, right-click the element and select **Properties** on the shortcut menu.
- The **New Volume Layout** (the bottom window) shows the volume layout and elements for the target system. If you initialize the configuration with the layout from a discovered configuration, map elements from the **Original Volume Layout** to the **New Volume Layout**.

The following is the hierarchy for volume information:

- A disk group, volume group, or disk set contains disks.
- A disk contains volumes and partitions.
- A volume or a partition contains file systems.

All volume managers may not use all of these logical concepts. For example, a Solaris slice does not belong to a disk group and has only a file system.

The following tables show the various elements in the tree view and what appears in the **Table View** tab and **Disk View** tab.

Table 8-11 lists details about the selected Windows elements.

Table 8-11 Windows elements

Node	Appears in Table View	Appears in Disk View
Windows Disk Management	Disk and volumes	Not applicable.
Disks	All disks in the system.	All disks in the system.

Table 8-11 Windows elements *(continued)*

Node	Appears in Table View	Appears in Disk View
Volumes	All the volumes that are defined in the system, both managed or unmanaged.	Disks that contain volumes, regardless of which volume manager created them.
One specific volume	Disks that the volume spans.	Disks that the volume spans.

Table 8-12 lists details about the selected Veritas Volume Manager elements.

Table 8-12 Veritas Volume Manager and Storage Foundation for Windows elements

Selected element	Appears in Table View	Appears in Disk View
Veritas Volume Manager	Disk groups, volume sets, and volumes.	Not applicable.
Disk groups	Disk groups in the configuration.	Disks that are part of any disk group.
A specific disk group	Disks that are part of that disk group.	Disks that are part of that disk group.
Volumes	All the volumes that Volume Manager manages.	Disks that contain Volume Manager volumes (ordered by disk group)
A specific volume	Disks that contain that volume.	Disks that contain that volume.

Table 8-13 lists details about the ZFS Manager elements.

Note: BMR can also restore Solaris 10 clients that have ZFS storage pool attached.

Table 8-13 ZFS Manager elements

Selected Element	Appears in Table View	Appears in Pool View	Appears in Disk View
ZFS Manager	Not applicable	Not applicable	Not applicable
ZFS pools	Not applicable	Details of File systems and Volumes on each ZFS Pool	Details of disks associated with each ZFS Pool

Table 8-13 ZFS Manager elements *(continued)*

Selected Element	Appears in Table View	Appears in Pool View	Appears in Disk View
ZFS file systems	Not applicable	Pool space consumption details of each selected ZFS File system	Not applicable
ZFS volumes	Not applicable	Pool space consumption details for each selected ZFS volume	Not applicable

Table 8-14 lists details about the selected Solaris Volume Manager elements.

Table 8-14 Solaris Volume Manager elements

Selected Element	Appears in Table View	Appears in Disk View
Solaris Volume Manager	Disk sets and volumes.	Not applicable.
Disk sets	All named (nonlocal) sets.	Disks that are part of a named (nonlocal) set (ordered by disk set).
A specific disk set	Disks that are part of that disk set.	Disks that are part of that disk set.
Volumes	All SVM volumes.	Disks that have SVM volumes.
A specific volume	Disks that include that volume.	Disks that include that volume.

Table 8-15 lists details about the selected non-managed Solaris elements.

Table 8-15 Non-managed Solaris elements

Selected element	Appears in Table View	Appears in Disk View
Non-managed	Disks and partitions.	Not applicable.
Disks	All disks that VxVM does not manage and all disks that are not in an SVM disk set.	All disks that VxVM does not manage and all disks that are not in an SVM disk set.
Slices	All slices that are not managed and not used as SVM meta devices.	All disks that contain nonmanaged slices.

Table 8-16 lists details about the selected empty disks elements.

Table 8-16 Empty disks elements

Selected element	Appears in Table View	Appears in Disk View
Empty disks	Disks that are not used.	Disks that are not used.

Table 8-17 lists details about the AIX and HP-UX logical volume manager elements.

Table 8-17 AIX and HP-UX logical volume manager elements

Selected Element	Appears in Table View	Appears in Disk View
Logical volume manager	Volume groups and volumes.	Not applicable.
Volume groups	Volume groups in the configuration.	Disks that are part of any volume group (ordered by volume group).
A specific volume group	Disks that are part of that volume group.	Disks that are part of that volume group.
Volumes	All the volumes that the LVM manages.	Disks that have LVM volumes.
A specific volume	Disks that contain that volume.	Disks that contain that volume.

Chapter 9

Managing BMR boot servers

This chapter includes the following topics:

About boot servers

Boot servers provide the environment that is required to rebuild a protected client, including system recovery needed resources such as shared resource trees (SRT). Boot servers also provide the resources that are used to boot the client system when it performs a network boot before restore.

This **temporary operating system environment** known in the NetBackup-BMR language as an SRT or Shared Resource Tree, needs to be created and hosted according to the peculiar requirements of a host's operating system and that of NetBackup-BMR as well. An SRT is a collection of OS files, NetBackup Client Software, and other required software like the Arctera Volume Manager. An SRT is NOT an image of the client and a single SRT can be used for recovering multiple clients. Many of the operations required to be carried out for creation and modification of an SRT are dependent on the target host's operating system. Hence, NetBackup-BMR needs a Boot Server of the same operating system as that of the hosts that are to be recovered.

Boot server software is installed from the NetBackup installation media.

The general deployment including the BMR Boot Server appears as follows:

Refer chapter *Configuring BMR* to understand BMR boot server setup.

Boot server requirements

More information is available about the SRT requirements that are related to boot servers.

See "About boot servers" on page 186.

Table 9-1 Boot server requirements

Type of server	Requirements
General boot server	You must have a boot server for each type of client that you want to protect. For example, a Solaris client requires a Solaris boot server, a Windows client requires a Windows boot server, and so on. For UNIX, Linux, and legacy Windows restores, a boot server at a particular operating system version can only host SRTs of the same operating system version or lower. For example, a Solaris 9 boot server can host Solaris 8 and Solaris 9 SRTs, but not Solaris 10 SRTs. For UNIX, Linux, and legacy Windows restores, a client at a particular operating system version requires an SRT of the same operating system version. Refer appendix *Network services configurations on BMR Boot Server* to know details about network-based recovery pre-requisite setup for different platforms.
AIX boot server	AIX boot servers do not have any special requirements. An AIX boot server can reside on the same subnet as the subnet of the client, or on a different subnet. However, AIX boot servers at a specific operating system version can only host SRTs of the same or earlier operating system version. For example, a 5.3.0.10 boot server can only host 5.1.x.x, 5.2.x.x, 5.3.0.0, and 5.3.0.10 SRTs, but not 5.3.0.20 SRTs. Likewise, a 5.2.x.x boot server cannot host 5.3.x.x SRTs. Also, to recover 5.3.0.10 client, you need to create 5.3.0.10 SRT. You cannot use 5.3.0.11 or 6.1.0.1 SRT to recover this client.
HP-UX boot server	Each network segment with HP-UX clients must have an HP-UX boot server that can support the clients. On an HP-UX boot server, the Ignite version of an SRT must match the Ignite version that is installed on the boot server.

Table 9-1 Boot server requirements *(continued)*

Type of server	Requirements
Linux boot server	Each network segment that has Linux clients must have a Linux boot server. Though in case of VLAN (Virtual Local Area Network) setup case, you can configure your switch settings to route network boot requests packets to the server located at other VLAN than where client exists. This way a single Linux boot server can recover Linux clients belonging to different VLANs.

Table 9-1 Boot server requirements *(continued)*

Type of server	Requirements
Solaris boot server	

Table 9-1 Boot server requirements *(continued)*

Type of server	Requirements
	Each network segment with Solaris clients must have a Solaris BMR boot server that can support the clients. However, you can use the following to minimize the effect of this requirement: ■ When necessary, you can install BMR boot server software on a Solaris computer in the network segment. Then create an SRT after the client has failed and needs to be restored. ■ The Solaris BMR boot server can be defined on a Solaris computer that has a physical IP presence on multiple networks. That is, you can use a single Solaris BMR boot server with multiple network interfaces for Solaris BMR clients on each network segment. ■ Configure a relay boot server to allow Solaris computers on remote subnets to boot from a BMR boot server using a network gateway. ■ You can contact support representative to get more information. ■ The BMR boot server for Solaris10_x64 requires the following software installed: ■ TFTP Server ■ DHCP server ■ NFS Server ■ **SRTs** for carrying out a bare metal restore of a Solaris10_x64 client can only be created and hosted on a Solaris10_x64 Boot server. The OS and Kernel level should be greater than or the same of the client to be restored. ■ The minimum Solaris 11 OS for BMR boot server is Solaris 11.3 SRU 20. ■ For SRT creation on Solaris 11.3 SRU 20+ boot server, you need to set the following repositories and their publishers on boot server: ■ solarisstudio (Oracle Solaris/Developer Studio 12.6. For more information about Solaris Developer Studio, refer http://support.oracle.com ■ solaris (Solaris repository version must be equal to or greater than Solaris 11.3 AI SRU version to be used for SRT creation. For more information

Table 9-1 Boot server requirements *(continued)*

Type of server	Requirements
	about Solaris 11 SRU, Repositories and AI image downloads, refer https://support.oracle.com If you want to use `bmrsrtadm` Media Creation to generate BMR-ISO SRTs, you must install the SUNWmkcd package on the boot server.
Windows boot server	Windows boot server requirements are as follows: ■ The network boot services on the boot server require a DHCP server somewhere on the network. ■ The boot server must not run a PXE service or a TFTP service.

Chapter 10

Troubleshooting

This chapter includes the following topics:

Problems booting from CD or DVD

AIX, Linux, and Solaris platforms use a common bootable CD or DVD format (ISO-9660). HP-UX uses Logical Interchange Format (LIF). If a system cannot boot from the CD or DVD, place it in a system that has a CD drive and examine the contents. (Either UNIX or Windows platforms can read ISO format.)

Do the following:

- If the CD or DVD contents consist of a single file, the CD or DVD was written as a data CD or DVD instead of an ISO-9660 CD or DVD image. Repeat the burning procedure but use the options that are required to burn an ISO image file.
- If the CD or DVD is blank or unreadable, remove it from the drive and examine it closely to determine if it has been written to. Some CD or DVD burning software by default simulates the burning of a CD or DVD to test the capabilities of the CD or DVD burning hardware. It does not burn the CD or DVD until the test-only option is turned off. Repeat the burning procedure with the test-only option disabled.
- If the boot was partially successful, or if it appears that some files are not present or some are corrupted, then one of the following occurred:
  - The burning process failed. A partially burned CD may be bootable but may not contain significant portions of its content. Lower the CD writing speed to allow a successful burn. Use the test after writing or use the option to verify that some CD writing software offers may help detect unsuccessful CD writes.
  - The file transfer from the BMR boot server to the computer with the CD writer failed.
    A common cause of corruption occurs when the file is transferred with FTP in ASCII transfer mode rather than binary mode.
- If the CD boots successfully on another similar computer, the drive on the restore system may be damaged or dirty. Similarly, the CD itself may be easily damaged or made unreadable by surface contamination after writing. Examine the physical media and the environment in which it is read.
- Verify that you use the correct procedures to boot the client computer from CD.
- Try booting the client from the installation media to ensure that the computer does not have a hardware problem when it boots from the CD.

Long restore times

If a restore takes an unusually long time (for example 20 hours instead of 2 hours), the media speed between the adapter and the switch or hub where it connects may not match. For example, the media speed is set to 100 MB full duplex, but the restore slows down because the hub uses half duplex. Change the media speed to match the hub speed or switch speed, or change the hub-switch setting to match that of the client.

Solaris media boot network parameters issue

In a media boot of a Solaris client, the Solaris code polls the local subnet. The code polls to determine if any computer on the local subnet has a record of the network parameters for the booting client. If a JumpStart server has network parameters for the client in the `/etc/ethers` or `/etc/bootparams` file, those parameters are used for the boot process. The parameters are used even if they are different than the network parameters for the boot interface that are configured in BMR.

If network parameters for the client exist, the restore may fail.

To work around this issue, do one of the following:

- Remove all references to the client system from the following files in all other computers in the subnet of the client:

```
/etc/ethers file
/etc/bootparams
```

- Unplug the booting client from the network until the media boot configures the network parameters for the restore.

How to recover client when BMR configuration is deleted accidentally

If you delete a client and its current configuration, the next time the client is backed up, its configuration is saved. The client appears again in the **Bare Metal Restore Clients** view.

If the client and configuration are deleted after a client fails (before it is restored), use the `bmrs` command to retrieve the client's previous configuration. (You cannot perform a point in time restore because a deleted client does not appear in the **Bare Metal Restore Clients** view.)

The following is the format of the `bmrs` command to use on the master server:

```
bmrs -resource config -operation retrieve -client clientName
-destination newConfigname -enddate dateFormat -policy policyName
```

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

First boot after BMR restore fails on UNIX platforms

After BMR restore, first boot may fail at Grub if root disk that is originally mirrored across two disks is changed to concatenate layout. In the system setup, root disk was mirrored across 2 disks say c3t0d0 and c4t0d0. In BIOS settings, c3t0d0 is the first disk in boot sequence. During DDR configuration, root disk is changed from mirror to concatenate and mapped on c4t0d0. In BIOS, this disk is the second disk in boot sequence. So, after BMR restore, when system boots for the first time, as c3t0d0 is the first disk in boot sequence AND as "grub signature is still present on this disk as it was mirrored earlier", system tries to boot from the grub on c3t0d0 and then fails to boot as it does not get root file system and other bootable files which are now on c4t0d0.

After BMR restore, during system boot, change the BIOS settings and choose the correct disk for system to boot.

Client network based boot issue

Different operating systems use different network protocols for network boot. BMR leverages this protocol/s for starting network-based client recovery. For example, Windows, Linux and Solaris-x86 uses PXE based network boot which comprises DHCP, TFTP protocols.

In case of,

Windows: BMR has PXE and TFTP services running on the BMR boot server. DHCP can be any server in the same subnet.

Linux: DHCP, TFTP services needs to be running on the boot server providing client network boot. (Note: Once services are deployed and running on boot server; BMR automatically register/de-register them to enable client network boot.) Sometimes it happens that in the same subnet where client recovery is being done has multiple network boot protocol servers running. One of them is correct PXE/DHCP/bootp servers which can assign IP_address to BMR client upon network boot. In such environment when client boots over network for BMR recovery, its network boot request gets broadcasted and it can be reached to unintended network boot server (PXE/DHCP/BOOTP) first. In such case it can return failure and BMR recovery may fail.

So ensure that no other network boot services except the valid one providing BMR client network boot is running in the same subnet. Note that this is limitation with PXE, DHCP, BOOTP boot protocols themselves where first DHCP reply failure stops network boot process.

