

# NetBackup™ Bare Metal Restore 管理者ガイド

UNIX、Windows および Linux

リリース 11.1

# NetBackup™ Bare Metal Restore™ 管理者ガイド

最終更新日: 2026-01-22

## 法的通知と登録商標

Copyright © 2026 Cohesity, Inc. All rights reserved.

Cohesity, Veritas, Cohesity ロゴ、Veritas ロゴ、Veritas Alta, Cohesity Alta, NetBackup は、Cohesity, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。その他の会社名、製品名は各社の登録商標または商標です。

この製品には、Cohesity 社がサードパーティへの帰属を示す必要があるサードパーティ製ソフトウェア（「サードパーティ製プログラム」）が含まれる場合があります。サードパーティプログラムの一部は、オープンソースまたはフリーソフトウェアライセンスで提供されます。本ソフトウェアに含まれる本使用許諾契約は、オープンソースまたはフリーソフトウェアライセンスでお客様が有する権利または義務を変更しないものとします。このCohesity製品に付属するサードパーティの法的通知文書は次の場所で入手できます。

<https://www.veritas.com/about/legal/license-agreements>

本書に記載されている製品は、その使用、コピー、頒布、逆コンパイルおよびリバースエンジニアリングを制限するライセンスに基づいて頒布されます。Cohesity, Inc. からの書面による許可なく本書を複製することはできません。

本書は、現状のまま提供されるものであり、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。Cohesity, Inc. およびその関連会社は、本書の提供、パフォーマンスまたは使用に関連する付随的または間接的損害に対して、一切責任を負わないものとします。本書に記載の情報は、予告なく変更される場合があります。

ライセンスソフトウェアおよび文書は、FAR 12.212 に定義される商用コンピュータソフトウェアと見なされ、Cohesityがオンプレミスまたはホスト型サービスとして提供するかを問わず、必要に応じて FAR 52.227-19 「商用コンピュータソフトウェア - 制限される権利 (Commercial Computer Software - Restricted Rights)」、DFARS 227.7202 「商用コンピュータソフトウェアおよび商用コンピュータソフトウェア文書 (Commercial Computer Software and Commercial Computer Software Documentation)」、およびそれらの後継の規制に定める制限される権利の対象となります。米国政府によるライセンス対象ソフトウェアおよび資料の使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

Cohesity, Inc.  
2625 Augustine Drive  
Santa Clara, CA 95054

<http://www.veritas.com>

## テクニカルサポート

テクニカルサポートはグローバルにサポートセンターを管理しています。すべてのサポートサービスは、サポート契約と現在のエンタープライズテクニカルサポートポリシーに応じて提供されます。サ

ポート内容およびテクニカルサポートの利用方法に関する情報については、次の **Web** サイトにアクセスしてください。

<https://www.veritas.com/support>

次の URL で **Cohesity Account** の情報を管理できます。

<https://my.veritas.com>

現在のサポート契約についてご不明な点がある場合は、次に示すお住まいの地域のサポート契約管理チームに電子メールでお問い合わせください。

世界共通 (日本を除く)

[CustomerCare@veritas.com](mailto:CustomerCare@veritas.com)

日本

[CustomerCare\\_Japan@veritas.com](mailto:CustomerCare_Japan@veritas.com)

## マニュアル

マニュアルの最新バージョンがあることを確認してください。各マニュアルには、2 ページ目に最終更新日が記載されています。最新のマニュアルは、**Cohesity** の **Web** サイトで入手できます。

## Cohesity Services and Operations Readiness Tools (SORT)

**Cohesity SORT (Service and Operations Readiness Tools)** は、特定の時間がかかる管理タスクを自動化および簡素化するための情報とツールを提供する **Web** サイトです。製品によって異なりますが、**SORT** はインストールとアップグレードの準備、データセンターにおけるリスクの識別、および運用効率の向上を支援します。**SORT** がお客様の製品に提供できるサービスとツールについては、次のデータシートを参照してください。

[https://sort.veritas.com/data/support/SORT\\_Data\\_Sheet.pdf](https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf)

# 目次

第 1 章	Bare Metal Restore の概要 .....	11
	Bare Metal Restore について .....	11
	BMR を使用したサーバー DR 保護 .....	12
	BMR の保護フェーズ図 .....	13
	BMR での UEFI-GPT のサポート .....	14
第 2 章	BMR の構成 .....	16
	BMR ソフトウェアのインストールについて .....	16
	BMR サーバー構成の前提条件 .....	16
	BMR サーバーの構成 .....	17
	BMR マスターサーバーの構成 .....	17
	Windows システムへの BMR マスターサーバーの設定 .....	17
	BMR ブートサーバーの構成 .....	18
	BMR サーバーの無効化 .....	21
	BMR マスターサーバーの無効化 .....	21
	BMR ブートサーバーの無効化 .....	22
第 3 章	クライアントの保護 .....	23
	.....	23
	BMR クライアントのバックアップ .....	23
	BMR クライアントをバックアップするためのポリシーの構成 .....	23
	複数のポリシーでの同じクライアント名の使用 .....	26
	完全バックアップの実行について .....	26
	リストア後の完全バックアップの実行について .....	26
	正常なバックアップの保障 .....	26
	UNIX または Linux でのカスタムファイルの保存 .....	27
	クライアントバックアップの監視 .....	28
	BMR 関連の他の NetBackup プロパティ .....	28
	特定のユースケースでのクライアントの保護 .....	29
	Storage Foundation for Windows Clients .....	29
第 4 章	リストア環境の設定 .....	30
	リカバリ手順 .....	30
	ブートサーバーソフトウェアのインストール .....	31

	共有リソースツリー .....	31
	クライアント固有のリソースの追加 .....	32
	ブートメディアの使用 .....	32
	クライアントのリストア準備 .....	33
<b>第 5 章</b>	<b>共有リソースツリー .....</b>	<b>34</b>
	共有リソースツリーについて .....	34
	共有リソースツリーの前提条件 .....	35
	共有リソースツリーの作成 .....	35
	<b>Windows</b> の <b>SRT</b> の作成 .....	37
	<b>UNIX</b> または <b>Linux</b> の <b>SRT</b> の作成 .....	52
	共有リソースツリーの管理 .....	66
	共有リソースツリーへのソフトウェアの追加 .....	66
	共有リソースツリーのインポート .....	72
	共有リソースツリーのコピー .....	72
	共有リソースツリーの削除 .....	74
	<b>SRT</b> の排他的な使用を有効にまたは無効にする方法 .....	75
	破損した共有リソースツリーの修復 .....	76
	共有リソースツリーの無効なロックの解除 .....	76
	ブートメディアの管理 .....	77
	<b>Windows</b> のサポート対象のブートメディアについて .....	78
	<b>CD</b> または <b>DVD</b> の書き込みについて .....	78
	<b>UNIX</b> および <b>Linux</b> のブートメディアの作成 .....	79
	<b>Windows</b> クライアントのブートメディアの作成 .....	82
<b>第 6 章</b>	<b>クライアントのリストア .....</b>	<b>83</b>
	<b>BMR</b> リストア処理 .....	84
	クライアントのリストアを準備する方法 .....	86
	<b>BMR</b> ディスクリカバリ動作 .....	88
	リストア準備オプションによる <b>BMR</b> のディスクの処理 .....	90
	リストア準備オプションによる <b>BMR</b> のディスククラスの処理 .....	90
	オペレーティングシステムまたは <b>Volume Manager</b> のインポート処理 .....	92
	ネットワークブートによる <b>BMR</b> クライアントのリストアについて .....	93
	ネットワークブートによる <b>AIX</b> クライアントのリストア .....	94
	ネットワークブートによる <b>HP-UX</b> クライアントのリストア .....	98
	ネットワークブートによる <b>Linux</b> クライアントのリストア .....	101
	ネットワークブートによる <b>Solaris</b> クライアントのリストア .....	103
	ネットワークブートによる <b>Windows</b> クライアントのリストア .....	105
	メディアブートによる <b>BMR</b> クライアントのリストアについて .....	107
	メディアブートによる <b>AIX</b> クライアントのリストア .....	109
	メディアブートによる <b>HP-UX</b> クライアントのリストア .....	110

メディアブートによる <b>Linux</b> クライアントのリストア .....	112
メディアブートによる <b>Solaris</b> クライアントのリストア .....	114
メディアブートによる <b>Windows</b> クライアントのリストア .....	116
汎用的な <b>BMR</b> リストア .....	117
ハードウェアの汎用的な検出 .....	119
指定した時点へのリストアについて .....	120
指定した時点へのリストア処理について .....	121
指定した時点へのリストア構成の作成 .....	121
異なるディスクへのリストアについて .....	123
<b>Dissimilar Disk Restore</b> 処理について .....	123
<b>DDR</b> 用のリストア構成の作成 .....	124
異なるディスクへのクライアントのリストア .....	125
異なる システムへのリストア .....	128
<b>Dissimilar System Restore</b> について .....	129
新しいシステムの構成の検出について .....	130
編集可能な <b>DSR</b> 構成の作成 .....	130
<b>NIC</b> ドライバと <b>MSD</b> ドライバの追加について .....	130
ネットワークインターフェースの変更について .....	131
リストア構成でのディスクのマッピングについて .....	132
ブートメディアの作成について .....	132
クライアントのリストアについて .....	133
システムのリストア後の最初のログオン .....	133
<b>NetBackup</b> メディアサーバーのリストアについて .....	133
代替メディアサーバーの構成について .....	134
メディアサーバーのリストア .....	135
<b>BMR</b> ブートサーバーのリストアについて .....	136
<b>AWS RHEL</b> および <b>Windows VM</b> クライアントのリストアについて .....	137
<b>BMR AWS RHEL</b> および <b>Windows VM</b> リストアの前提条件 .....	137
制限事項および考慮事項 .....	138
外部プロシージャについて .....	138
外部プロシージャのポイントと名前 .....	139
外部プロシージャの管理について .....	140
外部プロシージャの指定 .....	141
外部プロシージャのデータ転送について .....	141
外部プロシージャとの対話について .....	142
外部プロシージャのログ 例 .....	143
外部プロシージャの操作状態 .....	144
外部プロシージャの終了コードについて .....	144
外部プロシージャのエラー処理について .....	144
外部プロシージャの環境変数について .....	145
<b>SAN</b> (ストレージエリアネットワーク) のサポートについて .....	148
<b>Solaris</b> の <b>SAN</b> に接続されたボリュームがマッピングされていないま まの場合にそれらをリストアする方法 .....	149

	Windows クライアントでの SAN と Dissimilar System Restore につ いて .....	149
	複数のネットワークインターフェースのサポートについて .....	150
	ゲートウェイを使ったクライアント構成について .....	150
	リストア時のポートの使用 .....	152
<b>第 7 章</b>	<b>Windows ドライバパッケージの管理</b> .....	154
	Windows ドライバパッケージについて .....	154
	Windows ドライバパッケージの追加 .....	155
	Windows がインストールされている場合の正しいドライバの検索 .....	156
	Windows ドライバパッケージの削除 .....	156
<b>第 8 章</b>	<b>クライアントおよび構成の管理</b> .....	157
	クライアントと構成について .....	157
	構成のコピー .....	158
	構成の検出 .....	159
	構成の変更 .....	162
	構成の削除 .....	163
	クライアントの削除 .....	164
	クライアント構成プロパティ .....	164
	構成の概略 プロパティ .....	165
	[デバイスおよびドライバ (Devices & Drivers)] プロパティ .....	167
	[ホスト (Hosts)] プロパティ .....	170
	[ネットワークインターフェース (Network Interfaces)] プロパティ .....	172
	[ネットワークルート (Network Routes)] プロパティ .....	177
	[ボリューム (Volumes)] プロパティについて .....	178
<b>第 9 章</b>	<b>BMR ブートサーバーの管理</b> .....	192
	ブートサーバーについて .....	192
	ブートサーバー要件 .....	193
<b>第 10 章</b>	<b>トラブルシューティング</b> .....	198
	CD/DVD からのブートの問題 .....	199
	リストアにかかる時間が長い .....	200
	Solaris メディアブートネットワークパラメータの問題 .....	201
	BMR 構成が誤って削除された場合にクライアントを回復する方法 .....	201
	BMR リストアの後の最初のブートが UNIX プラットフォームで失敗します .....	202
	クライアントのネットワークベースのブートの問題 .....	202
	Windows クライアントのリカバリ中のバックアップエラーの検証 .....	203