Verify backup failure while recovering Windows client

During the Bare Metal Restore (BMR) restore process, the restoring client will attempt to verify that it has a valid backup image to complete the restore. This validation process is failing. The probable causes are:

- The backup images have expired.
- The client was backed up with the wrong policy type. As an example, a Windows client was backed up with a UNIX Standard policy.
- The backup image is missing critical files required for a proper system restore.
- The client is not authorized to perform list or restore operations on the master server.
- The restore configuration that was used for the restore has invalid or missing networking information.
- The NetBackup primary server is not able to perform proper reverse lookup of the client.

The best methodology for debugging this error message involves the following steps:

1. Perform a Prepare-to-restore operation from the NetBackup web UI or from the command line. If an error is encountered, then one of the below listed causes is at fault. Use normal NetBackup catalog query information to verify that a backup image is available using the correct policy type. Also, verify that the System State/ Shadow Copy Components were backed up properly. Also verify that the Bare Metal Restore software directory on the client was also backed up. If the Prepare To Restore operation is successful, the backup image information is valid. This in turn points to a problem in the BMR restore environment on the client or a network setting on the master server. Items that need to be verified as good in the restore configuration:
    - Check the 'Network Interfaces' section and ensure that the MAC address is correct and is the one being used during the restore. Verify that a network cable is attached to correct port on both the client NIC and the switch.
    - Check the "Hosts" section and verify that valid entries (host name and ip-address) exist for the NetBackup primary server and media server, as required.

- Look in the bmrrst log on the master server to see the progress of the restore. To determine the root cause on the restoring client:

2. Cancel and exit from the restore wizard. This should place you in the main menu.
3. Move the mouse to a location in the upper left-hand corner of the main screen, near the gear shaped icon. When the mouse pointer changes from an arrow to a hand, right-click the mouse. This opens a command-line window.
4. Change directory to `X:\BMR\NBU\bin`.
5. Execute the command,

   ```
   bpclimagelist -client $CLNT_NAME -T echo %ERRORLEVEL%
   ```

   The 'echo' command displays the return code of the command. The `bpclimagelist` command will fail to gather catalog backup image information for the following reasons:

   - Could not contact the master server (rc=25). This happens if the client has connected on the wrong interface port or has an invalid or incomplete host name and ip-address information for the master server. The fact that the client could initially access the client configuration is not relevant. At the time of the failure, the client network interfaces were modified to match what was in the restore configuration specified for the restore. The values entered on the first input page have been modified to match the configuration values.
   - The master server could not respond back to the client port (rc=23). Possible causes are missing client reverse lookup information, either in the Server's DNS entries or hosts file or invalid routing back to the client
   - The master server does not see the restoring client as a valid client (rc=131, 133, 135). The ip-address used by the client resolved to a different name than in the configuration, or the client does not have permission to perform list/restore requests. One way to resolve this is to place a temporary entry in the 'hosts' file of the master server and media server. This entry must match the data information found'Network Interfaces' section of the restore configuration used for the restore. Also check the **Host properties > Client attributes > select the Allow client restore** of the NetBackup web UI to ensure that the client has permissions to perform list and restore operations
   - The NetBackup primary server does not have a valid backup image (rc=227).

As a general rule, all BMR restores should make use of fixed ip-address information and not make use of DHCP or DNS during the restore. This can be reset after the BMR restore has completed, if so desired.

The VM takes long time for booting after BMR Physical backup conversion to virtual machine is performed on 32-bit architecture Windows OS

During VM boot up time, post-login, Windows pops up **New Hardware Found and Configuration** window. It prompts to configure device driver for SAS Controller - Base System Device. This windows dialog gives two options for new device configuration, which are, **Auto search and configure** and **Skip prompting for these devices.** If you select any one of these options then Windows makes error in SAS controller VMWare PVSCI device driver configuration. Due to this problem next boot may result in BSOD.

Do not take any action for the **New hardware configuration** dialog. Close this dialog window by using the Window cross button. You can ignore this dialog. This process may need to be done every time during VM boot up.

BMR-enabled physical backup to Virtual Machine conversion job fails on Windows platform

This issue shows job failure with error code 12. This means that the Virtual Instance Converter or NetBackup recovery host fails to mount file systems on the created VM.

Restart NetBackup recovery host so that VMWare mounter service gets registered correctly and then get started. It is always recommended to reboot NB Recovery host once upon NB Client installation.

Troubleshooting issues regarding creation of virtual machine from client backup

Following sections provide details about the troubleshooting steps that you might use while using the feature **Direct Virtual Machine creation from client backup**.

Client name is not visible under virtual machine conversion clients list

To debug the cause, follow these steps:

1. Check whether the client BMR backup is successful. See “Pre-requisites to create VM from backup ” on page 220.
2. Refer `bmrd` and `bmrsavcfg` logs to get more details about the failure.
3. If BMR backup is successful, check whether the client hostname is enlisted under the tab **Bare Metal Restore Clients.** If the client hostname is enlisted under **Bare Metal Clients** list, but not under **VM conversion Clients** list, refer the support matrix to validate whether the client meets the specified criteria. Refer Table 10-1 for logs location.

Failure during submitting the job of virtual machine creation

To find the reason for failure of job of virtual machine creation, follow these steps:

- On UI wizard window, if the intended NetBackup Recovery Host (Virtual Instance Convertor) is not visible under **Recovery Host** drop-down list, make sure that the Virtual Instance Convertor (VIC) is registered with the NetBackup primary server.
  See “Pre-requisites to create VM from backup ” on page 220.
- On UI wizard window, if you are not able to view the intended Hypervisor (vCenter or ESX) Server, follow these steps:
  - If your intended server is vCenter server or a standalone ESX server, make sure that it is registered with the master server.
    See “Pre-requisites to create VM from backup ” on page 220.
  - If Hypervisor is already registered, validate its connectivity with VIC as follows:
    - Open the target Hypervisor entry under the node **Media and Device Management** > **Credentials** > **Virtual Machine Servers**.
    - Select the intended recovery host under the tab **For Backup Host**.
    - Click **OK**.

    Completing the process will validate the connectivity of Hypervisor server through the selected NetBackup recovery host.
- If you are not able to view the datastores or resource pool/vApp or folder of hypervisor, check the connectivity of the Hypervisor as mentioned earlier in this section. If connectivity exists, but you are still not able to get the entries, refer the `bpVMutil` and `bpVMreq` logs with verbose level 6. Refer Table 10-1 for logs location.

Job of creating virtual machine failed

To refer the error codes, See "Monitoring VM Creation jobs" on page 239. Check the `bmrb2v`, `bmrb2vrst` and `bmrd` logs with verbose level 6. Refer Table 10-1 for logs location.

Table 10-1

Component	Log directory	Resides on
bpVMutil	install_path\NetBackup\logs\bpVMutil	Virtual Instance Convertor Recovery Host
bpVMreq	install_path\NetBackup\logs\bpVMreq	Master server from where conversion job is submitted.
bmrb2v	install_path\NetBackup\logs\bmrb2v	Master server from where conversion job is submitted.
bmrb2vrst	install_path\NetBackup\logs\bmrb2vrst	Virtual Instance Convertor Recovery Host
bmrd	install_path\NetBackup\logs\bmrd	Master server from where conversion job is submitted.
bmrsavcfg	install_path\NetBackup\logs\bmrsavcfg	Client whose BMR backup is taken.

Many services on Solaris 11 and newer print warning messages during a system boot and during BMR first boot

After a BMR restore during first boot on Solaris 11 and newer, error messages that are related to several services are seen.

Many services (such as `sendmail`) print warning messages during a system boot and during BMR first boot, such as:

```
sendmail/filesys_update failed
```

These messages are also seen during normal operating system installation on the system and therefore can be ignored.

Another set of messages that is seen on the console during BMR first boot are related to `zpool` and the Solaris Zones reconfiguration. All of these messages are harmless and have no effect on System Restore, and the zpools and the zones coming to the correct state

These messages come from SMF services and have no effect on system recovery.

Solaris Zone recovery on Solaris 11 and newer takes time to reconfigure after a BMR restore during first boot

During first boot after a Bare Metal Restore (BMR) restore operation, BMR reconfigures the zones using detach-attach commands. These commands may take some time to run if there are a large number of zones that need to be configured. After the BMR first boot command execution completes, the zpool, zones, and ZFS configurations may take some time to settle down with the new configuration.

Wait about 10 minutes after first boot (more depending on the number of zones) so that the system returns to the correct configuration state. You should not restart the system or log into any zones until that time to ensure a complete recovery.

A Solaris BMR restore operation fails if the text-installer package is not present in the customized AI ISO

A Solaris Bare Metal Restore (BMR) restore operation fails if the text-installer package is not present in the customized Automated Installer (AI) ISO that was created using the distribution constructor.

For shared resource tree (SRT) creation, if you use a customized AI ISO that was created using distribution constructor, then the text-installer package should not be removed from the AI manifest file.

For Solaris x86, this text-installer package is mandatory because the BMR restore makes use of a file from that package.

The /boot partition must be on a separate partition for a multiple device-based OS configuration

If the client is configured as root (`/`) under a multi-device, then for a successful BMR restore, the `/boot` partition must be on a separate partition. That means, if `/` and `/boot` are on the same partition, they are not supported for a multiple device-based OS configuration.

Multiple error messages might be displayed during the first boot after the restoration of a client with ZFS storage pools

During the first boot after the restoration of a client with ZFS storage pools, multiple error messages might be displayed. The following is an example:

```
SUNW-MSG-ID: ZFS-8000-D3, TYPE: Fault, VER: 1, SEVERITY: Major
EVENT-TIME: Mon May 23 13:10:09 CDT 2011
PLATFORM: SUNW,Sun-Fire-V215, CSN: -, HOSTNAME: bmrsol101.vxindia.veritas.com
SOURCE: zfs-diagnosis, REV: 1.0
EVENT-ID: c257eb38-495e-cdb6-9a52-a4d9c2ae38be
DESC: A ZFS device failed.  Refer to http://sun.com/msg/ZFS-8000-D3 for more information.
AUTO-RESPONSE: No automated response will occur.
IMPACT: Fault tolerance of the pool may be compromised.
REC-ACTION: Run 'zpool status -x' and replace the bad device.
```

For each disk in the computer you may see the error message. However, when you log on and run the `zpool status -x` command, you see the following message:

```
all pools are healthy
```

That is because of the ZFS import operation that is done during the first boot sequence. Bare Metal Restore (BMR) restores storage pools and contents in the BMR restoration environment and later imports to the client environment during first boot. That can cause an error message or a warning message during the first boot operation.

These messages only occur during the first boot operation and you can safely ignore them.

BMR may not format or clear the ZFS metadata

If you opt for the creation of a ZFS storage pool on small number of disks during a dissimilar disk restore (DDR), Bare Metal Restore (BMR) does not format or clear the ZFS metadata on the disks that remain. Because of that, if you attempt to use those disks to create other storage pools, you may see an error message that states a disk is in use under the ZFS storage pool.

To work around this issue, use the `-f` option to create a new storage pool on those disks.

Specifying the short name of the client to protect with Auto Image Replication and BMR

You must specify the short name of the client when you install NetBackup client packages on the computer that you want to protect with Auto Image Replication and Bare Metal Restore (BMR). You must also specify the short name of the client in the backup policy that you created on the primary domain. That policy backs up all of the client's local drives and gathers the client configuration that BMR requires. The DNS of the secondary or the tertiary domain cannot resolve the fully qualified name during a BMR recovery of that client at the disaster recovery site.

A restore task may remain in a finalized state in the disaster recovery domain even after the client restores successfully

In the case of a dissimilar domain restore where the primary and the disaster recovery domain names are different, the restore task remains in a finalized state in the disaster recovery domain even after the client restores successfully. The Bare Metal Restore (BMR) restore is successful in the disaster recovery domain and only the restore task update fails.

The update fails because of an invalid network configuration in the client. This behavior is expected because the restore does not modify the configuration files that are related to the DNS of the disaster recovery domain.

You must manually modify the following network configuration files to back up and restore the client in a disaster recovery domain:

- Solaris:
  - `/etc/hosts`
  - `/etc/resolv.conf`
  - `/etc/nodename`
  - `/etc/bge0.hostname`
- AIX:
  Use `smitty` to modify the network configuration.
- HP-UX:
  Use the HP System Management home page (SMH) to modify network configuration.
- Linux:
  `/etc/hosts`

```
/etc/resolv.conf
/etc/sysconfig/network-scripts/ifcfg-eth*
```

- Windows:

  See the following URLs to modify the domain name in Windows:

  - http://windows.microsoft.com/en-US/windows7/Connect-your-computer-to-a-domain
  - http://support.microsoft.com/kb/295017

After the restore process is complete, you can see some error message displayed. For more information, refer https://support.cohesity.com/s/article/article-100021764

Communication between the master server and the client may fail even if the client has a valid host ID-based certificate

This issue is observed primarily in the Dissimilar System Restore (DSR) on Windows platform.

This issue may occur due to a failure in the **Network Settings** during the cleanup operation in the first boot.

The issue may persist even after you have corrected or updated the **Network Settings** communication manually.

Workaround: To resolve this issue, perform the following steps:

1. Navigate to the path on your target client system which has NetBackup installed.

   For Example:

   ```
   c:\program files\veritas\netbackup\bin
   ```

2. Run the following command: `nbcertcmd -getcrl`

Automatic boot may fail for HP-UX after a restore

Sometimes after a Bare Metal Restore (BMR) restore and during the first boot of the client computer, the operating system automatic boot may fail. The HP BIOS then fails to identify the boot drive.

To resolve this issue, use the **HPBIOS > EFI** shell and select a hard drive that you can boot from (for example, `fs0:`) by looking at the device mapping table.

Change the directory (`cd`) to `\EFI\HPUX\` and run **HP-UX** to boot the operating system manually.

Note: Refer to the HP EFI manuals for more details on how to handle the EFI shell.

Once the client computer comes up, log on to the computer as `root` and run the following command to enable auto-booting.

`setboot -p <hardware_path_of_boot_harddrive>`

Prepare to Restore may not work for a Solaris client

A Bare Metal Restore (BMR) prepare-to-restore of a Solaris client computer may not work because the BMR boot server failed to resolve the IPv4 address of the client computer.

To work around this issue, perform the following:

- Make sure the IPv4 address, `client_host_name` mapping entry exists first in `/etc/hosts` before the IPv6 mapping entry.

  On the Solaris BMR boot server, if the `/etc/hosts` directory contains the IPv6 address `client_host_name` entry first, then the BMR boot server fails to identify client IPv4 address.
- Run **Prepare to Restore** again.

Use of Virtual Instance Converter (VIC) hosts on Windows (x64) having NetBackup 8.1 is not supported for NetBackup 8.0

NetBackup 8.1 BMR does not support direct virtual machine (VM) creation (Physical to Virtual) using Virtual Instance Converter (VIC) hosts on Windows (x64) having NetBackup 8.1 for NetBackup 8.0 clients. This issue occurs because NetBackup Bare Metal Restore functionality is not supported with Virtual Instance Converter (VIC) hosts having NetBackup 8.1 version.

Workaround: For a successful direct virtual machine (VM) creation (Physical to Virtual) operation, Veritas recommends that you use Virtual Instance Converter (VIC) hosts which have either NetBackup 8.0 or NetBackup 8.1.1 or later versions.

PTR or PTD failure because of boot server version mismatch after upgrade

During NetBackup 8.1.1 upgrade on a boot server, if you have continued the upgrade process with the incorrect master server fingerprint or have not provided the authorization token, the boot server version is not updated in the **NetBackup web UI**.

Because of the incorrect security certificate information, host ID-based certificate cannot be deployed on the boot server, which can lead to boot server version mismatch and failures of PTR or PTD operation:

To resolve the issue

1. Deploy a host ID-based certificate on the boot server host by running the following commands:

   ```
   nbcertcmd -getCACertificate
   ```

   ```
   nbcertcmd -getCertificate
   ```

   For more information on deploying host ID-based certificates, refer to the *NetBackup Security and Encryption Guide*.

   https://support.cohesity.com/s/article/article-100040135

2. Restart the NetBackup services.

   Alternatively, run the following command on the boot server host:

   ```
   bmrsetupboot -register
   ```

   For more details on the commands, see the *NetBackup Commands Reference Guide*.

   https://support.cohesity.com/s/article/article-100040135

Error messages for prepare to restore, prepare to discover, and the `bmrprep` command with reference to secure communication in BMR

This section provides information that helps you with troubleshooting the errors that you may encounter while you perform prepare to restore (PTR) or prepare to discover (PTD) operations and while you use the `bmrprep` command.

Table 10-2 Error messages with respect to secure communication in BMR

Error message	Description
Add an appropriate host entry or host mapping for <*Name of the host*> and retry the operation.	
Shared Resource Tree version <*Version*> is incompatible with client configuration version <*Version*>. .	To restore BMR configurations of NetBackup 8.0, you must use Shared Resource Tree (SRT) with NetBackup client version of 8.0 installed in the SRT. Shared Resource Tree (SRTs) with NetBackup 8.1.1 or later installed in them are not supported for restoring BMR configurations of NetBackup 8.0. Similarly, to restore BMR configurations of NetBackup 8.1.1 or later, you must use Shared Resource Tree (SRT) with NetBackup client version of 8.1.1 or later installed in the SRT. The usual conditions that the SRT version is greater than or equal to the BMR configuration version apply.
Reset the host attributes for <*Name of the host*> and retry the operation.	To restore BMR configurations of NetBackup 8.0 for a host that is known to the master as communicating securely (For Example: NetBackup 8.1 and above hosts), you must reset the host for a successful communication. For more information about resetting host attributes, refer *NetBackup Security and Encryption Guide* https://support.cohesity.com/s/article/article-100040135
Reset host attributes for all hosts with the mapping name <*Mapping Name*> and retry the operation.	A host name may be associated with multiple host IDs. For example: In a clustered environment. Some or all of those hosts may be known to the master as communicating securely (For Example: NetBackup 8.1 and above hosts). For restoring BMR configurations of NetBackup 8.0 or earlier for such hosts, you must reset all of those hosts for successful communication. For more information about resetting host attributes, refer *NetBackup Security and Encryption Guide* https://support.cohesity.com/s/article/article-100040135

Table 10-2 Error messages with respect to secure communication in BMR *(continued)*

Error message	Description
Configuration version of the specified host is 8.1, which is not supported by BMR.	Restoring BMR configurations of NetBackup 8.1 version is not supported.
Set the 'autoreissue' parameter for one of the host IDs of <*Name of the host*> and retry the operation.	A host name may be associated with multiple host IDs. For example: In a clustered environment. In such scenarios, you must set the **autoreissue** parameter for only one of the host IDs which you intend to restore. For more information about the host mapping, refer to the `nbhostmgmt` command in the *NetBackup Command Reference Guide* https://support.cohesity.com/s/article/article-100040135 For more information about the `autoreissue` parameter, refer *NetBackup Security and Encryption Guide*. https://support.cohesity.com/s/article/article-100040135
Authorization failed. A web login is required. Run the <*Command Name*> command to log in.	For a successful execution of `bmrprep` command, a web login is required. Perform a web login using the `bpnbat` command before you execute `bmrprep` command For more information about the `bpnbat` command, refer to the `bpnbat` command in the *NetBackup Command Reference Guide* https://support.cohesity.com/s/article/article-100040135

Table 10-2 Error messages with respect to secure communication in BMR *(continued)*

Error message	Description
BMR client <*Name of the client*> is ready to be restored. This operation is valid for a limited period of time. The default is 48 hours. Boot the client to proceed.	To restore BMR configurations of NetBackup 8.1.1 and later, you are provided with a limited period of time. The default is 48 hours. You can edit or update the default validity of 48 hours to the desired value using `web.conf` file. For more information about the autoreissue validity configuration setting, refer to the *NetBackup Security and Encryption Guide*. https://support.cohesity.com/s/article/article-100040135 **Note:** This is not a requirement to restore BMR configurations of NetBackup 8.0.
BMR client <*Name of the client*> is ready to be discovered. This operation is valid for a limited period of time. The default is 48 hours. Boot the client to proceed.	To discover BMR configurations of NetBackup 8.1.1 and later, you are provided with a limited period of time. The default is 48 hours. You can edit or update the default validity of 48 hours to the desired value using `web.conf` file. For more information about the autoreissue validity configuration setting, refer to the *NetBackup Security and Encryption Guide*. https://support.cohesity.com/s/article/article-100040135 **Note:** This is not a requirement to restore BMR configurations of NetBackup 8.0 and earlier versions.
The specified IP address <*IP address*> is not associated with the host name <*Name of the host*>. Specify an appropriate IP address for successful Prepare To Discover operation.	If the IP address that you have specified during Prepare to Discover (PTD) operation for a particular BMR client is not associated with that client, the PTD operation fails. You must ensure that you have entered the appropriate IP address.
The Prepare To Discover operation is not successful, because the specified IP address cannot be resolved.	If the IP address that you have specified during Prepare to Discover (PTD) operation cannot be resolved, the PTD operation fails. You must ensure that you have entered the appropriate IP address.

Media restore of Solaris x86 11.2 or later clients may prompt for maintenance mode user name and password

During media restore of clients with Solaris x86 11.2 or later versions installed, the restore system may show the following prompt:

```
Enter user name for system maintenance (control-d to bypass):
```

At the same time, BMR prompts you to enter the network adapter name:

```
Enter the network adapter (LINK) name from the above list
corresponding to MAC Address:
```

If you enter the network adapter name, it is received as user name for system maintenance and system may further prompt you to enter the password. For example, if you have entered the network adapter name as `net0`, system shows the following prompt:

```
Enter net0 password (control-d to bypass):
```

This issue is observed because one of the Solaris services which is non-critical for restore has fallen into the maintenance mode.

Workaround: To resolve this issue, enter `Ctrl+d` and proceed with BMR restore.

Discovery task may remain in Finalizing state after client PTD task completes successfully

For a Solaris client, the discovery task may display the state of the task as 'Finalizing' under the **Bare Metal Restore Management > BMR Tasks** tab even after the Prepare to Discover (PTD) task for the client completes successfully.

Workaround: Either update the state of the task or delete the task manually. To update the state of the task manually, run the following command on the master server for the target client:

```
bmrc -op complete -resource discovertask -client <clientName> -status
0
```

BMR restore task may remain in Finalizing state after the client is restored successfully

The Bare Metal Restore (BMR) restore task may display the state of the task as "Finalizing" under the **Bare Metal Restore Management > BMR Tasks** tab even after the restore task for the client completes successfully. An external procedure that you have configured for execution during the first boot or clean up may not have been executed.

Workaround: If the client is restored successfully, perform the following steps:

1. Open a command prompt or shell on the restored client.
2. Navigate to the appropriate directory in command prompt or shell based on the operating system of the restored client.
   - If the restored client runs Linux, then navigate to the following path:
     `<Installation Directory>/netbackup/bin`
   - If restored client runs Windows, then navigate to the following path:
     `<Installation Directory>\netbackup\bin`
3. Run the following command by providing the correct client host name for `<clientName>`:

   ```
   bmrc -op complete -resource restoretask -client <clientName>
   -status 0
   ```
4. If an external procedure is configured to be executed during the first boot or cleanup, then, execute the external procedure on the restored client manually.

Shared Resource Tree (SRT) creation fails with an error after BMR restore if a backup operation was initiated on the boot server and client while the SRT creation was in progress

This issue is observed in case of those windows boot server and clients wherein the backup has been performed while SRT creation was in progress.

Windows preboot environment is mounted in the staging area under `<NetBackup Install Path>/BareMetal/Server/Data/BaseSrd` path when the SRT creation is in progress. At this stage if you take a backup, the contents of the mounted staging area also get backed up. If you try to perform a restore of such a backup, during SRT creation post restore, the contents of the staging area cannot be unmounted

or removed as they are in an invalid state. Therefore, the SRT creation may fail with a blank error message after restore.

Workaround: Avoid taking a backup of boot servers and clients for which SRT creation is in progress.

If you encounter this issue inadvertently, perform the following steps:

1. Run the following command:

   `Dism /Get-MountedWimInfo`

   Output similar to the following sample is displayed:

```
C:\>dism /Get-MountedWimInfo

Deployment Image Servicing and Management tool
Version: 6.1.7600.16385

Mounted images:

Mount Dir : C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml.84e525b7#\
b2db45296eabfd00db1920158f3f5eb5\System.Xml.Serialization.ni.dll.aux
Image File : C:\Program Files\Veritas\NetBackup\BareMetal\server\data\baseSrd\EN
-x86\media\sources\boot.wim
Image Index : 1
Mounted Read/Write : No
Status : Invalid
```

1. To create a new SRT, you must remove or clean the directory `<NetBackup Install Path>/BareMetal/Server/Data/BaseSrd`.

   If you try to remove the `dir / files` which reside on this path, an error message is displayed.

```
You require permission from TrustedInstaller to make changes to this file
```

2. To clean up the Windows preboot environment, run the following command:

   `dism /Cleanup-Wim`

3. Take the ownership of the `<NetBackup Installed Dir>\BareMetal\server\data\baseSrd\EN -x86\mount\Windows` directory that you want to clean. Perform the following steps:

   - Right-click on the `<NetBackup Installed Dir>\BareMetal\server\data\baseSrd\EN -x86\mount\Windows` directory.

- Right-click and click **Properties**
- Click **Security** tab
- Click **Advanced**
- In the **Advanced Security Settings** dialog box, click **Owner** tab. Current ownership details are displayed.
- Click **Edit** to modify and take the ownership of `<NetBackup Installed Dir>\BareMetal\server\data\baseSrd\EN -x86\mount\Windows` directory.
- Provide permissions to UAC. Select the user name from the **Change owner to** dialog box that you want to assign as the owner for the object. Click **Ok**. Once you make the required changes, the same is displayed in the **Advanced Security Settings** dialog box.
- Click **Ok** to exit
- Repeat the steps 1 to 4 to open the `<NetBackup Installed Dir>\BareMetal\server\data\baseSrd\EN -x86\mount\Windows` directory's **Properties** window again.
- In the `<NetBackup Installed Dir>\BareMetal\server\data\baseSrd\EN -x86\mount\Windows` directory's **Properties** window, click **Edit** and confirm the UAC elevation request.
- Select the **Administrators** in the **Group or user names** dialog box. click **Add**, and type in the **Administrator's** user name into the **Enter object names to select** dialog box, and finish off by clicking **Ok**.
- In the **Permissions for Administrators** dialog box, click **Full Control** under the **Allow** column to assign full access rights control permissions to **Administrators** group.

4. Remove the `<NetBackup Installed Dir>\BareMetal\server\data\baseSrd\EN -x86\mount\Windows` directory.
5. Retry new SRT creation operation.

Error in receiving BMR information during backup

Error in receiving Bare Metal Restore information during backup of client RHEL 8.4 on Netbackup version 9.1.0.1 or later.

Error messages

- 01.12.2021 10:58:30 - Error bpbrm (pid=1761542) BMRERR: Received BMR error: Failed to import Config file. (27)
- 01.12.2021 10:58:31 - Error bpbrm (pid=1761542) BMRERR: Received BMR error: Unable to parse client information. (6)
- 01.12.2021 10:58:31 - Error bpbrm (pid=1761542) BMRERR: Received BMR error: Failed sending the discovery. (21)
- 01.12.2021 10:58:31 - Error bpbrm (pid=1761542) BMRERR: Received BMR error: BMR information discovery failed. (35)
- 01.12.2021 10:58:31 - Info bmrsavecfg (pid=0) done. status: 1: the requested operation was partially successful.

bmrsaveconfig -infoonly fails for the client

[root@gf0vsxas024l logs]# /usr/openv/netbackup/bin/bmrsavecfg -infoonly

sh: /bin/netstat: No such file or directory

sh: /sbin/ifconfig: No such file or directory

Cause

Identification of the failure in the logs reveals that the issue is related to the use of ifconfig and netstat - these commands are deprecated in RedHat 8.3 and RedHat 8.4 - these can be used if the net-tools package is installed - but they are not present by default - they have been replaced by IP and SS respectively

The common executables `netstat` and `ifconfig` are not installed on the Red Hat 8.4 client.

The BMR option in the policy calls `bmrsavecfg` to run on the client and this calls the executables and they are not found.

Solution

Follow the steps to receive BMR information during backup operation without error:

- Install the net-tools package
- Install the executables manually from the operating system.
- Then run the backup job again.

BMR backup and restore job details does not display on the NetBackup web UI's activity monitor

BMR backup and restore job details does not display in the activity monitor of the NetBackup web UI, after you run the `bmrsetupmaster` command.

This situation occurs because the NetBackup database password gets reset after a user runs the `bmrsetupmaster` command.

Recommended action: After you run the `bmrsetupmaster` command, the NetBackup database password is reset. Then the NetBackup web APIs connect with the NetBackup database to perform its functions. Due to technical limitations, you must restart the NetBackup services. This action aids in the performance of the NetBackup web APIs after the BMR primary server configuration.

Chapter 11

Creating virtual machine from client backup

This chapter includes the following topics:

About creating virtual machine from backup

NetBackup BMR supports direct virtual machine (VM) creation (Physical to Virtual) from FULL, SYNTHETIC, INCREMENTAL, and PIT (point-in-time) backups. This VM creation does not require BMR Boot server and Shared Resource Tree setup. For more information on platform support matrix, refer appendix section to See "BMR Direct VM conversion support matrix" on page 252.

This feature supports easy wizard-based or single CLI-based disaster recovery (DR) to virtual machine. VM creation is even possible at DR domain using NetBackup Auto Image Replication (A.I.R.) support. The feature aids a non-technical person to perform server level DR as the user need not create virtual machine layout or do dissimilar system recovery using BMR method. Run physical to virtual machine creation wizard or single command line to find the created client virtual machine and to boot it automatically.