VM は 32 ビットアーキテクチャ Windows OS で実行されている仮想マシンへの BMR 物理的バックアップ変換後にブートするのに長い時間がかかります。 .....	205
仮想マシンの変換ジョブへの BMR が有効に設定されている物理的バックアップが、Windows プラットフォームで失敗する .....	205
クライアントバックアップからの仮想マシンの作成に関する問題のトラブルシューティング .....	205
仮想マシン変換クライアントのリストにクライアント名が表示されない .....	206
仮想マシン作成のジョブの送信中のエラー .....	206
仮想マシン作成のジョブの失敗 .....	207
システムブート時や BMR の初回ブート時に Solaris 11 以降の多くのサービスが警告メッセージを表示する .....	207
BMR のリストア後の初回ブート時に、Solaris 11 以降の Solaris ゾーンリカバリを再構成するまでに時間がかかる .....	208
テキストインストーラのパッケージがカスタマイズされた AI ISO 内に存在しない場合、Solaris BMR のリストア操作に失敗する .....	208
複数のデバイスに基づく OS 構成では /boot パーティションが独立したパーティション上になければならない .....	208
ZFS ストレージプールを使ったクライアントのリストア後、初回のブート中に、複数のエラーメッセージが表示されることがある .....	209
BMR が ZFS メタデータをフォーマットまたは消去しないことがある .....	209
自動イメージレプリケーションおよび BMR を使って保護する場合のクライアントの短縮名の指定 .....	210
クライアントリストアの成功後もリストアタスクがディザスタリカバリドメインに完了状態で保持されることがある .....	210
クライアントに有効なホスト ID ベースの証明書があっても、マスターサーバーとクライアント間の通信が失敗する場合があります .....	211
リストア後に HP-UX の自動ブートに失敗することがある .....	211
Solaris クライアントのリストア準備が機能しないことがある .....	212
Netbackup 8.1 をインストールしている Windows (x64) での NetBackup 8.0 を対象とした仮想インスタンスコンバータ (VIC) ホストの使用はサポートされません。 .....	212
アップグレード後のブートサーバーのバージョンの不一致による PTR または PTD エラー .....	212
リストア準備および検出準備のエラーメッセージと、BMR 用の安全な通信に関連する bmrprep コマンド .....	213
Solaris x86 11.2 以降のクライアントのメディアリストアでメンテナンスモードのユーザー名とパスワードを求められる場合がある .....	217
クライアントの PTD タスクが正常に完了した後も検出タスクが完了中の状態のままになることがある .....	218
クライアントが正常にリストアされても BMR リストアタスクが完了中の状態のまま変わらないことがある .....	218

	共有リソースツリー (SRT) の作成中にブートサーバーとクライアントでバックアップ操作が開始されると、BMR のリストア後に SRT の作成が失敗してエラーが発生する .....	219
	バックアップ時に BMR 情報の受信中に発生するエラー .....	221
	BMR のバックアップジョブとリストアジョブの詳細が NetBackup Web UI のアクティビティモニターに表示されない .....	222
<b>第 11 章</b>	<b>クライアントバックアップからの仮想マシンの作成</b> .....	223
	バックアップからの仮想マシンの作成について .....	223
	BMR 物理マシンに対する仮想マシンの作成の利点およびユースケース .....	224
	仮想マシン作成のための配置ダイアグラム .....	225
	クライアント-VM 変換プロセスのフロー .....	226
	バックアップから VM を作成する際の前提条件 .....	227
	バックアップからの仮想マシンの作成 .....	228
	仮想マシン変換クライアント .....	228
	クライアントバックアップを VM に変換する .....	229
	[仮想マシン (Virtual Machine)] のオプション .....	232
	仮想マシン変換ストレージ先 .....	234
	ネットワーク接続の選択 .....	234
	仮想マシン変換の概略 .....	235
	リストアの完了後に実行される直接仮想マシン (VM) の変換 (物理から仮想) タスク .....	236
	仮想マシン変換タスク .....	237
	リストアタスクのプロパティ .....	237
	カスタム構成の作成 .....	238
	仮想マシン作成の CLI .....	240
<b>第 12 章</b>	<b>Bare Metal Restore アクティビティの監視</b> .....	243
	BMR リストアタスクの監視 .....	243
	バックアップジョブの監視 .....	245
	VM 作成ジョブの監視 .....	246
	BMR ログ .....	248
	BMR ログのオリジネータ ID .....	249
	統合ログとログファイルを管理するためのコマンド .....	250
	BMR リストアログ .....	250
<b>付録 A</b>	<b>NetBackup BMR 関連の付録</b> .....	251
	BMR ブートサーバーに対するネットワークサービスの設定 .....	251
	共通の UNIX ネットワーク構成 .....	252

Red Hat Enterprise Linux のネットワーク構成 .....	252
SuSE Linux ネットワークの構成 .....	253
Solaris でのネットワークの構成 .....	254
HP-UX および AIX NW の設定 .....	255
Windows ネットワークの構成 .....	255
BMR における Linux のネイティブマルチパスのサポート .....	256
BMR によるマルチパス環境のサポート .....	257
BMR のマルチパスの表 .....	258
BMR による仮想環境のサポート .....	258
BMR における直接 VM 変換のサポート表 .....	259
ZFS ストレージプールのサポートについて .....	259
Solaris のゾーンリカバリのサポート .....	261
自動イメージレプリケーションを使用した他の NetBackup ドメインへの BMR	
クライアントのリカバリ .....	263
DR ドメインのホストデータベースへのホストの追加 .....	265
NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換性の	
表 .....	265
Windows 環境での iSCSI ディスクの管理 .....	266

# Bare Metal Restore の概要

この章では以下の項目について説明しています。

- [Bare Metal Restore について](#)
- [BMR を使用したサーバー DR 保護](#)
- [BMR の保護フェーズ図](#)
- [BMR での UEFI-GPT のサポート](#)

## Bare Metal Restore について

NetBackup Bare Metal Restore (BMR) は NetBackup のサーバーリカバリオプションです。BMR では、サーバーのリカバリ処理が自動化され簡素化されるため、オペレーティングシステムの再インストールまたはハードウェアの構成を手動で実行する必要がなくなります。広範囲なトレーニングや面倒な管理なしでサーバーを復元できます。

BMR は、オペレーティングシステム、システム構成、およびすべてのシステムファイルとデータファイルを次の手順でリストアします。

- NetBackup マスターサーバーから 1 つのコマンドまたはワンクリックを実行します。
- クライアントを自動的にリカバリするには、クライアントをレポートします。  
システムのバックアップや再インストールを個別に行う必要はありません。

表 1-1 に、BMR 保護ドメインのコンポーネントを示します。

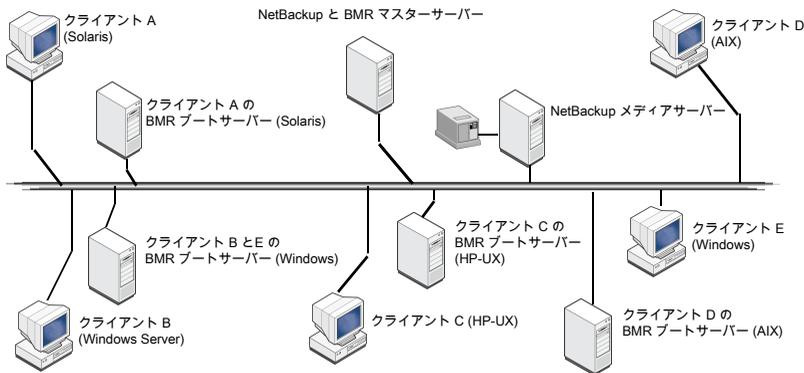
表 1-1 BMR コンポーネント

コンポーネント	説明
NetBackup および BMR のマスターサーバー	NetBackup マスターサーバーは、保護されたクライアントシステムのバックアップおよびリストアを管理します。また、NetBackup マスターサーバーは、BMR マスターサーバーをホスティングし、BMR の操作を管理します。

コンポーネント	説明
NetBackup メディアサーバー	NetBackup メディアサーバーはクライアントファイルが格納されているストレージデバイスを制御します。
BMR ブートサーバー	ブートサーバーは、システムリカバリや共有リソースツリー (SRT) などの重要なリソースを含む、保護対象のクライアントの再構築に必要な環境を提供します。共有リソースツリーは、NetBackup でオリジナルファイルをリストアできるように保護対象のシステムを再構築するために使われるソフトウェアを含んでいます。このソフトウェアには、オペレーティングシステムのソフトウェアと NetBackup クライアントのソフトウェアがあります。
クライアント	クライアントとは、NetBackup によってバックアップされ、BMR によって保護されるシステムのことで、他のアプリケーションやデータ用のサーバー、NetBackup メディアサーバー、または BMR ブートサーバーがクライアントとなる場合もあります。

環境に応じて、サーバーコンポーネントは、同一のコンピュータ、別のコンピュータまたは複数のコンピュータに、配置することができます。

図 1-1 BMR 保護ドメインの例



## BMR を使用したサーバー DR 保護

BMR を使用した障害からサーバーを保護する処理は 3 つのフェーズで生じます。これらのフェーズを次に示します:

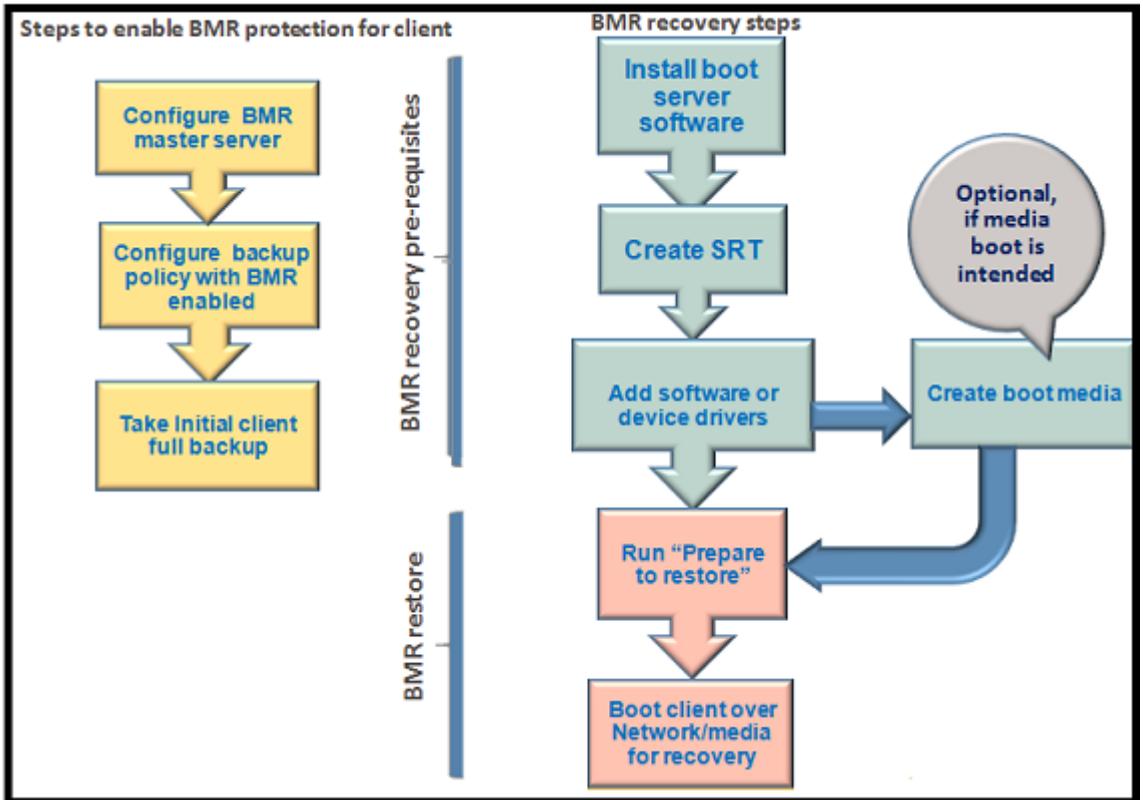
- BMR 有効バックアップ  
 Netbackup バックアップポリシーはクライアントバックアップ中にクライアントシステム骨組情報がバックアップされるように BMR が有効である必要があり、DR が意図される場合にクライアントをリカバリするために必要です。このシステム骨組情報は OS 詳