BMR physical to virtual machine creation benefits and use cases

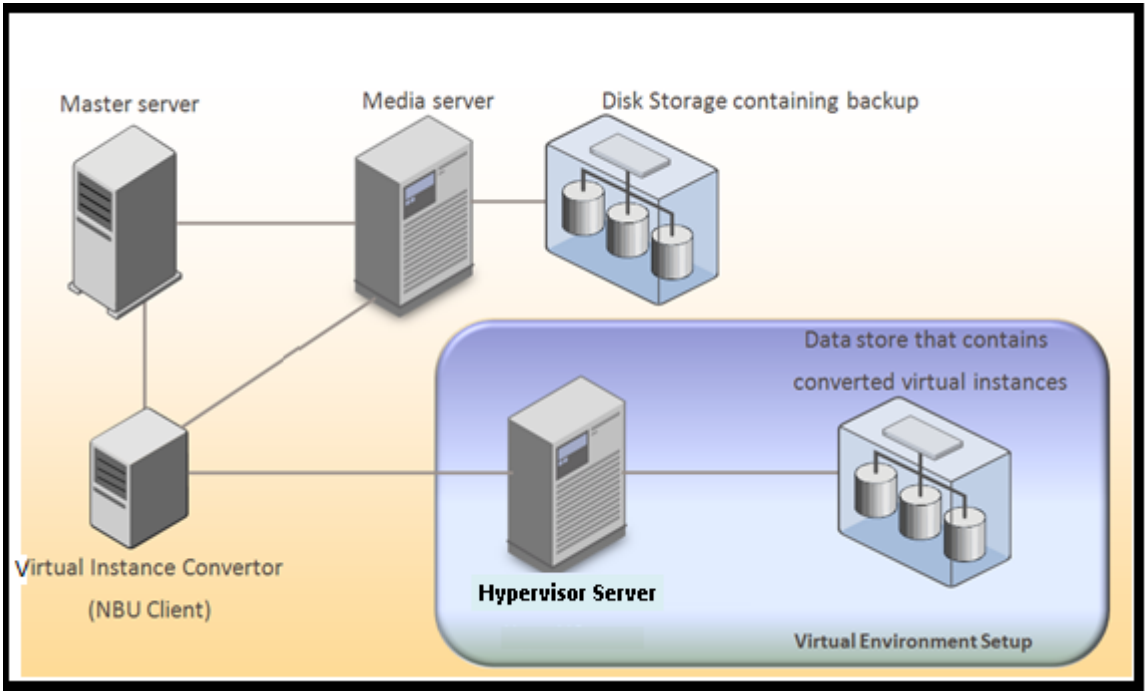
Client to VM creation process provides following major benefits and use-cases.

- Can be used as instant temporary DR mechanism.
- Lowers OPEX by leveraging virtual machines for recovery.
- Provides quick recovery of primary domain clients at DR domain by enabling NetBackup Auto Image Replication (A.I.R.). Refer NetBackup Web UI Administrator's Guide for more details on enabling Auto Image Replication.
- Reduces Recovery Time Objective (RTO) with easy-to-use VM conversion wizard as well as not requiring any system recovery pre-requisites preparation.
- Can be used to do compliance and fire-drill testing.
- Supports create VM from FULL, INCREMENTAL, and synthetic backup image.
- Supports create VM from Point-In-Time backup image.
- Provides VM creation flexibility by providing different preferences like:
  - System-only restore: Provides option to create VM with OS volumes only.
  - Overwrite existing VM: Any existing VM with the same name can be automatically overwritten.
  - Auto boot VM after creation: When selected, VM creation process automatically boots VM, post creation.
  - Flexibility to map individual virtual disk to required virtualization storage entity.
  - Network stripping: Option to remove original client network interfaces and IP configuration in VM.
- Provides option to create VM with only selected disks.
- Provides a single command-line facility to trigger client VM creation.

Note: The incremental data restore is not currently supported, however, fresh VM creation from an incremental backup is possible.

Deployment diagram for virtual machine creation

Following is a general deployment diagram for BMR client to virtual machine conversion.



Master server: NetBackup primary server that takes BMR enabled backup of client.

Note: Refer following sections and for more details on configuring BMR master server and enabling BMR client protection.

See "Configuring BMR Master Server" on page 17.

See "Configuring policies to back up BMR clients" on page 24.

Media server: NetBackup media server which contains client's BMR enabled backup image on disk-based storage unit.

Virtual Instance Convertor (VIC): This host is NetBackup recovery host which has configured NetBackup client. BMR client to VM conversion requires VIC operating system, belonging to same family as client's operating system, which is required to be converted to virtual machine. For example, Windows based VIC can create VMs of Windows based clients.

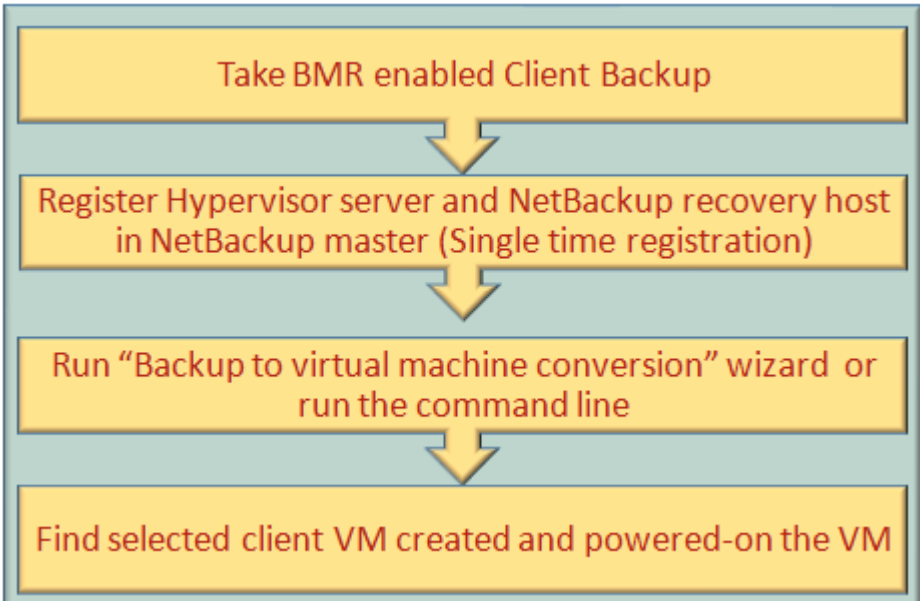
Hypervisor Server: The destination virtualization server where client VM is created. You need to select the intended Hypervisor server while running virtual machine conversion wizard.

Note: You do not need extra hardware for VIC host. VIC host can be optionally configured over a virtual machine.

VIC can also be configured over primary or media server if server OS is of same OS family as that of client being converted. Though it is not recommended to set up VIC on NetBackup primary or media server as VM creation process consumes resources and it can slow down NetBackup server Performance. For details on currently supported Hypervisor servers for virtual machine conversion operation See "BMR support for virtual environment" on page 251.

Client-VM conversion process flow

Following diagram shows the process flow of client to VM conversion process at high level.



Pre-requisites to create VM from backup

Following are the prerequisites to create a virtual machine from backups.

- Configured BMR primary server
  First, you need to enable the BMR server on your NetBackup primary server. For details on how to enable BMR server, see the following topic.

See “Configuring BMR Master Server” on page 17.

- Client's BMR enabled backup
  Configure NetBackup policy for BMR. Select the check box for BMR for the **Collect disaster recovery information** option in the policy attributes. More details are available:
  See “Configuring policies to back up BMR clients” on page 24.
- The BMR backup policy requires that the OS volumes are added as part of the backup selections. For Windows systems, you must add the Boot, System Volume, and System State in the backup selections list.

Note: For user convenience, in the backup selections the `ALL_LOCAL_DRIVES` option is available by default. This directive considers all the client volumes during backup.

After enabling BMR in the backup policy, take an initial full backup.

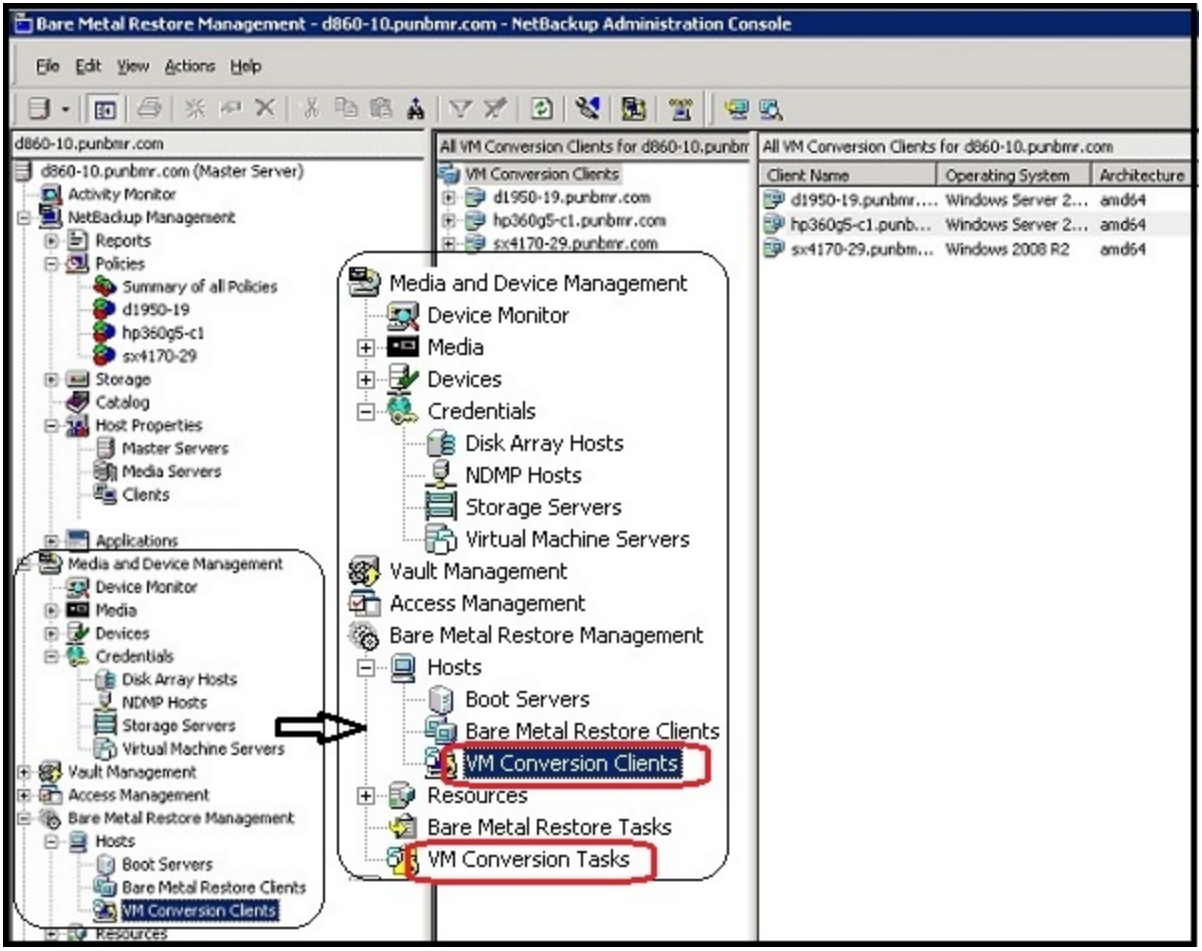
- Hypervisor-specific tools ISO file
  The VM creation process requires hypervisor-specific tools ISO file so that during VM creation it configures required device drivers into the VM system. Usually, the Hypervisor vendor provides their tools ISO file on their website and on the hypervisor server. For example, for VMware ESX server 5.0 you can locate the associated tools ISO on your ESX server or download them from the VMware website.
  Tools ISO path on ESX server: **/vmimages/tools-isoimages/windows.iso**
  Website location:
  http://packages.vmware.com/tools/esx/5.0latest/windows/x86_64/index.html
  You must have this tools ISO file on the VIC host. The virtual machine creation wizard prompts you for the full directory path of this ISO that is available on VIC.
- Hypervisor server name registration in NetBackup
  You need to register your Hypervisor server with NetBackup where the VM needs to be created. This registration requires Hypervisor server admin credentials.
- VIC (NetBackup recovery host) name registration in NetBackup
  For VMware type Hypervisor, the Virtual Image Converter host name needs to be registered in the host property **VMWare access host** for the primary server.

Virtual machine creation from backup

Following sections details about client’s VM creation process from backup.

Virtual Machine Conversion Clients

In NetBackup Administration Console, in tab **Bare Metal Restore Management > VM Conversion Clients** panel enlists all the clients available to be converted to virtual machines (VMs). You can see various details of the clients like operating system type, CPU, RAM, Hosts, and network-related information.

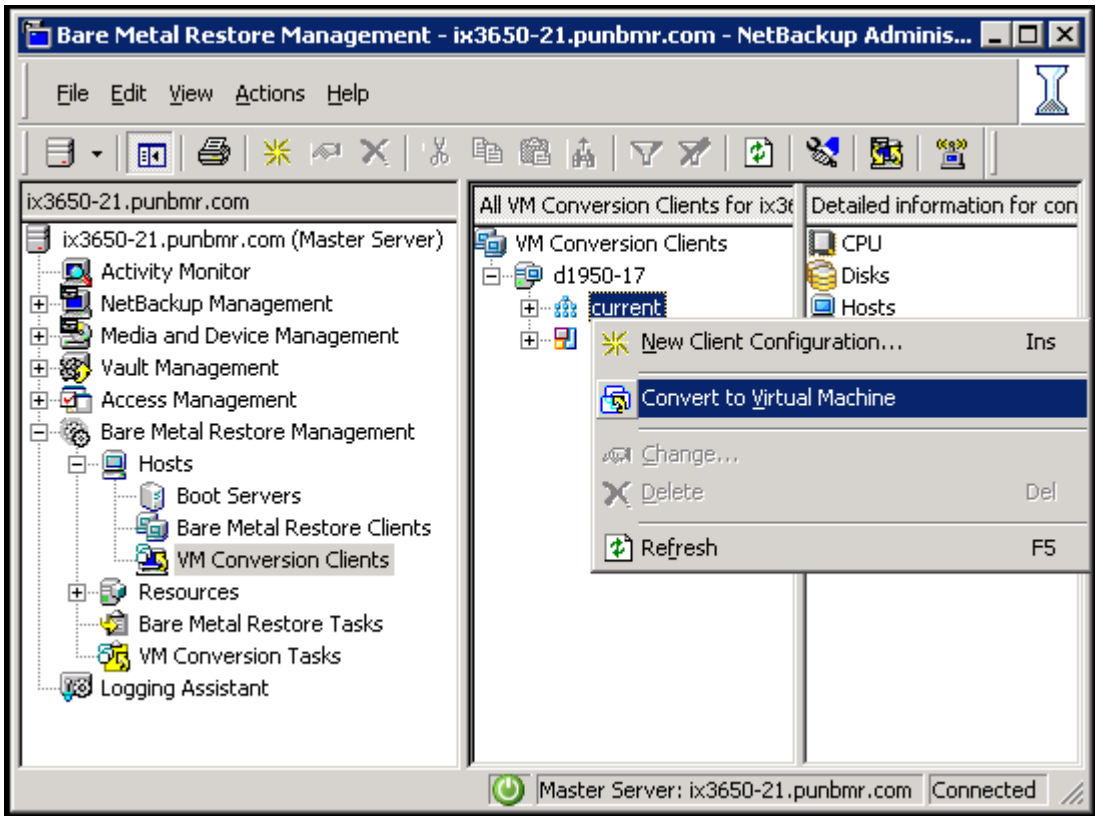


Converting client backup to VM

You can convert BMR-enabled backups to virtual machine using **Virtual Machine Conversion** wizard. Similar wizard is available in NetBackup web UI.

To initiate operations related to conversion of client backups to virtual machines, perform following actions:

1. Navigate to VM Conversion Clients panel on NetBackup console.
2. Right-click on intended client configuration to get a pop-up menu with conversion operation options.



Optionally, you can create a custom client configuration or PIT (Point-In-Time) configuration for VM creation. In such case, use **New Client Configuration** option to either create a PIT configuration or copy the existing client configuration. For details on how to change client configuration, See "Creating custom configurations" on page 231.

3. On conversion operations pop-up menu, click **Convert to Virtual Machine** to start conversion process wizard.

   This wizard prompts you the details about destination Hypervisor server parameters and conversion options.

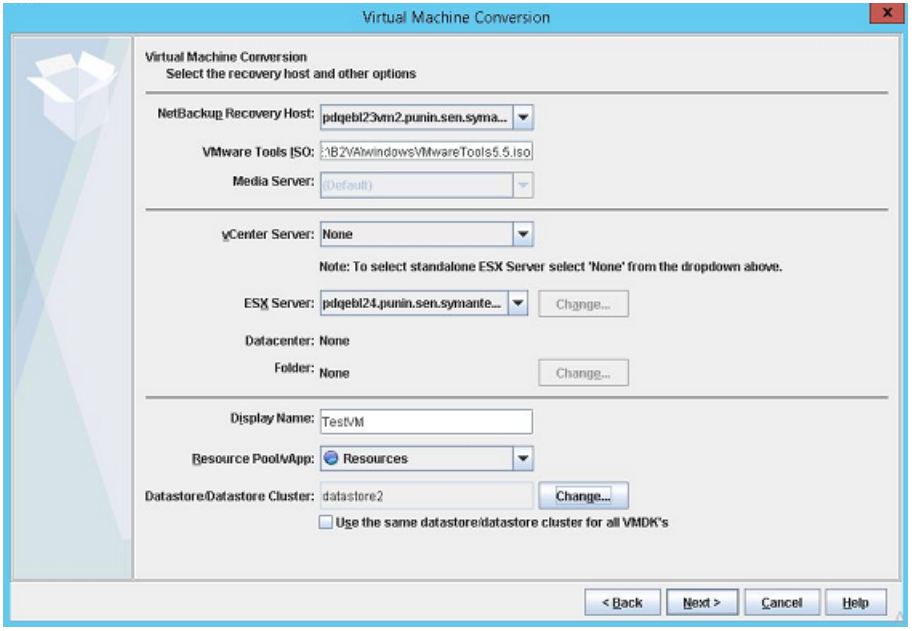
VMWare based VM Conversion Wizard Flow

The wizard first page prompts user for information about VMWare server parameters, VIC host details etc.

Table 11-1 Conversion to Virtual Machine

Parameter	Parameter Details
NetBackup recovery host:	This is NetBackup client host-name which to be used as VIC (Virtual Instance Converter). or recovery host. This host prepares VM on intended VMWare server. **Note:** VIC OS has a rule that if client that is being converted to VM has Windows-based family, then you Must set Windows-based VIC . VIC can be set on physical or virtual machine if this OS rule is satisfied. However, it is not recommended to set up VIC on NetBackup primary or media server as Virtual Machine creation process consumes resources and it can slow down NetBackup server Performance.
VMWare Tools ISO files:	Enter the absolute path where the VMWare .iso file is located on VIC host that is entered earlier in this dialog box. For details See “Pre-requisites to create VM from backup ” on page 220.
vCenter server:	Select vCenter server name if applicable.
ESX Server:	Select or Enter ESX server name.
VMWare Folder:	The folder where the destination virtual machine to be created.
Display Name:	Enter a display name for the virtual machine to be created.
Resource Pool:	Select the intended resource pool name from the drop-down menu.
Datastore/Datastore Cluster:	These are storages connected to ESX server. If you select option **Use the same datastore/datastore cluster for all VMDKs** then all V-disks belonging to the VM will be created on the same datastore or datastore cluster. If this option is not selected, then later screen of this wizard will provide option to map individual V-disk to the datastore.

Refer following sample dialog snapshot showing earlier described parameters populated. Refer following screenshot for more details.



Virtual Machine Options

The next wizard page prompts you to provide VM conversion options and allows selection of virtual disk types. Following table enlists all the required options related to VM and disk types.

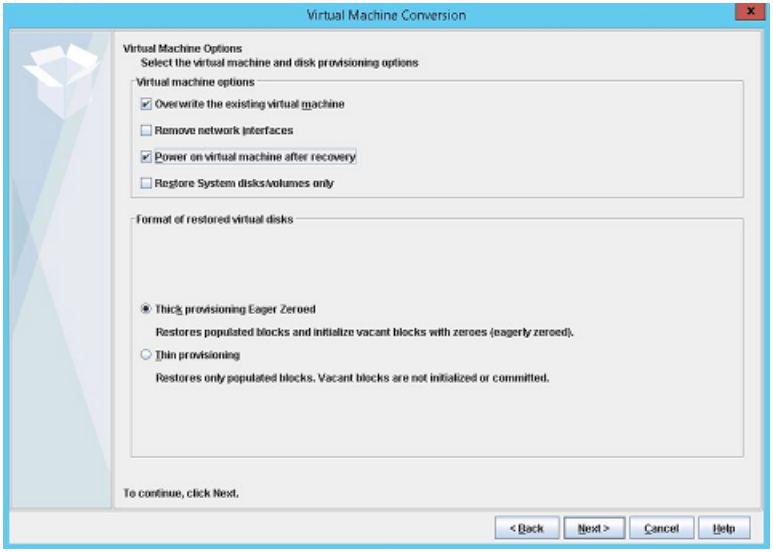
Table 11-2 Virtual Machine Options

Virtual Machine Options	
Over-write existing VM:	Select this option to enable deletion of existing virtual machine in case of duplication of display name. If a virtual machine with the same display name exists at the destination, that virtual machine will be automatically deleted before the restore begins; otherwise, the restore fails. If you do not select this option, you need to manually delete the duplicate VM name.
Remove network interfaces:	If this option is selected then original client network interfaces will not be configured on the destination. If this option is not selected, then same number of network interfaces and their details existing on source client configuration will be configured on the VM.

Table 11-2 Virtual Machine Options *(continued)*

Power-on virtual machine after recovery:	Select this option to have the recovered virtual machine automatically turned on when the recovery is complete.
Restore System disks and volumes only:	Select this option to restores the OS disk volumes only in case where only OS needs to be recovered on VM.
Virtual Disk Types	
Thin Provisioning:	Select this option to configure the restored virtual disks in thin format. Thin provisioning saves disk space through dynamic growth of the vmdk file. The vmdk files are no larger than the space that the data on the virtual machine requires. The virtual disks automatically increase in size as needed.
Thick Provisioning:	Select this option to configure the restored virtual disks in thick format. It creates virtual disk length that is equivalent to physical disk length on the VM. Creation of the virtual disks may take more time with this option.

Refer following sample snapshot showing VM options.



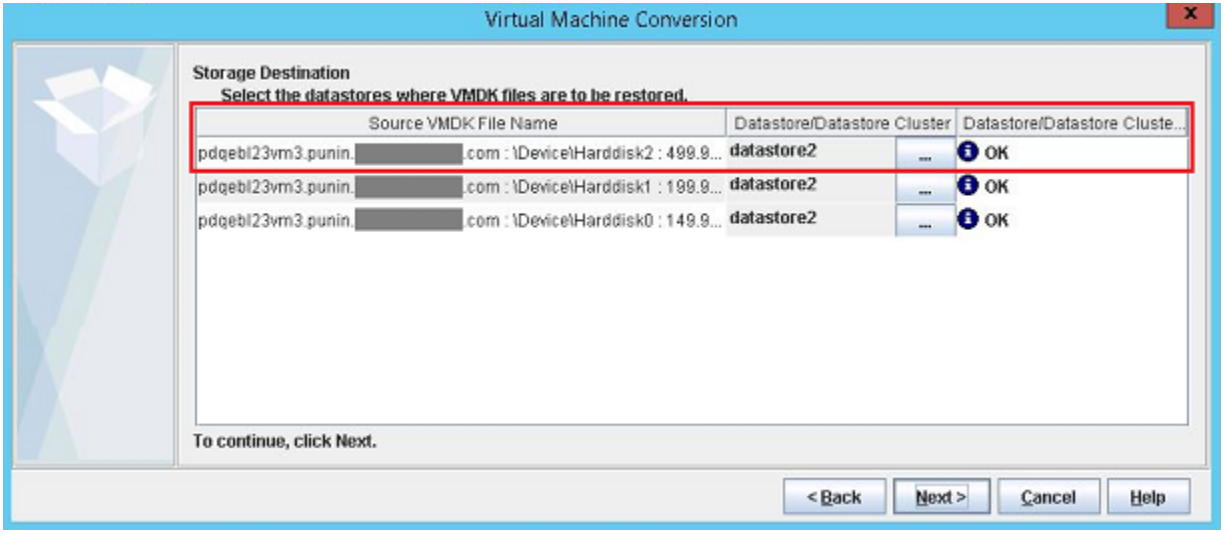
Virtual machine conversion storage destination

VM Conversion storage destination wizard lists all the disks belonging to client being converted to virtual machine. It lets you select datastore to be mapped with

the individual disks where recovery process creates equivalent VMDK file on the correspondent datastore.

Note: In case you have checked the option **Use the same datastore/datastore cluster for all VMDKs** in the **Conversion to VM** wizard, then the storage destination is already selected.

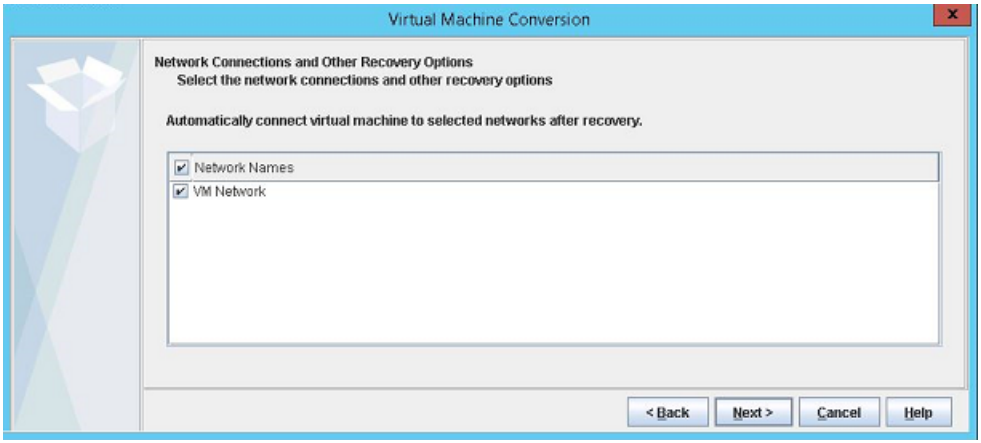
Refer following sample screenshot with destination details.



Network connection selections

You can select VMWare network connection name in order to create VM Network interface belonging to virtual network. The wizard lists all the available network connections.

Refer following sample screenshot showing network names to select from.



Virtual machine conversion summary

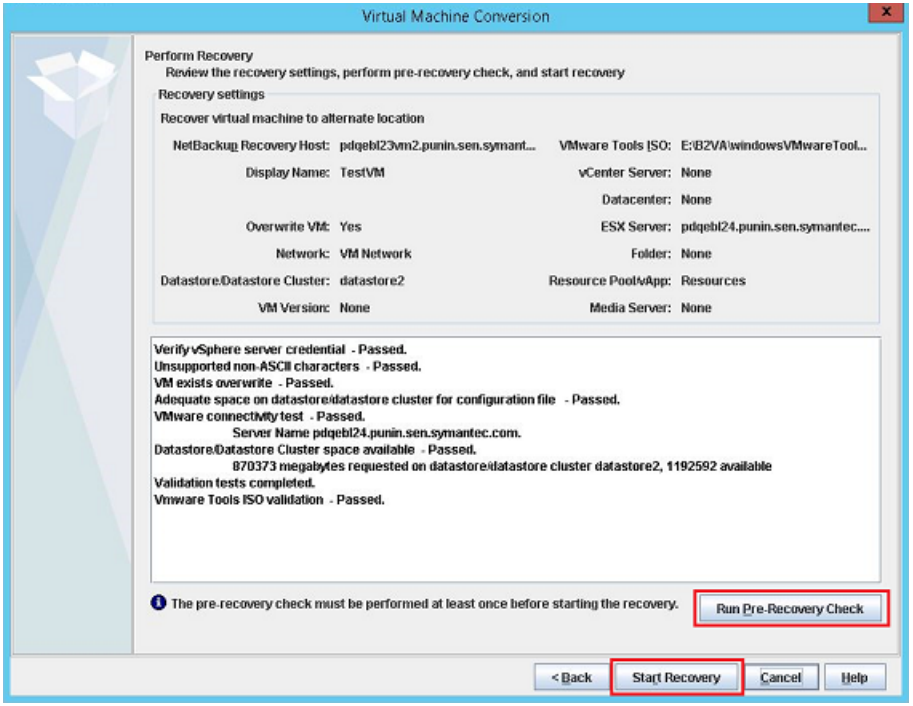
The summary page displays all the details related to client conversion that are configured through VM Conversion wizard.

Execute a pre-check to confirm that the environment details are intact. The validation tests show status as **Passed** if all the environment configurations are intact.

Click **Start Recovery** to create tasks for VM creation process through NetBackup primary server. Check the tasks listed in **VM Conversion Tasks** under **Bare Metal Restore Management** tab and refer task status and operation to know the progress status.

Refer chapter *Monitoring bare metal restore tasks* for more details about tasks and status information.

Refer following sample summary screen.