細、ディスク情報、ボリューム詳細、ファイルシステム情報およびネットワーク情報などで構成されます。BMR バックアップ処理について詳しくは、クライアントの保護の章を参照してください

- リカバリの前提条件  
リストア前提条件の設定はクライアントの DR が意図される前であれば、いつでも行えます。リカバリの遅延を避けるため、わずかに先行してこの前提条件を設定することが推奨されます。このフェーズの間に、リカバリに重要なソフトウェア、すなわち、共有リソースツリーを BMR ブートサーバーに準備する必要があります。この SRT はクライアントリカバリをするためにステージング環境を形成します。同じオペレーティングシステムファミリーに属しているクライアントをリカバリするため、単一の SRT を使うことができます。リカバリの前提条件について詳しくは、リストア環境のセットアップの章を参照してください
- クライアントリカバリ  
これは、クライアントコンピュータがリカバリ環境にブートする実際のクライアントリカバリフェーズです。クライアントは単一のコマンドラインまたはクリック 1 回の実行によってリカバリを準備する必要があります。BMR はネットワークベースのブートとメディアベースのブートという 2 つのリカバリ方式をサポートします。クライアントリカバリ処理について詳しくは、クライアントのリストアの章を参照してください。プライマリドメインホストを DR ドメインにリカバリするため、BMR を NetBackup の自動イメージレプリケーションセットアップで活用することもできます。  
詳しくは、p.263 の「[自動イメージレプリケーションを使用した他の NetBackup ドメインへの BMR クライアントのリカバリ](#)」を参照してください。

## BMR の保護フェーズ図

次の図は、バックアップからリストアまでの BMR プロセスの概要です。



Microsoft ADK をダウンロードし、オフラインブートサーバーに SRT を作成することに関するその他の図については、オンラインとオフラインのブートサーバーでの SRT の作成の図を参照してください。p.43 の「オフラインのブートサーバーまたはホストでの SRT の作成」を参照してください。

## BMR での UEFI-GPT のサポート

表 1-2 は、Linux および Windows オペレーティングシステムにおける BMR での UEFI-GPT のサポートについての情報を示しています。

表 1-2 BMR での UEFI-GPT に導入されたサポート

オペレーティングシステム	導入されたサポート
Red Hat Enterprise Linux 7.x, 8.x	<p>NetBackup BMR では、GUID パーティションテーブル (GPT) ディスクタイプと BIOS クライアントに類似した Dissimilar Disk Restore (DDR) 機能をサポートしています。UEFI マシン上でサポートされる BMR 機能は、セルフリストア、DDR、および Dissimilar System Recovery (DSR) です。Dissimilar System Restore サポートは、UEFI クライアントに拡張されます。詳しくは、テクニカルノートを参照してください。</p> <p><a href="https://www.veritas.com/support/ja_JP/article.000034868">https://www.veritas.com/support/ja_JP/article.000034868</a></p> <p>新しく作成された共有リソースツリーは、BIOS および UEFI マシンのブートに使用できます。また、VFAT ファイルシステムもサポートされています。</p> <p><b>メモ:</b> Linux マルチデバイスのサポートは限定的であるため、BMR は一部の構成を正確にリストアできない場合があります。</p>
Windows	<ul style="list-style-type: none"> <li>■ UEFI、およびレガシー BIOS でブートされたマシンの場合、NetBackup BMR は、レガシー MBR と GUID パーティションテーブル (GPT) ディスクタイプの両方に対して、セルフリストア、DDR (Dissimilar Disk Recovery)、DSR (Dissimilar System Recovery) をサポートします。</li> <li>■ UEFI システムと GPT ディスクが搭載された BIOS システムの場合、NetBackup BMR はダイレクトな仮想マシン作成 (物理から仮想) をサポートしません。</li> </ul> <p>新しく作成された共有リソースツリーは、BIOS および UEFI マシンのブートに使用できます。また、FAT32 ファイルシステムもサポートされています。</p>

# BMR の構成

この章では以下の項目について説明しています。

- [BMR ソフトウェアのインストールについて](#)
- [BMR サーバー構成の前提条件](#)
- [BMR サーバーの構成](#)
- [BMR サーバーの無効化](#)

## BMR ソフトウェアのインストールについて

Bare Metal Restore には次のソフトウェアコンポーネントが含まれています。

- BMR の操作を制御するマスターサーバー。NetBackup マスターサーバーをインストールした後で、BMR マスターサーバーを構成する必要があります。
- システムの再構築に使用されるリソースを管理および提供するブートサーバー。BMR では、ブートサーバーは NetBackup クライアントにバンドルされており、NetBackup クライアントと共にインストールされます。NetBackup クライアントをインストールした後で、BMR ブートサーバーを BMR マスターサーバーに登録する必要があります。
- NetBackup クライアントソフトウェアとともにインストールされるクライアントソフトウェア。特別なインストールまたは構成は必要ありません。

後続の項では、BMR のインストールについて説明します。

## BMR サーバー構成の前提条件

BMR ソフトウェアをインストールする前に、『NetBackup リリースノート UNIX、Windows および Linux』を参照してください。BMR のサポート対象のシステムとクラスタ、依存関係、制限事項、オペレーティングシステムのインストール前提条件について説明されています。

## BMR サーバーの構成

Bare Metal Restore コンポーネントは NetBackup のインストール時にインストールされます。ただし、BMR を使用するには次の操作を行う必要があります。

- p.17 の「[BMR マスターサーバーの構成](#)」を参照してください。
- p.18 の「[BMR ブートサーバーの構成](#)」を参照してください。

## BMR マスターサーバーの構成

NetBackup をインストールした後、BMR マスターサーバーを設定し、BMR データベースを作成します。

Bare Metal Restore マスターサーバーは NetBackup マスターサーバーと一緒にインストールされます。インストールした後で Bare Metal Restore マスターサーバーを構成する必要があります。

NetBackup マスターサーバーのインストールについては、『[NetBackup 管理者ガイド](#)』を参照してください。

クラスタ環境では、アクティブノードの BMR マスターサーバーのみを構成します。

### BMR データベースを作成し、BMR マスターサーバーを設定する方法

- 1 NetBackup マスターサーバーがインストールされているシステムに、root ユーザーとしてログオンします。
- 2 BMR データベースを構成するには、次のコマンドを実行します。

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

BMR マスターサーバーを設定した後、NetBackup クライアントから BMR の必要な情報を収集するようにバックアップポリシーを構成できます。

---

**メモ:** マスターサーバーで `bmrsetupmaster` コマンドを実行した後、NetBackup サービスを再起動する必要があります。

---

## Windows システムへの BMR マスターサーバーの設定

マスターサーバーのセットアップウィザードを使って、Bare Metal Restore マスターサーバーを Windows システムに設定します。

## Windows システムに BMR マスターサーバーを設定する方法

- 1 Windows の BMR マスターサーバーで、[スタート]メニューから[プログラム]、[Cohesity NetBackup]、[Bare Metal Restore -- マスターサーバーのセットアップ (Master Server Setup)]の順に選択します。
- 2 プロンプトに従って BMR マスターサーバーを設定します。  
情報を入力する必要はありません。ウィザードで、マスターサーバーの設定に必要なすべての手順が実行されます。
- 3 クラスタ環境で BMR を設定する場合、この処理の完了後にアクティブノードを解凍します。  
実行しているクラスタのソフトウェアのサービスグループを解凍する方法に関する詳細情報が利用可能です。  
[『高可用性の環境管理者ガイド』NetBackup のクラスタ化のセクション](#)を参照してください。

## BMR ブートサーバーの構成

BMR ブートサーバーソフトウェアは、NetBackup クライアントのインストール時にインストールされます。個別のインストールは必要ありません。ただし、ブートサーバーを登録する必要があります。

すべての NetBackup サーバーには、デフォルトで NetBackup クライアントソフトウェアが含まれています。したがって、NetBackup サーバーまたはクライアント (BMR がそのプラットフォームをサポートしている場合) のいずれかで BMR ブートサーバーを実行できます。ブートサーバーは、共有リソースツリー (SRT) などのリソースを含む、保護対象のクライアントの再構築に必要な環境を提供します。

---

**メモ:** BMR ブートサーバーを構成する前に、BMR マスターサーバーを NetBackup プライマリサーバーで構成する必要があります。

---

### ブートサーバーのホストの選択について

BMR はブートサーバー用の特定のシステムと環境が必要です。ブートサーバーを実行するホストを選択する前に、ブートサーバー要件を確認してください。

p.193 の「[ブートサーバー要件](#)」を参照してください。

### ブートサーバーの前提条件

ネットワークベースの BMR のリカバリが意図されている場合、BMR のブートサーバーで構成する必要のあるネットワークサービスはほとんどありません。これらの構成はプラットフォームによって変わります。

詳しくは、p.251 の「[BMR ブートサーバーに対するネットワークサービスの設定](#)」を参照してください。を参照してください。

## BMR ブートサーバーのセットアップ

既存の NetBackup システムに BMR ブートサーバーを設定するには、次の手順を実行します。

---

**メモ:** NetBackup ホストの BMR ブートサーバー構成する前に、NetBackup ホストが NetBackup プライマリサーバーで構成されていることを確認してください。NetBackup クライアントを NetBackup プライマリサーバーに登録する方法について詳しくは、[『NetBackup 管理者ガイド』](#)を参照してください。

---

### BMR ブートサーバーに登録する方法

- 1 NetBackup をインストールするディレクトリに移動します。

UNIX の場合: /usr/opensv/netbackup/bin

Windows の場合: c:\program files\veritas\netbackup\bin

- 2 ブートサーバーホスト上で次のコマンドを実行します。

```
bmrsetupboot -register
```

コマンドを実行した後、NetBackup Web UI にブートサーバー名 ([Bare Metal Restore]、[ホスト (Hosts)]、[ブートサーバー (Boot Servers)]の順に選択) が表示されます。このコマンドによって BMR ブートサーバーのデーモンの実行が開始されます。

## UNIX クラスタ内の BMR ブートサーバー

次に、クラスタ環境で BMR ブートサーバーを使用するための一般的な手順を示します。

- クラスタアプリケーションで、BMR ブートサーバー機能を提供するノードに仮想 IP アドレスを設定します。
- 各ノードに NetBackup クライアントソフトウェアをインストールします。NetBackup クライアントがインストールされている各ノード上に Bare Metal Restore ブートサーバーに登録できます。  
[『NetBackup インストールガイド』](#)を参照してください。NetBackup クライアントソフトウェアには BMR ブートサーバーのソフトウェアが含まれています (BMR がそのプラットフォームをサポートしている場合)。
- 各ノードで、NetBackup クライアント名を仮想 IP アドレスを解決する名前に設定します。システムで、bp.conf ファイル内の最後の CLIENT\_NAME エントリにこの名前を使用します。
- アクティブなノードにブートサーバーを設定します。

p.19 の「[BMR ブートサーバーのセットアップ](#)」を参照してください。

- ブートサーバーデーモンの次の開始および停止スクリプトを呼び出すクラスタアプリケーションリソースを作成します。

```
/usr/opensv/netbackup/bin/rc.bmrbd start
/usr/opensv/netbackup/bin/rc.bmrbd stop
```
- SRT を作成する場合、共有ディスク上のファイルシステムの場所を選択します。
- ブートサーバーがフェールオーバーしてリストアタスクが完了していない場合には、完了していない各リストアタスクで新しいリストア準備処理を実行します。

## Windows クラスタ内の BMR ブートサーバー

BMR ブートサーバーをクラスタ化できるシステムについては、『[NetBackup リリースノート UNIX、Windows および Linux](#)』を参照してください。

次に、クラスタ環境で BMR ブートサーバーをインストールして使用するための一般的な手順を示します。

- クラスタアプリケーションで、BMR ブートサーバー機能を提供するノードに仮想 IP アドレスを設定します。
- 各ノードに NetBackup クライアントソフトウェアをインストールします。
- 各ノードで次を実行します。
  - NetBackup クライアント名を、仮想 IP アドレスを解決する名前に設定します。
  - バックアップ、アーカイブおよびリストアインターフェースを起動します。
  - NetBackup クライアント名を[NetBackup マシンおよびポリシー形式の指定 (Specify NetBackup Machines and Policy Type)]ダイアログボックスにクライアント名として入力します。
  - NetBackup クライアント名を現在のクライアントにします。
- 各ノードに BMR ブートサーバーソフトウェアをインストールします。ブートサーバーソフトウェアをインストールする前に、仮想アドレスを各ノードに切り替えます。
- ブートサーバーサービスの開始および停止スクリプトを呼び出すクラスタアプリケーションリソースを作成します。