Direct Virtual Machine (VM) conversion (physical to virtual) tasks performed after the restore is complete

Starting with NetBackup 8.1.1 and later releases, for a windows client, after a successful completion of restore during Direct Virtual Machine (VM) conversion (physical to virtual), you have to manually deploy the Certificate Authority (CA) certificate and the host ID-based certificate on the client that is restored.

To generate and deploy a host ID-based certificate manually

1. The host administrator must have obtained the authorization token value from the CA before proceeding. The token may be conveyed to the administrator by email, by file, or verbally, depending on the various security guidelines of the environment.
2. Run the following command on the non-master host to establish that the master server can be trusted:

   ```
   nbcertcmd -getCACertificate
   ```

3 Run the following command on the non-master host and enter the token when prompted:

```
nbcertcmd -getCertificate -token
```

Note: To communicate with multiple NetBackup domains, the administrator of the host must request a certificate from each master server using the -server option.

If the administrator obtained the token in a file, enter the following:

```
nbcertcmd -getCertificate -file authorization_token_file
```

4 To verify that the certificate is deployed on the host, run the following command:

```
nbcertcmd -listCertDetails
```

Use the `-cluster` option to display cluster certificates.

For more information on how to deploy host-ID-based certificates, refer to the Deploying host ID-based certificates section in the NetBackup Security and Encryption Guide

https://support.cohesity.com/s/article/article-100040135

Virtual Machine Conversion Tasks

On Virtual Machine Conversion wizard, when you click **Convert to Virtual Machine** it creates a task for virtual machine creation process. You can check the status of this task in **Virtual Machine Conversion Tasks** tab and can check tasks operation to know the progress status.

Refer chapter *Monitoring bare metal restore tasks* for details about tasks and status information.

Restore Task Properties

Restore Task Properties dialog summarizes all parameters for client-VM conversion viz. general configuration and recovery options. The summary also includes virtual machine conversion configurations such as VM name, vCenter server, VMWare Tools ISO file location, and datacenters for VMDKs. It also lists configured network parameters and restores disk types.

Refer chapter *Monitoring bare metal restore tasks* for details about tasks and status information.

Creating custom configurations

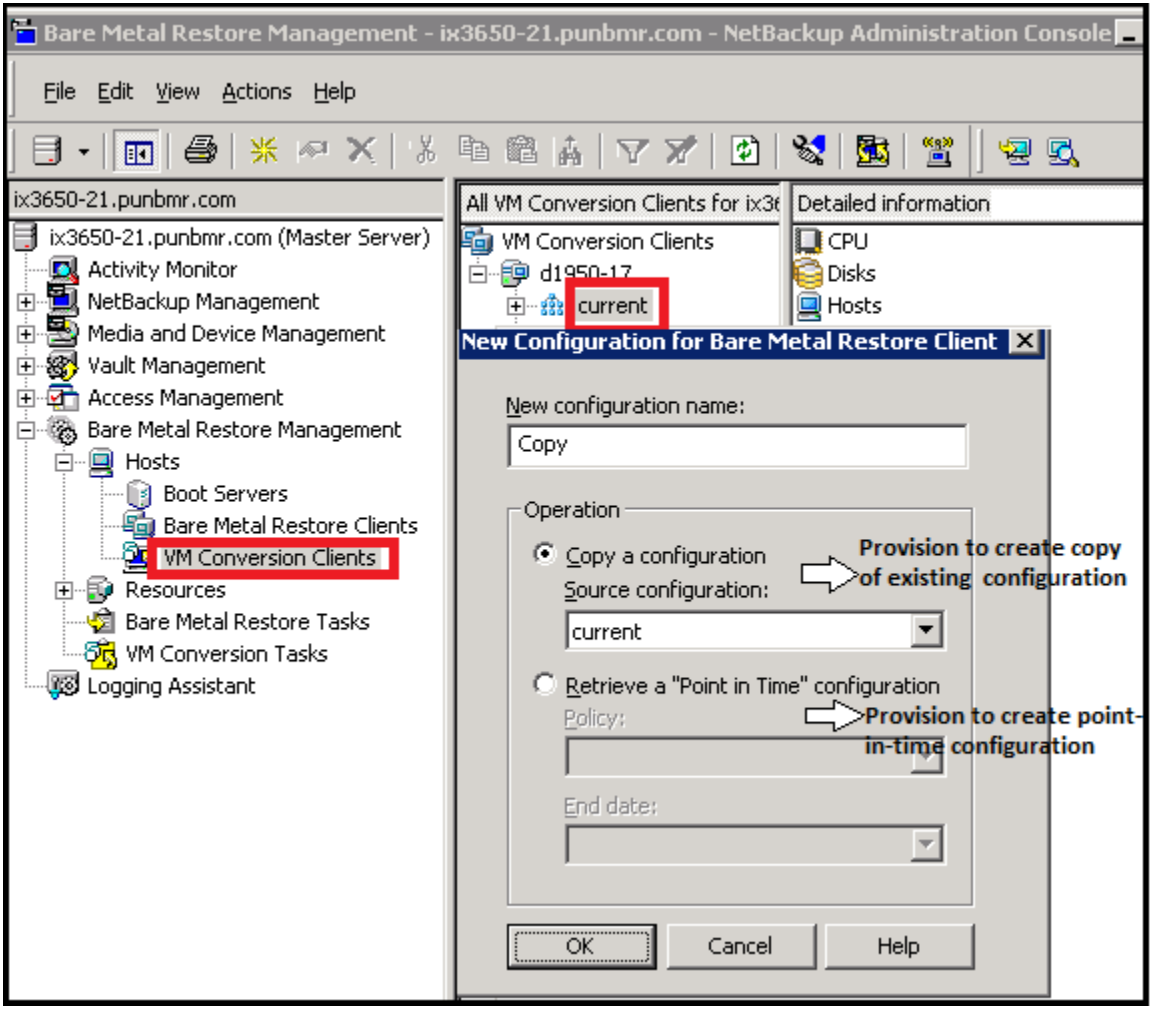
When creating new client configuration, you can either copy an existing client configuration or a Point-in-time (PIT) configuration policy to have PIT VM creation. Customized configuration creation is required for the following:

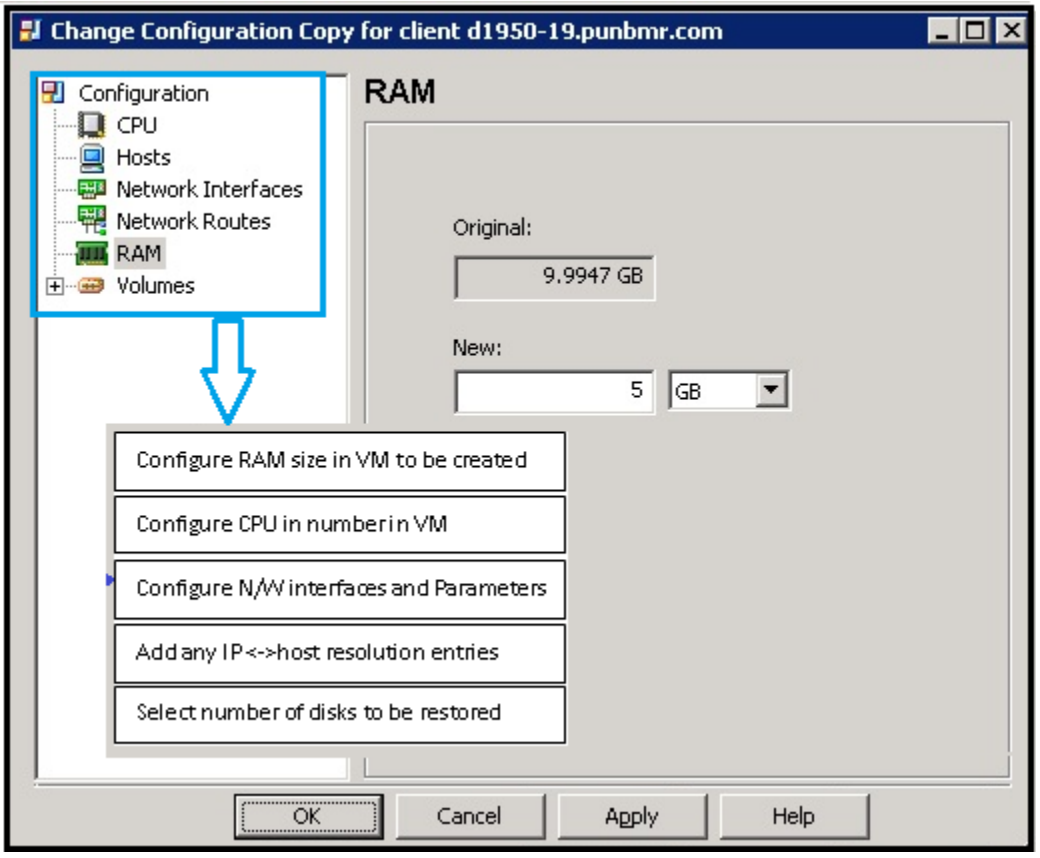
- Create a copy configuration: You can copy existing client configuration for conversion customizing original configuration. You can customize client properties viz. RAM size, allocated CPU units, disks to be created on VM, and network parameters.

  This customization provision helps in some cases like you may not want to recover all original disks or volumes on VM. In this case, you can mark unwanted disks as restricted to avoid creating VM conversion process create corresponding virtual disk/s during VM creation.

  Note: Make sure that you are not restricting OS disk/s. Otherwise created VM will not boot.

- Point-in-time (PIT) VM creation from PIT backup: You can retrieve PIT configuration for a backup image.You can also retrieve the PIT configuration and copy it from the NetBackup web UI.


Bare Metal Restore Management - ix3650-21.punbmr.com - NetBackup Administration Console
File Edit View Actions Help
ix3650-21.punbmr.com
ix3650-21.punbmr.com (Master Server)
Activity Monitor
NetBackup Management
Media and Device Management
Vault Management
Access Management
Bare Metal Restore Management
Hosts
Boot Servers
Bare Metal Restore Clients
VM Conversion Clients
Resources
Bare Metal Restore Tasks
VM Conversion Tasks
Logging Assistant
All VM Conversion Clients for ix3
VM Conversion Clients
d1950-17
current
Detailed information
CPU
Disks
Hosts
New Configuration for Bare Metal Restore Client
New configuration name:
Copy
Operation
Copy a configuration
Source configuration:
current
Provision to create copy of existing configuration
Retrieve a "Point in Time" configuration
Policy:
Provision to create point-in-time configuration
End date:
OK
Cancel
Help



Refer chapter *Managing clients and configurations* for more information.

Virtual Machine Creation CLIs

You can use command-line interface to perform various operations related to VM creation from client backup.

- Submitting a job for VM creation from backup
  Submit a job for VM creation using command `nbrestorevm` from master server or any client with administrative privilege. In case you fire `nbrestorevm` without any parameter, following help is displayed.
  For VM restore:

```
nbrestorevm -bmr {-vmw|-vmhv} -C vm_client [-S master_server] [-O]
[-R rename_file (must be an absolute path)] [-L progress_log [-en]]
[-k "keyword phrase"] [-disk_media_server media_server] [-s
```

```
mm/dd/yyyy [HH:MM:SS]] [-e mm/dd/yyyy [HH:MM:SS]] [-w [hh:mm:ss]]
[-vmtm vm_transport_mode] [-vmserver vm_server] [-vmproxy vm_proxy]
[-vmpo] [-vmtd] [-vmfd] [-vmbz] [-vmdrs] [-vmpdrs] [-vmvxd]
[-vmkeephv] [-vmid] [-vmsn] [-vmrb] [-force] [-vcd] [-vcdred]
[-vcdovw] [-vcdrte] [-vcdtemplate] [-vcdlfree] [-vcdremv]
[-ir_activate] [-temp_location temp_location_for_writes]
[[-ir_deactivate | -ir_reactivate | -ir_done]
instant_recovery_identifier] [-ir_reactivate_all [-vmhost vm_host]
[-media_server media_server_activate_vm]] [-ir_listvm]
```

For BMR VM Conversion:

```
nbrestorevm -bmr {-vmw|-vmhv} -C vm_client [-S master_server] [-O]
-vmserver vm_server -vmproxy vm_proxy -veconfig ve_config_file_Path
(must be an absolute path) [-config bmr_config_name] [-vmpo]
[-vmsn] [-systemOnly]
```

Where,

-vmw : VMWare

-C : Name of the client to be converted to VM

-S : Name of the master server

-O : Option to overwrite VM if already exists with the same name

-vmserver : vCenter or ESX server name

-vmproxy : Virtual Image Converter or NB-Proxy name

-veconfig : File full path containing virtual environment details

-vmpo : [optional] If provided VM will be automatically powered On

Example:

```
nbrestorevm -bmr -vmw -C d1950-17.punbmr.com -vmserver
bmrrh10.vxindia.veritas.com -vmproxy ix3650-21.punbmr.com -veconfig
C:\B2V\veconfig-vmw1.txt -config current -O -vmpo
[Info] V-433-32 Successfully submitted job. For more details please
see VM Conversion Tasks
```

Details for `-veconfig` file.

For example, C:\B2V\veconfig.txt contains below information in parameter = value manner.

```
esxhost="bmrvmw1.vxindia.veritas.com"
name="Test_NBRestoreVM"
network="VM Network"
diskformat="ThinVdisk"
toolsIsoPath="C:\B2V\windows_esx5.iso"
datacenter="/TestFolderAboveDC/Public Datacenter"
folder=[optional]"/TestFolderAboveDC/Public Datacenter/vm"
```

```
resourcepool= [optional]"/TestFolderAboveDC/Public
Datacenter/host/bmrvmw1.vxindia.veritas.com/Resources"
harddisk=0:"B2V_4TB"
harddisk=1:"storage1 (2)"
harddisk=2:"storage2 (1)"
```

- Tracking VM creation jobs
  You can track submitted VM creation jobs using following CLIs.
  On master server, to list submitted jobs which are in running state, fire:
  ```
  <C:\Program Files\Veritas\NetBackup\bin>bmrs -operation list
  -resource B2VrestoreTask
  ```
  On master server, to list VM creation jobs history (successfully completed or failed), fire:
  ```
  <C:\Program Files\Veritas\NetBackup\bin>bmrs -operation list
  -resource B2VrestoreTaskLog
  ```
- Deleting VM creation related task logs
  On master server, to clean-up logs from the database, fire:
  ```
  <C:\Program Files\Veritas\NetBackup\bin>bmrs -o delete -resource
  b2vrestoretasklog -id <p2vRestoreTaskLogId>
  ```
  You can get **p2vRestoreTaskLogId** by using command in the list operation for task log keyword.

For more information, refer NetBackup Commands Reference Guide.