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

- SRT を作成する場合、共有ディスク上のファイルシステムの場所を選択します。
- ブートサーバーがフェールオーバーし、処理予定のリストアタスクが存在する場合、保留中の各リストアタスクで新たにリストア準備処理を実行します。

すべての NetBackup マスターサーバーには、デフォルトで NetBackup クライアントソフトウェアが含まれています。したがって、NetBackup マスターサーバーまたはクライアント (BMR がそのプラットフォームをサポートしている場合) のいずれかで BMR ブートサーバーを実行できます。

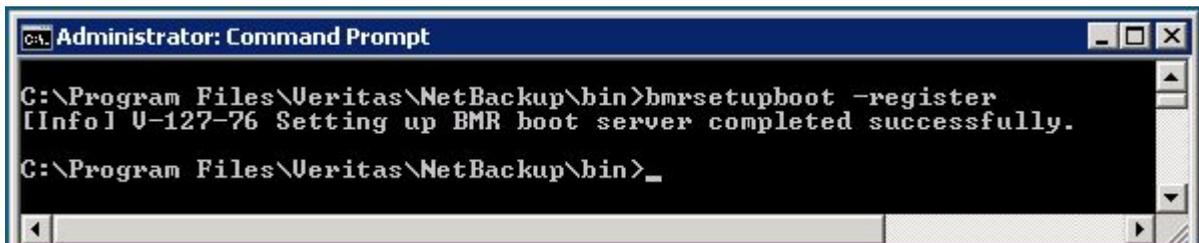
### Windows システムで BMR ブートサーバーを登録する方法

- 1 BMR ブートサーバーをインストールするサーバーに、管理者としてログオンします。
- 2 command プロンプトを開き、NetBackup のディレクトリに移動します。

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

- 3 BMR ブートサーバーを登録します。コマンドプロンプトを閉じます。

次のスクリーンショットは[BMR ブートサーバー (BMR Boot Server)]の登録を示しています。



## BMR サーバーの無効化

BMR コンポーネントはアンインストールしません。そうせずに、無効にします。NetBackup BMR マスターサーバーは NetBackup マスターサーバーにバンドルされており、BMR ブートサーバーは NetBackup クライアントとともにインストールされます。NetBackup マスターサーバーとクライアントをアンインストールすると、BMR マスターサーバーとブートサーバーはシステムから削除されます。NetBackup のアンインストールについて詳しくは『[NetBackup 管理者ガイド](#)』を参照してください。

### BMR マスターサーバーの無効化

BMR マスターサーバーと BMR データベースを無効化し、BMR ライセンスを削除するには、次の手順を実行します。

ライセンスを削除した後、BMR は使用できなくなります。

### BMR マスターサーバーを無効化する方法

- 1 NetBackup マスターサーバーがインストールされているシステムに、**root** ユーザーとしてログオンします。
- 2 BMR マスターサーバーを無効化するには、次のコマンドを実行します。

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

たとえば、UNIX または Linux システムの場合には次を実行します。

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

Windows マスターサーバーの場合には、次を実行します。

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

## BMR ブートサーバーの無効化

次の手順で、BMR ブートサーバーを無効化します。

### BMR ブートサーバーを無効化する方法

- 1 BMR ブートサーバーのホストに **root** ユーザーとしてログオンします。
- 2 BMR ブートサーバーを登録解除するには、BMR ブートサーバーで次のコマンドを実行します。

```
%usr%\opensv\netbackup\bin\bmrsetupboot -deregister
```

たとえば、Windows で次のコマンドを実行します。

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

UNIX または Linux の場合には次を実行します。

```
%usr%\opensv\netbackup\bin\bmrsetupboot -deregister
```

コマンドが問題なく実行されれば、NetBackup Web UI の [NetBackup Administrator Web UI]、[Bare Metal Restore]、[ホスト (Hosts)]、[ブートサーバー (Boot servers)] にブートサーバーインスタンスが表示されません。登録を解除すると、BMR ブートサーバーのデーモンの実行が停止します。

---

**メモ:** BMR ブートサーバーを無効化しても、BMR ブートサーバーによってホスティングされている SRT は削除されません。SRT は、別の BMR ブートサーバーまたは同じブートサーバー (将来再度有効化された場合) でインポートする必要がある場合のために存在します。Windows で登録解除する BMR ブートサーバーでは、BMR PXE と TFTP サービスが、BMR ブートサーバーサービスと共に削除されます。

---

# クライアントの保護

この章では以下の項目について説明しています。

- 
- [BMR クライアントのバックアップ](#)
- [クライアントバックアップの監視](#)
- [特定のユースケースでのクライアントの保護](#)

## BMR クライアントのバックアップ

BMRを使用してクライアントのディザスタリカバリを実行するには、**NetBackup** バックアップポリシーを **BMR** 用に構成する必要があります。クライアントをリカバリするには、**BMR** 対応バックアップポリシーに 1 つ以上の完全バックアップが必要です。

保護対象となる各クライアントは、完全バックアップを実行する1つ以上のポリシーによって、定期的にバックアップする必要があります。ポリシーによって、累積増分バックアップまたは差分増分バックアップを実行することもできますが、完全バックアップを実行する必要があります。

バックアップにより、コンピュータのファイルは **NetBackup** メディアサーバーが管理するストレージデバイスに保存されます。バックアップにより、クライアントの構成は **BMR** マスターサーバーに保存されます。

**BMR** 保護用に構成されたポリシーでクライアントのバックアップを作成すると、保護対象のクライアントとして **BMR** に登録されます。登録されると、**NetBackup Web UI** の [Bare Metal Restore]、[ホスト (Hosts)]、[Bare Metal Restore クライアント (Bare Metal Restore Clients)] ビューに表示されます。

## BMR クライアントをバックアップするためのポリシーの構成

1 台のクライアントの保護に、1 つ以上のポリシーを使用できます。

BMR クライアントを保護するための要件を次に示します。

- ポリシー形式は[MS-Windows] (Windows クライアントの場合) または[標準 (Standard)] (UNIX または Linux クライアントの場合) のいずれかである必要があります。
- ポリシーには、[Bare Metal Restore 用にディザスタリカバリ情報を収集する (Collect disaster recovery information for Bare Metal Restore)]属性が設定されている必要があります。

---

**メモ:** [BMR 用にディザスタリカバリ情報を収集する (Collect disaster recovery information for BMR)]属性を有効にすると、自動的に[True Image Restore 情報を収集する (Collect true image restore information)]の[移動検出を行う (with move detection)]属性が設定されます。

---

これらの属性によって、バックアップ時にシステムに存在していたファイルのみを **NetBackup** でリストアできます。移動検出によって、移動、名前の変更、または新規インストールが行われたファイルを **NetBackup** で正しくリストアできます。また、これらの属性によって、リカバリ時に、BMR によって作成されたボリュームおよびファイルシステムに、リストアされたすべてのファイルが確実に格納されます。

---

**メモ:** ユーザー主導バックアップでは、True Image Restore 情報が収集されないため、BMR による保護が行われません。

---

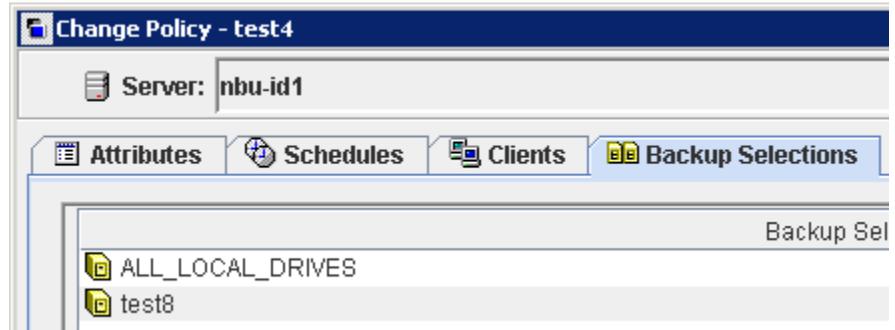
---

**メモ:** BMR バックアップを有効にする同様のオプションは、NetBackup Web UI の [ポリシー管理 (Policy management)] タブでも利用可能です。

---

- システム全体のリカバリを確実に実行するには、`ALL_LOCAL_DRIVES` 指示句を使用して、すべてのローカルドライブをバックアップします。この指示句はクライアント上のすべてのファイルをバックアップし、Windows クライアントの場合は、システムオブジェクト (`SYSTEM_STATE`) をバックアップします。

NetBackup データベースエージェントまたはその他のポリシーを使ってバックアップを行うデータベースまたはアプリケーションのファイルがクライアントに含まれている場合は、エクスクードリストを使って、`ALL_LOCAL_DRIVES` を指定したポリシーからそれらを除外します。ファイルが BMR ポリシーで除外される場合、後の BMR リカバリでは、除外済みのファイルを明示的に回復する必要があります。



---

メモ: `All_Local_Drives` が選択されない場合でも、Windows システム状態の場合には最低限の OS ボリュームが必要となります。

---

- クラスタ構成のクライアントの場合、最も効果的なバックアップ戦略は、複数のポリシーを使用することです。各ノードで、ローカルファイルシステムをバックアップする個別のポリシーを使用する必要があります。共有ファイルシステムは、現在リソースを所有するノードをバックアップする追加のポリシーによってバックアップする必要があります。
- 異なるバックアップ対象で同じクライアントに対して複数のポリシーが構成されている場合には、すべてのポリシーを同時に実行するようにスケジュールすると、一貫した後のリカバリを実現できます。
- NetBackup メディアサーバーを BMR クライアントとして保護できます。自身のストレージデバイス (SCSI 接続または SAN 接続) にバックアップするメディアサーバーの場合、特殊な手順でリストアする必要があります。この手順を使用することで、リストアに必要な時間と労力が最小限に抑えられるように、NetBackup を構成することができます。  
p.133 の「NetBackup メディアサーバーのリストアについて」を参照してください。

バックアップポリシーの構成について詳しくは、『NetBackup 管理者ガイド』を参照してください。

## 複数のポリシーでの同じクライアント名の使用

クライアントのバックアップに複数のポリシーを使用する場合は、各ポリシーで、同じクライアント名を正確に使用します。

BMRは、システムファイルをバックアップするポリシーで名前が指定されたクライアントのみをリストアすることができます。複数のポリシーを使用し、各ポリシーで異なる名前を使用すると、クライアント名ごとにクライアントレコードおよびそれに関連付けられた構成が作成されます。システムファイルをバックアップしないポリシーに指定された名前ですべてのクライアントをリストアすると、リストア準備処理が失敗します。失敗の原因は、BMRは、システムファイルをバックアップするポリシーで名前が指定されたクライアント名のみをリストアが可能なためです。

したがって、同じ名前を使用すると、リストア時に複数のクライアント名の中から選択する必要があります。

## 完全バックアップの実行について

クライアント上にあるすべてのファイルをリストアするには、すべてのファイルをバックアップする必要があります。バックアップ時に特定のファイルを除外していた場合、それらのファイルはバックアップされないため、リストアもされません。

## リストア後の完全バックアップの実行について

クライアントをリストアした直後および増分バックアップを実行する直前に、クライアントの完全バックアップを実行する必要があります。増分バックアップの後、完全バックアップの前にクライアントが再度失敗した場合、BMRは最後の増分バックアップにクライアントをリストアできないことがあります。

特定のクライアントを手動でバックアップできます。この場合、ポリシーを[有効 (Active)]に設定する必要があります。[開始日時の設定 (Go into effect at)]属性には、将来の日時を設定しないでください。

## 正常なバックアップの保障

バックアップが不完全になる危険性が最小になる時間帯にバックアップをするようにスケジューリングしてください。バックアップ時にクライアントを *inactive* 状態にできない場合は、次の操作を実行します。

表 3-1 バックアップを正常に完了するための手順

手順	処理	参照先
手順 1	UNIX クライアントの場合は、バックアップ試行中にファイルが変更された場合に、ファイルのバックアップを再試行するように NetBackup を構成します。ビジー状態のファイルのプロパティに関する詳細情報が利用可能です。	『NetBackup 管理者ガイド Vol. 1』を参照してください。
手順 2	Windows クライアントの場合は、Windows Open File Backup オプションを使用するように NetBackup を構成します。Windows Open File Backup のプロパティに関する詳細情報が利用可能です。	『NetBackup 管理者ガイド Vol. 1』を参照してください。
手順 3	バックアップ時のエラーに迅速な対応ができるように、NetBackup のログファイルは必ず確認してください。バックアップ時に、ネットワークまたはサーバーでバックアップに影響を及ぼすエラーが発生する可能性があります。	

## UNIX または Linux でのカスタムファイルの保存

次の情報は UNIX と Linux クライアントにのみ適用されます。

通常、クライアントのファイルは、NetBackup によって、リストア処理の最後の段階で、リストアされます。クライアント上のカスタムファイルを指定して、リストア処理中にクライアント上の一時的なオペレーティングシステム環境で使用できます。

たとえば、一時オペレーティングシステムでは、保護対象のクライアントからの特定のデバイスドライバ構成が必要になります。それらのデバイスドライバファイルをリストア環境に含まれるように指定できます。

カスタムファイルは、クライアントの構成の一部として保存されます。クライアント上にある次のテキストファイルの中でカスタムファイルを指定します。

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

1 行につき 1 つのカスタムファイルをフルパス名で指定します。行の先頭に、シャープ記号 (#) を入れるとコメント行になります。

カスタムファイルが保存された後 (クライアントをバックアップしたとき) に、SRT にコピーされます。SRT の排他的な使用を有効にすると、リストア時にも使用できます。SRT を有効にする方法に関する詳細情報が利用可能です。

p.75 の「[SRT の排他的な使用を有効にまたは無効にする方法](#)」を参照してください。

カスタムファイルを指定すると、バックアップから除外されません。また、カスタムファイルも NetBackup でバックアップされ、NetBackup がクライアントのファイルをリストアする際にリストアされます。(ファイルまたはファイルのディレクトリがポリシーのバックアップ指示句に含まれる場合、バックアップとリストアが行われます。)

## クライアントバックアップの監視

NetBackup アクティビティモニターを使用してバックアップジョブを監視できます。バックアップジョブの詳細には、保護対象のクライアントの構成を保存するエージェントに関する情報が含まれます。

p.245 の「[バックアップジョブの監視](#)」を参照してください。

## BMR 関連の他の NetBackup プロパティ

以下のプロパティはデフォルトで設定されますが、構成または調整が必要になることがあります。

- [クライアントによるリストアを許可する (Allow client restore)] プロパティ。BMR のリストア処理では、BMR マスターサーバーおよび BMR クライアントの両方でリストアを要求できる必要があります。クライアントによるリストアは、NetBackup のデフォルトの動作で許可されています。[クライアントによるリストアを許可する (Allow client restore)] プロパティは、NetBackup マスターサーバープロパティの[クライアント属性 (Client Attributes)] タブにあります。
- サーバー主導リストア。サーバー主導リストアを使うように NetBackup クライアントを構成します。これによって、マスターサーバーがサーバー主導リストアにクライアントファイルのリストアをリダイレクトできます。サーバー主導リストアは、NetBackup のデフォルトの動作です。サーバー主導リストアが許可されていることを確認してください。詳しくは、『[NetBackup 管理者ガイド Vol. 1](#)』を参照してください。
- [True Image Restore (TIR) 情報を保持する (Keep true image restoration (TIR) information)] プロパティ。このプロパティは、TIR 情報が NetBackup カタログに保持される期間を制御します。TIR 情報によって、カタログサイズおよび使用されるディスク領域が増加します。

必要に応じて次の設定をします。

- この属性の値をポリシーの保持期間と一致するように選択します。
- 反対に、NetBackup カタログのサイズを最小限に抑える場合は、属性を 0 日に設定します。TIR 情報もバックアップメディアに保存されるため、カタログサイズは増加しませんが、リストアが低速になります。

NetBackup マスターサーバープロパティの[クリーンアップ (Clean-up)]タブで、[True Image Restore (TIR) 情報を保持する (Keep true image restoration (TIR) information)]プロパティを設定します。

NetBackup を構成する方法については、『NetBackup 管理者ガイド Vol. 1』を参照してください。

## 特定のユースケースでのクライアントの保護

### Storage Foundation for Windows Clients

BMR はレガシーリストアメソッドだけではなく、高速リストア (非 SFW ボリュームリカバリ) メソッドの両方を使用して、Storage Foundation for Windows (SFW) Clients をリストアできます。ただし、現在 FAST リストアメソッドは SFW Volume Manager により管理されていない非 SFW ディスクのみをリストアすることのみをサポートできます。レガシーリストアメソッドを使用してリストアするために必要なバックアップ構成は、高速リストアメソッドに対して使用されるものとは異なります。

高速リストアを使用する BMR

BMR を使用してバックアップし、高速リストアメソッドを使用してリストアするとき (SFW)、バックアップを試みる前にいくつかの追加ステップを実行する必要があります。

---

**メモ:** SFW ではなく、Windows ディスクマネージャの下にシステムディスクを維持することをお勧めします。このようにして、BMR ファストリカバリメソッドを使用してシステムをリカバリし、後で、SFW ボリュームに戻すことができます。

---

高速リストアを使用して BMR を実行するには、

- 1 DWORD - レジストリキー「BMR\_USE\_WINDOWS\_VOL\_MGR」を HKLM¥SOFTWARE¥Veritas¥NetBackup¥BareMetal の下で構成し、保護される SFW クライアントで値を「1」にセットします。これは重要なステップで、結果としてキーが正しく設定されていることを検証します。
- 2 SFW クライアントの BMR バックアップを実行します。
- 3 システムディスクを除くすべてのディスクが、「現在」の構成で BMR により「制限付き」としてマークされています。SFW ディスクが「制限付き」としてマークされていない場合、レジストリキーの設定に問題が生じる場合があります。BMR は制限付きとしてマークされているディスクをリストアせず、そのまま維持します。

---

**メモ:** BMR は制限付きとしてマークされているディスクをリストアせず、これらのディスクをそのまま維持します。

---

# リストア環境の設定

この章では以下の項目について説明しています。

- [リカバリ手順](#)
- [ブートサーバーソフトウェアのインストール](#)
- [共有リソースツリー](#)
- [クライアント固有のリソースの追加](#)
- [ブートメディアの使用](#)
- [クライアントのリストア準備](#)

## リカバリ手順

保護対象のクライアントをリストアするには、リストア処理中に使用するリストア環境を設定する必要があります。

環境はいつでも設定できます。ただし、リカバリ時間目標 (RTO: Recovery Time Objective) が短い場合は、すべてのリソースを準備しておくこともできます。設定よりもリカバリに時間が使用されます。

表 4-1 リストア環境を設定するプロセス

手順	処理	関連項目
手順 1	ブートサーバーソフトウェアのインストール	p.31 の「 <a href="#">ブートサーバーソフトウェアのインストール</a> 」を参照してください。
手順 2	共有リソースツリーの作成	p.31 の「 <a href="#">共有リソースツリー</a> 」を参照してください。

手順	処理	関連項目
手順 3	クライアントリソースの追加	p.32 の「 <a href="#">クライアント固有のリソースの追加</a> 」を参照してください。
手順 4	ブートメディアの作成	p.32 の「 <a href="#">ブートメディアの使用</a> 」を参照してください。
手順 5	クライアントのリストア準備	p.33 の「 <a href="#">クライアントのリストア準備</a> 」を参照してください。

## ブートサーバーソフトウェアのインストール

ブートサーバーは、共有リソースツリー (SRT) などのリソースを含む、保護対象のクライアントの再構築に必要な環境を提供します。ブートサーバーは、保護するクライアントの種類ごとに用意する必要があります。また、SRT を作成して、それらにリソースを追加する前に、BMR ブートサーバーソフトウェアをインストールしておく必要があります。詳しくは、「BMR の構成」の章を参照してください。

BMR マスターサーバーへのブートサーバーとして登録されていない NetBackup クライアント、または BMR マスターサーバーとの通信ができないブートサーバーは [マスターなしブートサーバー (master-less boot server)] と見なされます。すべての SRT 関連操作のうち、SRT の作成、SRT のエクスポート、SRT の削除操作のみがマスターなしブートサーバーの場合に可能です。BMR SRT 操作には Microsoft 社の ADK が利用可能である必要があるためです。ユーザーはマスターなしブートサーバーに ADK をインストールし、SRT を作成してエクスポートできます。この SRT は登録されているその他のブートサーバーでインポート可能なため、これらのブートサーバーでの ADK インストールは不要になります。

## 共有リソースツリー

共有リソースツリー (SRT) は次の集合である、システムリカバリにとって重要なソフトウェアです。

- オペレーティングシステムファイル
- NetBackup クライアントソフトウェア
- 任意で、デバイスドライバ、Volume Manager、ファイルシステム管理ソフトウェアなど、元のシステムを再構築するために必要なその他のソフトウェア

SRT の概要および SRT の作成手順と管理手順に関する詳細情報が利用可能です。「共有リソースツリーの管理」の章を参照してください。

## クライアント固有のリソースの追加

Dissimilar System Restore では、保護対象のクライアントの保存される構成に含まれないリソースがいくつか必要になる場合があります。その場合は、リストアに使用する SRT またはクライアント構成 (リストア構成) にそのリソースを追加する必要があります。

そのようなリソースの例を次に示します。

- ネットワークインターフェースカード (NIC) ドライバ
- 大容量記憶装置デバイス (MSD) ドライバ

Windows の場合には、必要なデバイスドライバのリストアを BMR のパッケージのプールにリストアに追加できます。このため、リストア構成に追加して利用可能です。

パッケージプールにパッケージを追加する方法とソフトウェアを Windows SRT に追加する方法に関する詳細情報が利用可能です。これについて詳しくは「Windows ドライバパッケージの管理 (Managing Windows drivers packages)」の章を参照してください。

p.71 の「Windows SRT へのソフトウェアの追加」を参照してください。

UNIX システムの場合には、BMR-SRT 管理ユーティリティを使用して必須ソフトウェアまたはデバイスドライバを追加できます。

p.67 の「UNIX または Linux SRT へのソフトウェアの追加」を参照してください。

p.157 の「クライアントと構成について」を参照してください。

## ブートメディアの使用

BMR のリストア処理は、BMR によって準備されたブートメディア (CD、DVD またはフロッピー) または (ネットワークブートを使用した) BMR ブートサーバーからのクライアントのブートによって開始されます。ネットワークブートを使用してリストアを開始する場合、ブートメディアは必要ありません。

最小のネットワーク接続があったり、ネットワークベースのリカバリに必要なサービスを展開しないという制限がある場合 (すなわち DHCP または TFTP) には、共有リソースツリーを含むブートメディアを使うことを Cohesity は推奨します。

---

**メモ:** BMR メディア SRT が作成された時点で、BMR ブートサーバーはリカバリの間に必要となりません。

---

ブートメディアの概要およびブートメディアの作成手順に関する詳細情報が利用可能です。詳しくは、「ブートのメディアの管理」の章を参照してください。

p.77 の「ブートメディアの管理」を参照してください。

## クライアントのリストア準備

クライアントリカバリに最適な SRT が準備できると、NetBackup プライマリサーバーから「リストア準備」手順がトリガされます。この手順では、リカバリの対象となるクライアント構成のダイジェスト、リソースの検証、およびそのクライアントリストアのリカバリ環境を調整します。

この主題について詳しくは、「クライアントのリストア」を参照してください。

# 共有リソースツリー

この章では以下の項目について説明しています。

- [共有リソースツリーについて](#)
- [共有リソースツリーの前提条件](#)
- [共有リソースツリーの作成](#)
- [共有リソースツリーの管理](#)
- [ブートメディアの管理](#)

## 共有リソースツリーについて

共有リソースツリー (SRT) は次の集合である、BMR システムリカバリにとって重要なソフトウェアです。

- オペレーティングシステムファイル
- NetBackup クライアントソフトウェア
- NetBackup クライアントソフトウェアを使用して、ドライブのフォーマット、パーティションの作成、ファイルシステムの再構築、元のファイルのリストアを行うプログラム

また、SRT では、クライアントシステムのブートおよびリストア処理の開始に必要なリソースも提供されます。

SRT 内のソフトウェアは、保護対象のシステムに永久にインストールされません。保護対象のシステムをリストア可能な元のファイルの状態に戻す場合にのみ使用されます。

次の点に注意してください。

- UNIX システムと Linux システムの場合: クライアントの種類とオペレーティングシステムのバージョンごとに、個別の SRT が必要です。たとえば、Solaris 11 には Solaris 11 SRT が必要であり、AIX 7.1 TL3 には AIX 7.1 TL3 SRT が必要です。