Chapter 12

Monitoring Bare Metal Restore Activity

This chapter includes the following topics:

Monitoring BMR restore tasks

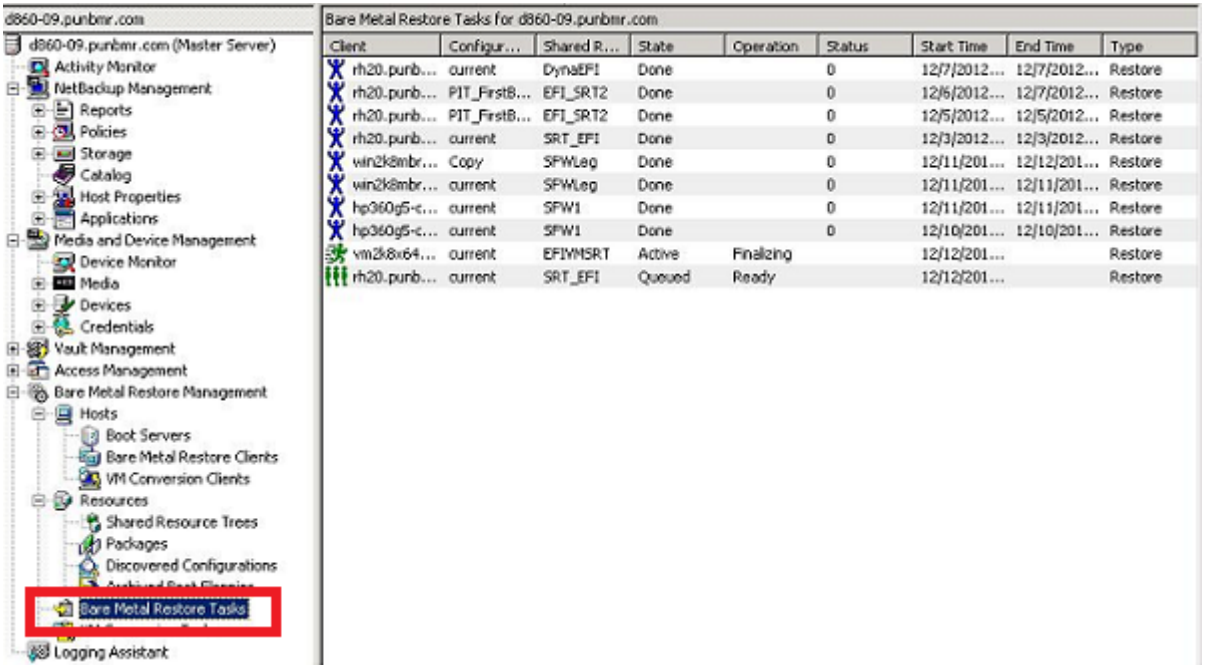
The **Tasks** window shows the status and the resource allocation for the prepare-to-restore and prepare-to-discover operations.

To monitor BMR restore tasks

1 In the NetBackup web UI, select **Bare Metal Restore > BMR 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.

Following screenshot shows a restore task created for client post PTR (prepare-to-restore operation). The task status indicates that the client is ready for BMR recovery.



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

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

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

Monitoring backup jobs

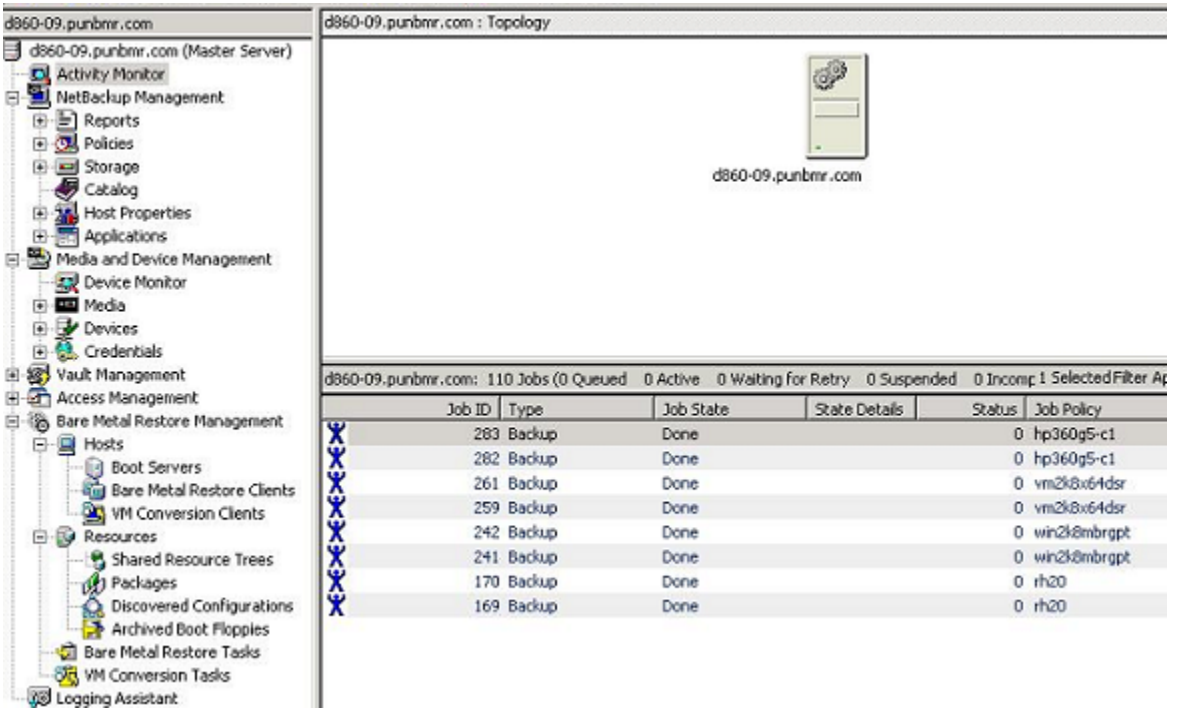
You can monitor the jobs that back up the protected clients by using the **Activity monitor > Jobs** of the NetBackup web UI.

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

The tabs display job information, as follows:

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

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



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

Note: In case BMR configuration backup job fails (normally, the job with the lowest job ID), the file system data backup completes successfully. In this case, after successful file system data backup, BMR configuration backup job is marked as Partially Completed highlighted in yellow.

Monitoring VM Creation jobs

On Virtual Machine Conversion wizard execution, when you click Convert to Virtual Machine button, NetBackup creates a task for VM creation process. You can check the status, selected hypervisor environment details and VM conversion options under this task tab.

To monitor VM conversion tasks, perform the following tasks:

1. In the **NetBackup web UI**, navigate to **Bare Metal Restore** > **Hosts > VM Conversion Tasks**.
2. Use the **Refresh** option to update the details pane with new information retrieved from the master server. Only the update item is highlighted.

   Following screenshot shows a VM conversion task created upon execution of VM conversion wizard.
3. To display details about a task, **right-click** a task in the **Details** pane and then select **Properties**.

Note: You cannot cleanup or cancel submitted VM conversion task similar to BMR restore or discover tasks. You can see selected clients file system data recovery jobs under **NetBackup Activity Monitor**.

Following table shows different task status codes related to VM conversion, with description.

Status Code	Description
0	VM conversion task completed successfully.
3	Resource allocation failed.
4	Unsupported client configuration for VM creation. Some unidentified exception has been thrown during VM creation process execution.
6	Failure while loading client configuration.
7	Failure while creating VM node for the selected client configuration.
8	Failure while preparing for client physical machine object.
9	Failure while constructing VM conversion metadata.
12	Failure while mounting file systems on the created VM.
13	Failure while loading windows registry on the created VM.
15	Failure while configuring network settings.
16	Failure while auto-rebooting created VM. Sometimes if the hypervisor server is fully loaded then this task may fail. You can try booting VM manually in such case.
17	Failure while handling device driver configuration.

Status Code	Description
18	Failure while handling MSD device driver configuration.
19	An unidentified exception has been thrown during VM conversion process execution

BMR logs

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

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

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

BMR uses a standardized naming format for log files.

The following is an example log file name:

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

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

- `51216` is the product ID for NetBackup.
- 119 is the originator ID of the process that wrote the log (`bmrd` or `bmrbd`, the Bare Metal Restore master or boot server service).
- 3892578826 is a decimal ID for the host that created this log.
- 050225 is the date in YYMMDD format.
- 0000000000 is the rotation number indicating the instance of this log file. If the file reaches maximum size and a new log file is created for this originator, the file rotation number increases by 1.

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

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

BMR logging originator IDs

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

119	`bmrd`. Bare Metal Restore master.
121	`bmrsavecfg`. Bare Metal Restore the agent that runs on client systems, collects the client configuration, and saves the client configuration to the master server.
122	`bmrc`. Bare Metal Restore the utility that clients use to communicate with the BMR master server during a restore. Runs on the restoring client.
123	`bmrs`. The Bare Metal Restore command-line interface for the various activities that are performed by the GUIs.
125	`bmrsrtadm`. Bare Metal Restore utility that creates and manages shared resource trees and creates bootable CD media or DVD media for restores. Runs on a BMR boot server.
126	`bmrprep`. Bare Metal Restore utility that prepares BMR for a client restore or discovery. Runs on the master server.
127	`bmrsetupmaster` and `bmrsetupboot`. Bare Metal Restore master server and boot server configuration utilities.
128	Miscellaneous programs and Bare Metal Restore libraries.
129	`bmrconfig`. Bare Metal Restore utility that modifies a client's configuration.
130	`bmrcreatepkg.exe`. Bare Metal Restore utility to add Windows drivers, service packs, and hotfixes to the BMR master server so they can be used in a restore. Runs on Windows boot servers.
131	`bmrrst.exe` and `bmrmap.exe` (Windows systems only). Utilities that restore Windows Bare Metal Restore clients. Run on the restoring client.
142	`bmrepadm`. A utility that manages Bare Metal Restore the external procedures that are used during restores. Runs on the master server.
152	`bmrovradm`. A utility that manages custom override functions for Bare Metal Restore.
248	`bmrlauncher`. A utility that prompts for IP information in the new Windows Fast Restore environment.
433	`bmrb2v`: This is BMR backup to VM creation command-line interface.
434	`bmrb2vrst`. A utility that does VM creation on VIC (NetBackup recovery) host.
529	`bmrbd`. The BMR Boot Server Service running with root/admin privileges.

530	`bmrbd`. The BMR Boot Server Service running with Service Account.

Commands to manage unified logging and log files

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

See the NetBackup Administrator's Guide, Volume I.

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

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

The following commands manage unified logging and log files:

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

These commands are located in the following directories:

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

BMR restore logs

The BMR restore process writes messages to restore logs on the master server if **logging** option is selected during Prepare-To-Restore step. Following is the location and naming convention for the log files:

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

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

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

Appendix A

NetBackup BMR related appendices

This appendix includes the following topics:

Network services configurations on BMR boot Server

For Network boot based recovery, BMR leverages OS-specific NW boot protocols to start recovery. Different NW configurations like PXE, bootp, DHCP, or TFTP,

would need to be done for network boot recovery depending on the type of OS. Following sections provide the details for specific platforms.

Common UNIX network configuration

The TFTP service must be available. On some of the operating systems, this service is commented out of the **/etc/inetd.conf** file. They must be uncommented and inetd needs to be refreshed for the BMR boot server to function.

The NFS service must be available and the nfsd daemon must be running. **/etc/exports** contain the file system entries which are exposed to other clients over NFS protocol. Make a note that no **/etc/exports** configuration is required to be done manually. BMR handles this configuration automatically.

Red Hat Enterprise Linux network configuration

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

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

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

```
option routers                10.10.5.1;
}
```

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

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

SUSE Linux Network configuration

The following system prerequisites apply only to SUSE Linux systems:

- Install the following RPM packages (unless they are installed already):
  - `nfs-utils`
  - `dhcp-base`
  - `dhcp-server`
  - `inetd`
  - `tftp`
- Enable the `tftp` service by doing the following:
  - Edit the `/etc/inetd.conf` file and uncomment the `tftp` line.
  - Start the service by running the following command:
    `/etc/init.d/inetd restart`
- Modify the **/etc/dhcpd.conf** file to define the networks it serves. You do not have to define host information; hosts are added and removed as needed by the Bare Metal Restore software. The following is an example configuration:

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

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

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

Note: DHCP server needs to be configured on Linux BMR boot server. Any existing DHCP server in the network cannot be used for Linux BMR network-based boot recovery. It is recommended to shut down any other DHCP server while Linux client is network booting over BMR boot server. If the client DHCP boot request goes to the other DHCP server, then network boot recovery fails. This is not a BMR limitation and instead the way this boot protocol works.

Solaris Network configuration

The network configuration boot strategy that is used in Oracle Solaris comprises TFTP, NFS, and BOOTP or Dynamic Host Configuration Protocol (DHCP) NW services. TFTP and NFS services configuration is the same as that explained in earlier section.

See "Common UNIX network configuration" on page 245..

Network boot service configuration for Solaris version 10

No specific DHCP configuration is required on Solaris-10 SPARC architecture as BMR internally handles the required network configurations on boot server while preparing the client for restore.

Solaris 10 x64 architecture requires DHCP and TFTP services configuration to be done on the boot server manually.

To configure DHCP services, perform following steps:

- Run dhcpconfig command to initialize dhcp:
  ```
  dhcpconfig -D -r SUNWfiles -p /var/dhcp
  ```
- Add network table entry.
  ```
  pntadm -C <Network-IP> E.g. : pntadm -C 10.209.4.0
  ```
- Configure subnet/route details.
  ```
  dhtadm -A -m <Network-IP> -d <
  ':option=value:option=value:option=value:'>
  ```
  Example:
  ```
  dhtadm -A -m 10.209.4.0 -d
  ':Subnet=255.255.252.0'':Router=10.209.4.1'':DNSdmain="<yourdomainname>.com"'':DNSserv=10.216.16.101
  10.217.160.131:'
  ```
- Enable DHCP server using following command.
  ```
  svcadm -v enable dhcp-server.
  ```

To configure TFTP services, perform following steps:

- Create TFTP base directory.

```
mkdir /tftpboot
```

- If the TFTP entry is not present in file **/etc/inetd.conf** file, add the following line.
  ```
  tftp dgram udp6 wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
  ```
- Import the configuration changes.
  ```
  /usr/sbin/inetconv
  ```
- Restart TFTP.
  ```
  svcs network/tftp/udp6 svcadm restart network/tftp/udp6
  ```

Note: For Solaris, BMR does not support Solaris WAN-based boot protocol. Though in case of cross subnet network-based boot recovery is intended then Relay Boot server can be used.

Network boot service configuration for Solaris version 11.0 and later

Both x64 and SPARC architecture platforms require DHCP service configuration to be done on BMR boot server. A GUI-based utility, DHCP Manager is required to configure DHCP server on boot server. This utility is wizard-based guiding the required setup steps.

Note: Do not use **dhcpconfig** command-line utility to set up DHCP server in case of Solaris 11.0 and later versions. IP lease time-line related issues have been observed with command-line usage.