- **Windows** システムの場合: 1 つの **SRT** で、同じアーキテクチャの **Windows** のすべてのバージョンをリストアできます。

**UNIX** および **Linux** システムの場合、同じオペレーティングシステムのブートサーバー上に複数の **SRT** を作成できます。そのブートサーバーで稼動するオペレーティングシステムのバージョンは、**SRT** にインストールされているオペレーティングシステムのバージョン以上である必要があります。たとえば、**Solaris 11 SRT** は **Solaris 11** 以上のブートサーバーに存在する必要があります。**Windows** システム場合、任意のバージョンの **Windows** で **SRT** をホスティングすることができます。

クライアント、**SRT**、ブートサーバーに対してサポートされるオペレーティングシステムについて詳しくは、『**NetBackup** リリースノート』を参照してください。

リストア中に、クライアントはネットワークを経由してブートサーバーから **SRT** にアクセスするか、あるいは **CD** または **DVD** 上の **SRT** にアクセスします。**SRT** がブートサーバー上に存在する場合でも、**SRT** を **CD** メディアまたは **DVD** メディアにコピーし、クライアントをそのメディアからブートすれば、メディア上の **SRT** にアクセスすることができます。**BMR** メディアを使用している場合、リカバリの間にブートサーバーを必要としません。

**SRT** を作成したオペレーティングシステムに応じて、**SRT** サイズ要件は **100 MB** から **1 GB** のディスク領域の範囲で異なります。

ディスク領域要件について詳しくは、『**NetBackup** リリースノート』を参照してください。

## 共有リソースツリーの前提条件

以降のセクションで、共有リソースツリーの前提条件について詳しく説明します。

## 共有リソースツリーの作成

共有リソースツリー (**SRT**) は、ブートサーバーのローカルファイルシステム上に作成する必要があります。**SRT** ディレクトリの権限は、すべてのユーザーに読み込み権限を許可し、**root** ユーザーまたは管理者ユーザーに読み込みおよび書き込み権限を許可するように設定されます。

**SRT** の作成時に、オペレーティングシステムソフトウェアおよび **NetBackup** クライアントソフトウェアを **SRT** にインストールします。また、**SRT** の作成時、または作成後いつでも、他のソフトウェアもインストールできます。

---

**メモ:** **BMR** ブートサーバーでレガシーの **SRT** は作成できません。

---

**SRT** を作成するには、次の項目に対するインストールソフトウェアまたはイメージが必要です。

- オペレーティングシステム (**UNIX** および **Linux** のみ)。

- **Linux SRT** の場合は、**Bare Metal Restore** のサードパーティ製品 CD。この CD には、ベンダーの **Linux** ディストリビューションに含まれない可能性のあるオープンソース製品が含まれています。

---

**メモ:** **Cohesity** は、**3PPCD** のサードパーティのコンポーネントをそれぞれの最新リリースにときどき更新します。新しい **SRT** の作成時に、最新の利用可能なバージョンの **3PPCD** を使用することを常にお勧めします。**NetBackup** バージョン **8.3** 以降のブートサーバーには、バージョン **3.0** の **BMR 3PPCD** が必要です。**8.3** より前のバージョンの **NetBackup** では、**3PPCD** のバージョン **2.0** を使用することをお勧めします。それよりも新しいバージョン **3.0** の **3PPCD** の使用は許可されていません。同様に、**8.0** より前のバージョンの **NetBackup** のブートサーバーでは、**3PPCD** のバージョン **1.0** のみを使用できます。また、ユーザーは以前のバージョンの **3PPCD** で作成された既存の **SRT** を引き続き使用できます。初めて **SRT** を作成するとき、ユーザーが **3PPCD** を指定すると、**BMR** は **3PPCD** のコンテンツを `/usr/opensv/netbackup/baremetal/server/data/media/3PPCD/` に保持します。それ以降の **SRT** の作成では、この場所にあるコンテンツを使用します。何らかの理由によりこの場所が空の場合、`bmrstadm` は **SRT** の作成中に **3PPCD** を要求します。古いブートサーバーを **8.3** にアップグレードした後、**SRT** の作成中に、**BMR** は **SRT** が作成された **OS** のバージョンを確認し、この場所のコンテンツを検証し、領域をクリーニングして、**3PPCD** のバージョン **3.0** を要求します。

[https://www.veritas.com/content/support/ja\\_JP/downloads/update.UPD238422](https://www.veritas.com/content/support/ja_JP/downloads/update.UPD238422)

---

- 必要に応じて、他のアプリケーションまたはパッケージ (**Arctera Volume Manager** または **Arctera File System** など)。
- 必要に応じて、**SRT** にインストールされているオペレーティングシステムまたはその他のソフトウェアで必要な、パッチ、メンテナンスレベル、**Maintenance Pack**、**Service Pack**、ファイルセット、またはドライバ。**NetBackup** クライアントソフトウェアに必要なオペレーティングシステムパッチを **SRT** にインストールする必要があります。このオペレーティングシステムパッチがインストールされていない場合、**NetBackup** は一時的なリストア環境で正しく機能せず、リストアが失敗する場合があります。パッケージまたはパッチの依存関係について詳しくは、『**NetBackup** リリースノート **UNIX**、**Windows** および **Linux**』を参照してください。

同じオペレーティングシステムの **SRT** が複数必要である場合は、オペレーティングシステムと **NetBackup** クライアントソフトウェアだけを含む **SRT** を作成します(たとえば、異なるバージョンの **Arctera Volume Manager** や異なるドライバを含むクライアントをリストアする場合などです)。次に、必要な数だけコピーを作成し、そのコピーに異なるバージョンの他のソフトウェアを追加します。通常、既存の **SRT** をコピーした方が **SRT** を作成するよりも効率的です。

**SRT** の作成中、次のいずれかの操作を行う場合に、インストールプログラムまたはソフトウェアへのパスを入力するプロンプトが表示されます。

- インストールプログラムをブートサーバーのリムーバブルメディアドライブに配置する。この場合は、そのリムーバブルメディアドライブへのパスを入力します。
- インストールプログラムの内容をローカルディレクトリにコピーする。この場合は、そのローカルディレクトリへのパスを入力します。
- インストールプログラムの内容を、NFS などのネットワーク共有を経由してブートサーバーから使用できるリモートディレクトリにコピーする。この場合は、そのリモートディレクトリまたは共有の場所へのパスを入力します。

SRT の作成には、5 分から 60 分程度の時間がかかります。この時間は、システムの速度、作成する SRT のオペレーティングシステムおよびインストールする他のソフトウェアによって異なります。

p.52 の「[UNIX または Linux の SRT の作成](#)」を参照してください。

p.37 の「[Windows の SRT の作成](#)」を参照してください。

## Windows の SRT の作成

BMR Windows リカバリは迅速なリストア方法によってサポートされています。これにより Windows SRT でユーザーは Windows のバージョンを入力する必要はありません。SRT ではブートサーバー上にプリインストールされている Windows の物理環境が使用されます。物理環境を作成するため、Microsoft ADK をブートサーバーにインストールする必要があります。SRT を作成する手順については、p.38 の「[SRT の作成](#)」を参照してください。を参照してください。

### 共有リソースツリー管理ウィザード

このウィザードは Windows システムにのみ適用されます。

共有リソースツリー管理ウィザードを使用して、次の処理を行うことができます。

- SRT の作成
- SRT の編集
- SRT のエクスポート
- SRT のインポート
- SRT のコピー
- SRT の削除
- ブート CD/DVD イメージの作成
- SRT へのパッケージの追加または更新
  - SRT への NetBackup クライアントソフトウェアの追加
  - SRT への NetBackup Release Update または Maintenance Pack の追加

- NetBackup 言語パックの追加

## SRT の作成

BMR SRT には、クライアントシステムのブートおよびリストア処理の開始に必要なリソースがあります。BMR Windows SRT は、ベースリカバリ環境として Windows プリインストール環境 (WinPE) を使用します。このベース WinPE リカバリ環境を作成するには、Microsoft ADK (Assessment and Deployment Kit) バージョン 10 をホストにインストールする必要があります。Microsoft ADK のインストールは、新しい SRT を初めて作成する場合に不可欠です。BMR ブートサーバーホストに ADK をセットアップするには、次に示す複数のオプションがあります。

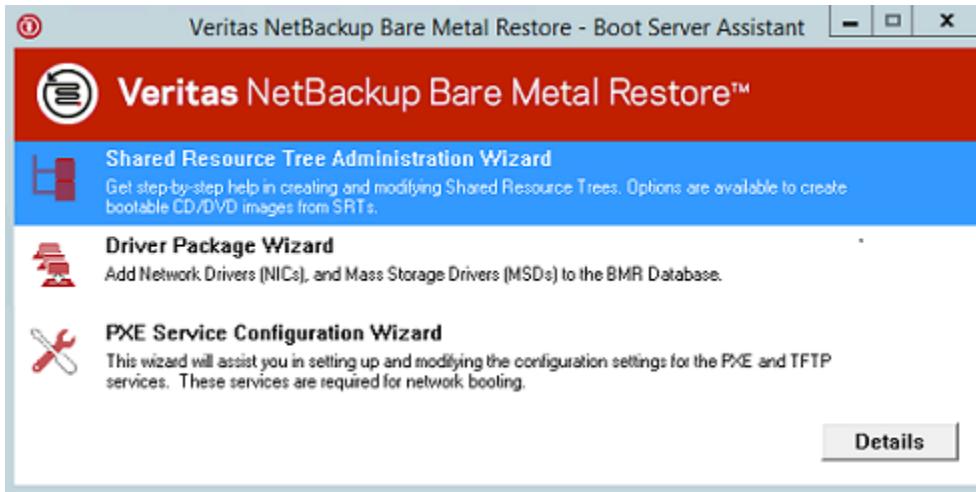
- BMR 共有リソースツリー管理ウィザードは、以下を使用してインストールできます。
  - ADK の自動ダウンロードとインストール
  - SRT を作成するためにリモートでダウンロードした ADK インストーラを使用する
- FULL ADK 10 によってインストールできる ADK 10 による ADK の手動セットアップはダウンロード可能で (ADKsetup.exe)、Microsoft の Web サイト (<https://go.microsoft.com/fwlink/p/?LinkId=526740>) から直接インストールできます。または Microsoft の Web サイトから ADK インストーラパッケージ全体をダウンロードしてオフラインでインストールすることもできます。

ADK セットアッププログラムのサイズは約 3 GB です。

## Windows の SRT を作成する方法

- 1 SRT をホスティングする Windows BMR ブートサーバーの [スタート] メニューから、[プログラム]、[Cohesity NetBackup]、[Bare Metal Restore ブートサーバーアシスタント (Bare Metal Restore Boot Server Assistant)] の順に選択します。

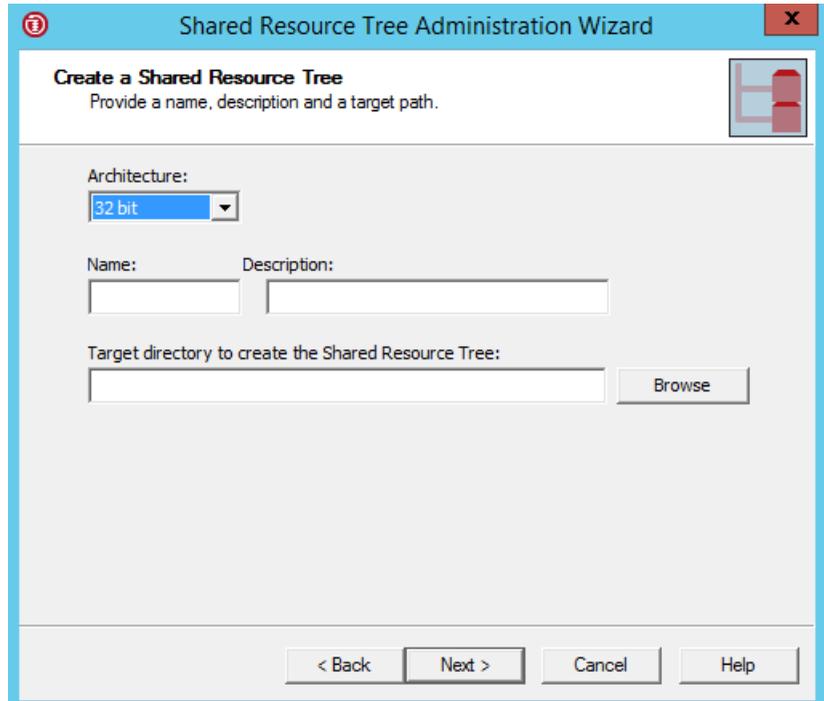
Bare Metal Restore ブートサーバーアシスタントが表示されます。



- 2 [共有リソースツリー管理ウィザード (Shared Resource Tree Administration Wizard)] をクリックします。

共有リソースツリー管理ウィザードが表示されます。

- 3 共有リソースツリーの形式を **Fast Restore SRT** として選択します。
- 4 プロンプトに従って、共有リソースツリーを作成します。次の情報を入力する必要があります。



アーキテクチャ (Architecture)	ドロップダウンのオプションからアーキテクチャを選択します。
名前 (Name)	SRT の名前は、その SRT が存在するディレクトリにも使用されます。英数字とアンダースコア ( _ ) のみを使用できます。
説明 (Description)	SRT の説明を入力します。
ターゲットディレクトリ	パスを入力するか、SRT のターゲットの場所を参照します。

### Microsoft のアセスメント & デプロイメントキット(ADK) のインストール

NetBackup Bare Metal Restore を使って、NetBackup で保護されているクライアントをリカバリするには、カスタマイズされた Windows プリインストール環境 (WinPE) が必要です。SRT 作成用にカスタマイズされた物理環境を構築するには、Microsoft ADK のインストールが不可欠です。

Microsoft ADK をインストールする場合は、次の 2 つのオプションを使用できます。

- ADK のダウンロードおよびインストールを自動実行する
- リモートサイトにすでにダウンロードされている ADK を使って現在のホストにインストールする

#### 自動ダウンロードおよびインストールオプションを使った ADK のインストール

このオプションは Microsoft の Web サイトから Microsoft ADK を自動的にダウンロードして、インストールします。

次の手順を実行します。

- 1 [ダウンロードとインストールの自動実行 (Automatically Download and Install)] オプションを選択して、[次へ (Next)] をクリックします。

これにより、ADK のダウンロードおよびインストールが自動的に開始されます。ウィザードでプロセスの進捗状況を観察できます。

- 2 インストール用パスを指定して、[次へ (Next)] をクリックします。
- 3 カスタマエクスペリエンス向上プログラム (CEIP) は任意です。応答を入力して、[次へ (Next)] をクリックします。
- 4 使用許諾契約に同意して、続行します。
- 5 配備ツールおよび Windows プレインストール環境で BMR の基本リカバリ環境を構築する場合は、事前に選択された機能の選択を解除しないでください。これらの機能は不可欠です。[インストール (Install)] をクリックします。

Windows ADK のインストールが完了したことは、進捗状況バーで確認できます。

- 6 [閉じる (Close)] をクリックします。
- 7 共有リソースツリー管理ウィザードの進行バーで、引き続き回復ディスクイメージをカスタマイズします。

#### ADK のダウンロードおよびインストールプロセスの進捗状況

ADK を自動的にダウンロードおよびインストールするオプションを選択すると、BMR はインストールプロセスの事前チェックを実行して開始します。これは、SRT 作成用の物理環境を開発するために構成前のコンプライアンスを確認する際に必要となります。

ADK の自動ダウンロードおよびインストールを開始したら、進捗状況の詳細、およびウィザードで実行されている構成前チェックを観察できます。各ステージは次のとおりです。

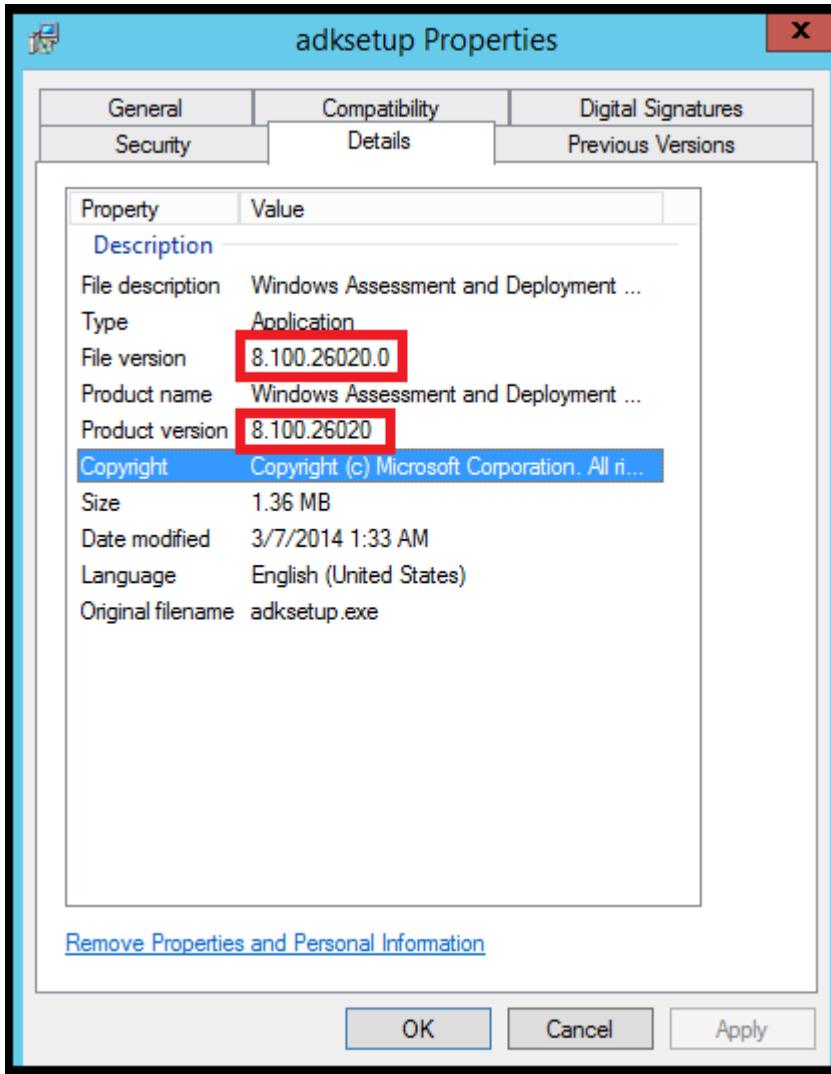
- ADK のダウンロードとインストール
- NetBackup BMR Windows リカバリの環境の作成
- シマンテック回復ディスクイメージのカスタマイズ

すべての事前チェックが完了するまで待機してから、[次へ (Next)] をクリックします。

### 事前にダウンロードされた ADK 実行可能ファイルの使用

事前にダウンロードされた ADK 実行可能ファイルを使うには、インターネット接続を通してホストにダウンロードする必要があります。ADK の詳しいダウンロード手順については、[Technote21353](#) を参照してください。

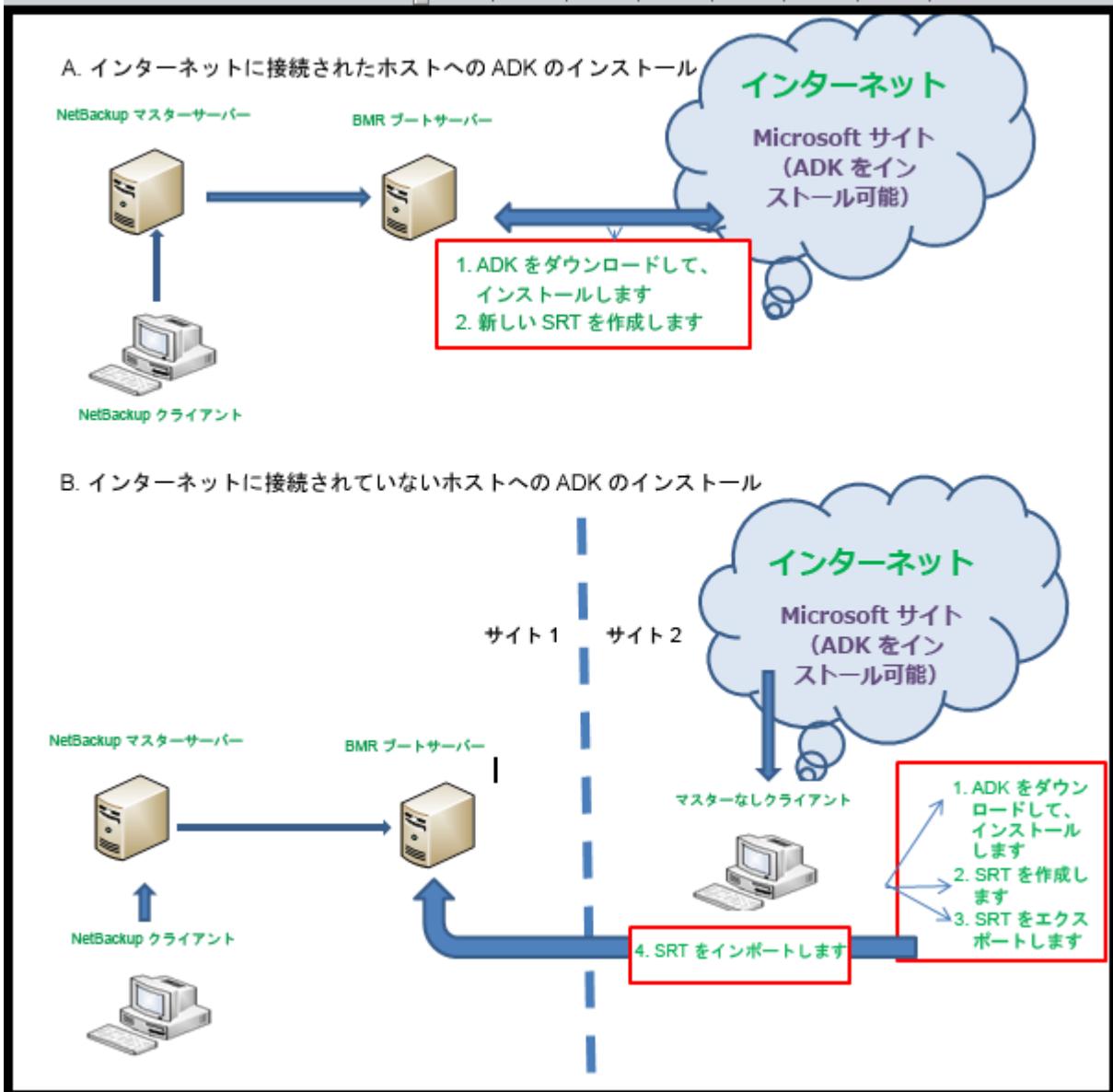
ADKsetup.exe をダウンロードします。このファイルは、<http://www.microsoft.com> から Windows ADK をインストールする場合に必要となります。Windows ADK のセットアッププログラムは、グラフィカルユーザーインターフェース (GUI) またはコマンドラインを使って、インターネットから直接ダウンロードされます。ADK セットアップの実行中は、BMR ブートサーバーをインターネットに接続したままにしてください。ADK セットアップにより、インターネットからインストールパッケージがダウンロードされます。ADK セットアップが完了するまでの所要時間は、インターネット接続の帯域幅、コンピュータのパフォーマンス、およびインストールするよう選択した Windows ADK 機能によって変わります。



### オフラインのブートサーバーまたはホストでの SRT の作成

BMR マスターサーバーにブートサーバーとして登録されていない NetBackup クライアント、または BMR マスターサーバーと通信できないブートサーバーは、マスターレスサーバー、またはオフラインブートサーバーとみなされます。BMR SRT 操作を行うには Microsoft の ADK が利用可能でなければならないため、マスターレスブートサーバーで実行できるのは SRT の作成、エクスポート、および削除操作のみです。ホストまたはブートサーバーからインターネットに接続できない場合は、一時的なブートサーバーに ADK をインストールして新しい SRT を作成し、それをホストにエクスポートすることができます。

一時的なブートサーバーは、マスターレスであってもかまいません。この SRT を登録された他のブートサーバーにインポートすると、これらのブートサーバーがインターネットに接続されていない場合に、ADK をインストールする必要がなくなります。SRT の自動インポートに関するセクションを参照してください。