HP-UX and AIX NW configuration

In addition to common network services configuration, enable BOOTP service for both HP-UX and AIX platforms. Make sure TFTP, NFS, and BOOTP services are running on your BMR boot server.

Windows Network configuration

Windows BMR Boot server registration enables the following services:

- BMRBD (BMR BOOT server) service
- BMR TFTP Service
- BMR PXE Service

BMR TFTP and PXE services are used in case of network-based boot recovery. Apart from these services, DHCP service is also required.

DHCP service requirements: DHCP server can exist on the same Boot Server host or somewhere on the network.

BMR PXE and TFTP service requirement and configuration:

- Make sure that there is no other PXE server running in the same subnet while BMR NW boot is happening.
  This restriction is more due to the way this network protocol works. In case client NW boot request goes to un-intended PXE server then client NW boot fails. It does not re-direct the request to other valid PXE server in the network. Hence recommendation is to keep only valid BMR PXE service running while NW booting your client for BMR recovery.
- Post BMR boot server registration, navigate to **BMR PXE Configuration Wizard** available on Windows boot server.
  This wizard can be located in **Start > Programs > NetBackup.** This wizard prompts user for DHCP server location. Depending upon your DHCP server location (either same boot server computer or any other computer in the network), the wizard prompts to run `netsh` command-lines on your DHCP server.
- Finish the wizard for successful PXE, TFTP, and DHCP server configuration.

If the Windows boot server is to be installed on an Active Directory Server, let the legacy restore method to share SRTs with restoring clients. Set the following security settings:

Microsoft network server

```
Digitally signed communications (always) – Disabled
```

Microsoft network server

```
Digitally signed communications (if client agrees) -- Enabled
```

About the support for Linux native multipath in BMR

In the data storage domain, multipathing is the ability of a server to communicate with its mass storage devices using more than one physical path; through the buses, controllers, switches, and bridge devices connecting them. Multipathing protects against the failure of paths but not from the failure of a specific storage device. Another advantage of using multipath connectivity is the increased throughput by way of load balancing.

Once the System Administrator has configured the Linux native multipath on the client systems, no additional installation, un-installation, or configuration steps are required from the BMR side to enable the native multipath.

For details about general BMR support for multipath environment, See "BMR support for multi-pathing environment" on page 250.

BMR support for multi-pathing environment

BMR has compliance support for multi-pathing environments. What this means is, during the client's BMR backup which has BMR known multi-pathing environments set up; BMR automatically marks the multi-pathed disks restricted in that client's captured BMR configuration. This restricts the user to use those disks during recovery. Though any file systems running over the multi-pathed disks can be recovered to alternate non-multipathed disks. For example, if the client setup has EMC PowerPath enabled over SAN LUNs, then the BMR backup will mark those SAN LUNs as restricted. The user can recover file systems on top of them to either local disks or other SAN LUNs not having multi-path enabled.

Why this restriction is?

BMR recovery environment has no multi-path software setup and configured (like EMC PP). Hence BMR recovery environment cannot identify multi-path enabled disks on given target hardware. Currently Supported Multi-pathing environments are:

- EMC PowerPath on UNIX/Linux/Windows supported platforms
- Linux Native Multi-pathing

The details of the environment are as described in the following topics:

What does it mean BMR supported multi-pathing environments?

BMR supports only above mentioned multi-pathing environment setups. If the client being BMR backed-up has any one of these multi-pathing enabled; then while capturing client's BMR configuration, BMR resolves multi-paths to exact unique physical disk and shows it in BMR config. Also as mentioned above, BMR marks them restricted and avoids recovery time failure.

What if client has any different multi-pathing environments than above?

BMR backup will fail to identify unique disk names and BMR captured configuration will show multiple-disk names as shown by multi-path software. Also it will not be able to mark the disks restricted automatically. Here you need to copy BMR configuration using administrator GUI (Refer chapter Managing client configurations from NetBackup BMR Administrator's Guide)and identify MP disks and mark them restricted manually. If file systems on top of these MP disks need to be recovered then map them to other non-MP disks. If you ignore MP-based file systems recovery

and restore only operating system then post BMR recovery if the multi-pathed disks are attached to the target host then file systems on top of them may come online automatically. Refer tables *Actions for nonsystem disks* and *Import Actions* for more details.

If the client setup has operating system volumes based on multi-pathing environment, then BMR cannot recover this system.

BMR multipath matrix

Following table describes platform support matrix for BMR multipathing.

Platform	EMC Power Path Version	Native Multipath	SF Version
Windows	EMCPower.5.5.SP1	N/A	SFW 5.1SP1 & SP2
HPUX	EMCPower.HPUX.5.1.SP2.GA	N/A	SF 5.0 MP3
AIX	EMCPower.AIX.5.5.GA	N/A	SF 6.0, SF 6.0RP1
Solaris	EMCPower.SOLARIS.5.5	Not Supported	SF 5.1
RHEL	EMCPower.LINUX.5.6.GA	Supported	Not Supported
SUSE	EMCPower.SUSE_LINUX.5.5.GA	Supported	Not Supported
OEL	EMCPower.LINUX.5.7.GA	Supported	Not Supported

BMR support for virtual environment

Following table lists BMR Boot server and Client versions supported on virtualization technologies.

Hypervisor Type and Version	OS Version on Guest VM
ESX 4.1	Windows, RHEL-Linux, SuSE-Linux
ESX 5.0	Windows, RHEL-Linux, SuSE-Linux, Solaris x64
ESX 5.1	Windows, RHEL-Linux, SuSE-Linux, Solaris x64
IBM VIO AIX 7.1	AIX 6.1 and 7.1 versions
Hyper-V	Windows, RHEL-Linux, SuSE-Linux

Note: Solaris Zones recovery is supported by protecting host operation system. Refer See "Solaris zone recovery support" on page 253.

For information: Following OS recoveries on their supported virtual platforms have not been officially tested or supported but some of the customers have tried them successfully.

- AIX recovery on LPAR
- HPUX recovery of vPar, nPar
- Solaris recovery on LDOM instance

BMR Direct VM conversion support matrix

For the latest support matrix refer to http://www.veritas.com/docs/000006177

About ZFS storage pool support

Zettabyte File System (ZFS) is a combined file system and logical volume manager, which is part of Solaris operating system. ZFS is available on both SPARC and x86-based systems.

Support for ZFS is added in Solaris 10 6/06 ("U2"). When you install Solaris 11.0 ZFS is also installed and set as the default file system.

Bare Metal Restore can protect Solaris 10 Update 11 and later clients that are attached to ZFS storage pools.

BMR 7.6 supports backup and restore of Solaris 10 Update 11 and later clients with the following configurations:

- ZFS Root Pool and Data Pools
- ZFS storage pools on slice
- ZFS file system with zones
- ZFS with SAN boot
- ZFS storage pools along with VxVM and SVM disk groups

Note: All above features are supported on Solaris SPARC and Solaris x86_64 architectures.

BMR does not support Solaris clients with the following configurations:

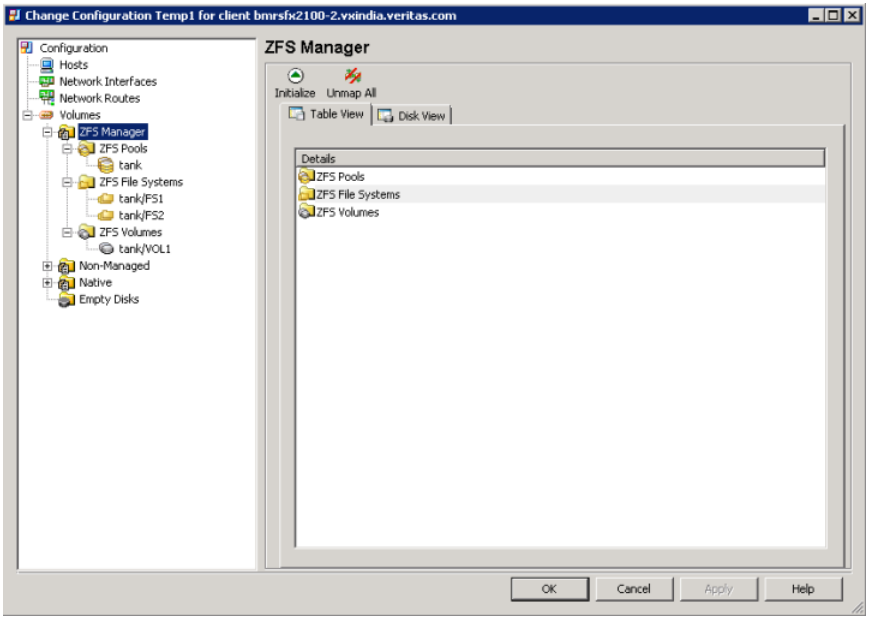
- UFS to ZFS migration
- Different file system on ZFS volumes

To view the ZFS Manager elements and its parameters, do the following:

- In the NetBackup web UI, click Bare Metal Restore > Hosts > Bare Metal Restore Clients. Open the Change Configuration dialog box for the client for which you want to view all associated volumes.

Figure A-1 shows the ZFS Manager GUI screen.

Figure A-1 ZFS Manager UI



Solaris zone recovery support

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

Bare Metal Restore can restore a Solaris system running Zones. Although BMR cannot restore individual non-global zones, all non-global zones in a system are re-created as part of the global zone restoration. If global and non-global zones are based upon ZFS filesystems, then user does not require to do the 'vfstab' configuration."

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

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

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

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

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

2. Test

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

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

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

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

To automate BMR zone restoration, Add entries to the global zone `/etc/vfstab` that cause BMR to restore them (unless unmapped by DDR), as follows:

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

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

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

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

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

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

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

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

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

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

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

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

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

The entry must use two device entries, as follows:

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

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

BMR client recovery to other NetBackup Domain using Auto Image Replication

This appendix explains how BMR and Auto-Image-Replication (A.I.R.) can be leveraged together to do bare metal recovery of primary domain clients onto other clients or disaster recovery domain.

NetBackup A.I.R. feature helps duplicating clients backup image onto defined destination or DR domain NetBackup setup. The feature performs fast backup import automatically providing primary data recovery readiness at DR site.

Refer to the NetBackup Administrator's Guide to learn more about A.I.R. and how to enable it.

For this dual-domain dual-site protection requirement, you need to enable Bare Metal Restore option in Auto Image Replication enabled backup policy. When Auto Image Replication and BMR enabled backup image gets imported at DR domain; NetBackup server checks if the image being imported is BMR enabled. If NetBackup server finds the image is BMR enabled then it automatically imports client BMR configuration as well. You can see client's bare metal restore configuration node appears under UI menu **NetBackup web UI** > **Bare Metal Restore** > **Hosts** > **Bare Metal Restore Clients**.

During BMR configuration import at DR site, BMR master server automatically tunes client configuration for DR site entities like NetBackup primary and media server host names and their IP-addresses. It updates older domain entries with new server details so that BMR recovery environment can approach to DR domain NetBackup servers while recovering client's data. Optionally, you can add or update required host entries manually by copying or editing client's imported BMR configuration. To manually edit client configuration, refer to the *Managing clients and configurations* chapter.

Note: While you restore BMR configurations in a BMR A.I.R. setup, you may come across the following error: `Add an appropriate host entry or host mapping for Name of the host and retry the operation.`

To resolve the issue, you need to add a host in the host database of the DR domain.

See "Adding a host in the host database of the DR domain" on page 257.

Without any manual backup import or configuration change, client can be completely recovered at DR domain using BMR network or media based recovery procedure. You can also create client VM onto DR domain Virtual Environment Server using the **Direct VM creation from backup** feature.

Refer to the *Creating virtual machine from client backup* chapter.

Note: It is recommended to list client short names in NetBackup backup policy at primary domain. If FQDN of DR domain is different than primary domain then client data recovery at DR domain may fail due to mismatch in client domain name. Primary domain **Primary domain** > **backup selection** must enlist minimum OS file systems where NetBackup client is installed. In case of Windows, system state should be listed as well. If these points are not listed, then BMR configuration import at DR site may fail. Refer chapter *Protecting Clients* for more details about defining BMR backup policy.

Note: Make sure BMR master server on DR domain is enabled; otherwise BMR configuration import at DR site fails.

Adding a host in the host database of the DR domain

The clients that appear on the **NetBackup web UI** > **Bare Metal Restore** > **Hosts** > **Bare Metal Restore Clients** screen may not be part of the host database of the DR domain. For successful BMR operations like Prepare To Restore, Prepare to Discover, or Bare Metal Restore, you need to manually add the respective client in the host database. By doing this, a host ID-based certificate is issued to the client during the recovery process and the client can be successfully recovered through BMR.

Note: Cohesity does not recommend adding a host manually except for specific scenarios, such as in a BMR A.I.R. setup. Before adding a host, you must ensure that the host entry that you want to add does not already exist in the host database.

To manually add a client to the host database

1. Run the following command to authenticate your web services login on the master server:

   ```
   bpnbat -login -loginType WEB
   ```

2. Run the following command to add a host:

   ```
   nbhostmgmt -addhost -host host name -server master server
   ```

Secure communication compatibility matrices for BMR for NetBackup 8.1.1 and later releases

This section provides information about the NetBackup boot server, client, and SRT versions compatibility with reference to secure communication.

Table A-1 provides details about the secure communication compatibility for BMR for different NetBackup boot server, client, and SRT version combinations.

Table A-1 Secure communication compatibility matrix for BMR

Boot server	Client to be restored	Client version initiating the restore (SRT client version)	Description
NetBackup 8.1.1 and later*	NetBackup 8.1.1 and later*	NetBackup 8.1.1 and later*	Supported
NetBackup 8.1.1 and later*	NetBackup 8.1.1 and later*	NetBackup 8.0	Not Supported
NetBackup 8.1.1 and later*	NetBackup 8.0	NetBackup 8.1.1 and later*	Not Supported
NetBackup 8.1.1 and later*	NetBackup 8.0	NetBackup 8.0	Supported
NetBackup 8.0	NetBackup 8.1.1 and later*	NetBackup 8.1.1 and later*	Not Supported
NetBackup 8.0	NetBackup 8.1.1 and later*	NetBackup 8.0	Not Supported
NetBackup 8.0	NetBackup 8.0	NetBackup 8.1.1 and later*	Not Supported
NetBackup 8.0	NetBackup 8.0	NetBackup 8.0	Supported

* NetBackup 8.1.2 release onwards BMR operations are supported on AIX and HP-UX platforms.

Management of iSCSI disks in Windows environment

BMR manages the iSCSI disks in Windows as follows:

- During backup, BMR identifies the iSCSI disks, and automatically marks them as **Restricted**. The iSCSI disks are not allowed to be unrestricted.
- As the disks are restricted, you cannot map any volumes with them for DDR.
- BMR does not set up iSCSI disks during the restore process. So, the disks remain restricted, and any volumes lying fully or partially on these disks, are not restored during BMR.
- BMR does not support iSCSI disks when NetBackup is installed on a volume that resides on an iSCSI disk.