## SRT 自動インポート

この操作は、ブートサーバーとして BMR マスターサーバーに登録されていなかったクライアント、またはマスターサーバーに接続されていないブートサーバーに作成された共有リソースツリーの自動インポートを有効にします。ブートサーバーを登録するか、マスターサーバーに接続し直した後、ブートサーバーアシスタントウィザードで[共有リソースツリー管理 (Shared Resource Tree Administration)]オプションを選択すると、以前に作成したすべての SRT エントリが BMR マスターサーバーデータベースに自動的に挿入されます。これらの SRT はリカバリ操作に使用できます。

---

**メモ:** 重複した SRT (マスターサーバーのデータベースに名前がすでにあるマスターなしブートサーバーに作成された SRT) は自動インポートされません。

---

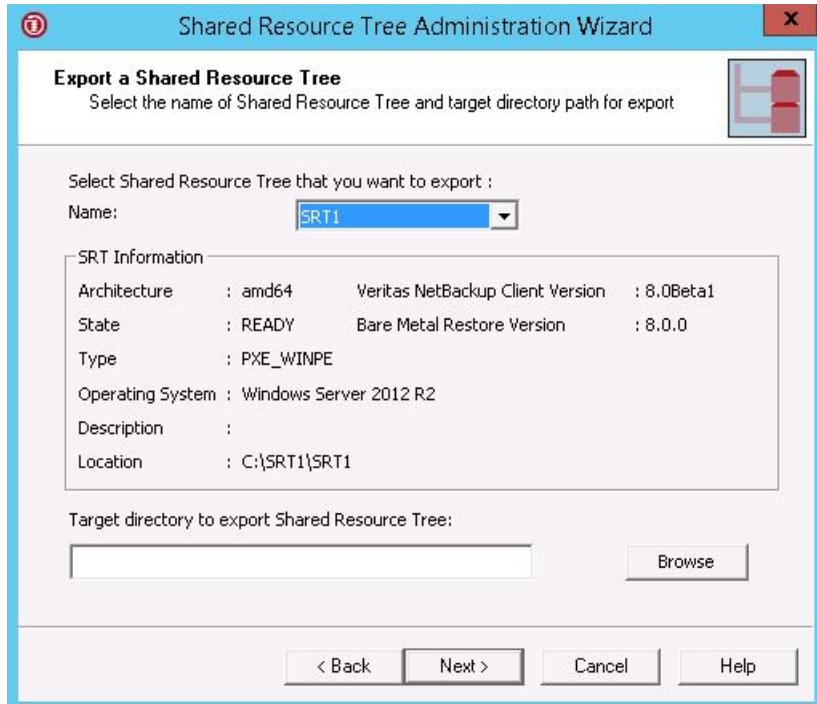
## SRT のエクスポート

このオプションを使うと、準備完了状態にある SRT をエクスポートできます。SRT をエクスポートすると、ADK 実行可能ファイル、SRD ファイル (x86 と amd64 の両方)、SRT wim ファイルを含む 1 GB のサイズの圧縮ファイルが作成されます。この圧縮ファイルは他のどのブートサーバーにもインポートできます。

---

**メモ:** SRT をエクスポートするには、C:¥ドライブに 1.4 GB 以上の追加領域が必要です。エクスポートプロセスが完了し、SRT がターゲット場所に正常にエクスポートされるまで、この追加領域が一時的なストレージとして機能するためです。

---



SRT をエクスポートするには次の手順を実行します。

- 1 エクスポートする SRT を選択します。
- 2 パスを入力するか、参照して、エクスポート済み SRT の新しい CAB を作成する場所を選択します。

---

**メモ:** CD/ISO ベースの SRT エクスポートはサポートされていません。ネットワーク上の場所へ SRT をエクスポートする前に、ネットワーク上の場所がすでに認証されていて、アクセス可能であることを確かめてください。

---

## SRT の編集

次のパネルで SRT パラメータを編集できます。

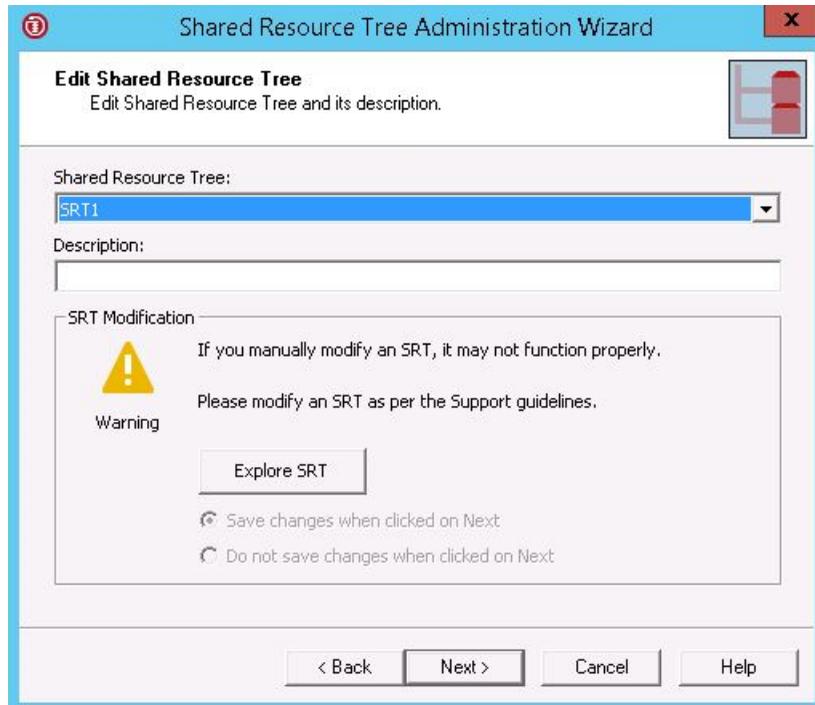
特定の場、SRT の内容を修正する必要があることもあります。たとえば、既存の BMR バージョンへ新しいリリース更新を適用する一部として SRT に新しいバイナリを追加します。このような場合、最初に SRT をマウントし、次に内容を修正する必要があります。

[SRT の探索 (Explore SRT)] オプションは自動的に選択された SRT をマウントして、新しいバイナリを追加したり、または存在するバイナリを修正したりできるファイルエクスプ

ローラービューに表示します。このオプションは、ユーザーが SRT 内でエンジニアリングバイナリを適用するときに特に有用です。

SRT を手動で変更する場合、正しく動作しないことがあります。この場合、Cohesity サポートがリリース更新内容で提供するガイドラインに従う必要があります。

図 5-1 共有リソースツリーの編集



パラメータを修正する SRT を選択します。

- SRT の説明を編集します。
- [SRT の探索 (Explore SRT)]をクリックして SRT の内容を修正します。

SRT を修正した後、次のどちらかをクリックします。

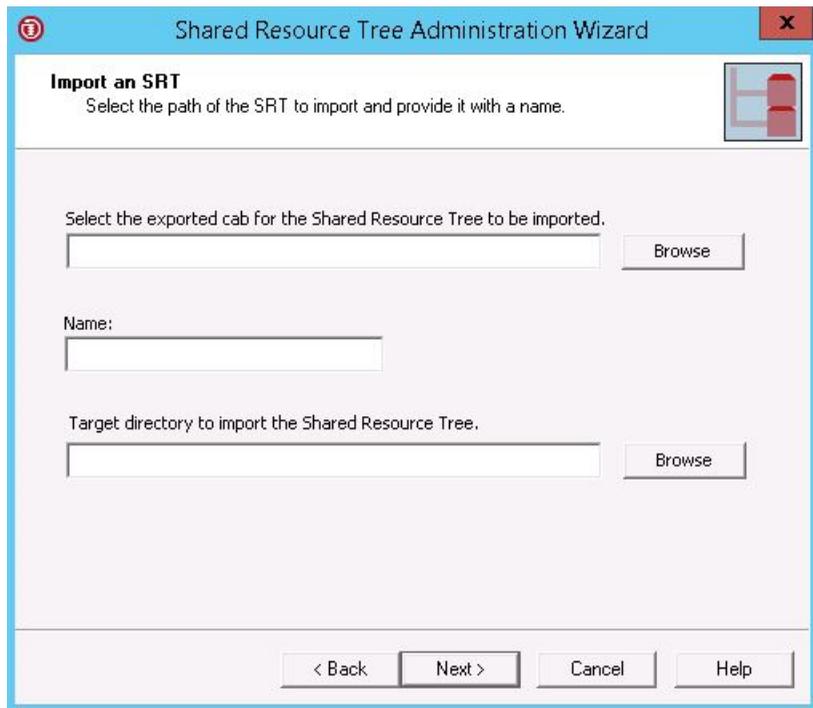
- [[次へ]をクリックするときに変更を保存する (Save changes when clicked on Next)]をクリックします。
- [[次へ]をクリックするときに変更を保存しない (Do not save changes when clicked on Next)]をクリックします。  
このオプションを選択し、[次へ (Next)]をクリックすると、SRT の説明または内容への修正は保存されません。

[次へ (Next)]をクリックして、SRT の修正手順を完了します。

## SRT のインポート

このオプションは圧縮された実行可能ファイルの形式の既存 SRT をインポートすることを可能にします。別のホストからインポートする SRT を最初にリモートホストからエクスポートする必要があります。特定の手順については、SRT のエクスポートの項を参照してください。SRT をエクスポートした後、SRT を新しい場所にインポートしている間に、次の操作がブートサーバーで実行されます。

- 指定パスでブートサーバーに CAB 内容を抽出します。
- Mini-ADK (OSCDIMG.exe) をコピーします
- SRD ファイル (x86 および amd64) をコピーします。
- 指定されたパスで SRT.wim ファイルをコピーします。
- マスタデータベースに SRT のエンTRIESを追加します。
- ローカルデータベースの SRT のエンTRIESを変更します。



The screenshot shows a Windows-style dialog box titled "Shared Resource Tree Administration Wizard" with a close button (X) in the top right corner. The main heading is "Import an SRT" and the instruction below it is "Select the path of the SRT to import and provide it with a name." There is a small icon of a red storage tank in the top right of the dialog area. The dialog contains three input fields, each with a "Browse" button to its right:

- The first field is for the "exported cab" path, with the instruction "Select the exported cab for the Shared Resource Tree to be imported." above it.
- The second field is for the "Name" of the SRT.
- The third field is for the "Target directory" to import the SRT, with the instruction "Target directory to import the Shared Resource Tree." above it.

At the bottom of the dialog, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

**SRT をインポートするには次の手順を実行します。**

- 1 インポートする既存の SRT が存在するブートサーバー上のディレクトリを選択します。
- 2 新しい SRT の名前を入力します。
- 3 パスを入力するか、参照して SRT をインポートする場所を選択します。

---

**メモ:** SRT をインポートできるようにするには、C:¥ドライブで最小 1.4 GB の追加領域が必要になります。この領域は、インポート処理が完了し、SRT がターゲットの場所に正常にインポートされるまで一時ストレージとして機能するためです。

---

### SRT のコピー

このオプションは 1 つのブートサーバーからの既存の SRT をコピーすることを可能にします。コピー操作は高速であるため、新しい SRT を再作成する際には常に推奨されません。

SRT をコピーするには、以下のステップを実行します。

- コピーする SRT を選択します。
- 新しい SRT の名前を入力します。SRT の名前には 9 文字以上の英数字を指定しないでください。
- 新しい SRT の説明を入力します。
- パスを入力するか、参照して新しい SRT を作成する場所を選択します。

### SRT の削除

削除する SRT を選択し、確認のダイアログボックスで[OK]をクリックします。

---

**メモ:** マウント済みの状態であったり編集のために開いている SRT は削除できません。

---

### Fast Restore SRT のブート可能 CD または DVD イメージの作成

Fast Restore SRT からのブート可能 CD/DVD イメージの作成では、次のステップが表示されます。

- 共有リソースツリーの選択  
p.50 の「**SRT の選択**」を参照してください。
- ISO の場所の指定とクライアントの確認  
p.50 の「**ISO イメージの場所の指定**」を参照してください。

この処理は、[コピー 9 (Copy Progress)]パネルと[共有リソースツリー管理ウィザードの完了 (Completing the Shared Resource Tree)]パネルで終了します。

## SRT の選択

リストアで使用するためにブート可能 CD/DVD イメージに変換する共有リソースツリーを選択します。

## ISO イメージの場所の指定

ISO イメージの場所を指定する必要があります。

ISO イメージを格納するディレクトリへのパスを入力するか、参照して選択します。ウィザードでは CD または DVD を作成しません。ウィザードが作成するのは、CD または DVD に書き込む必要があるイメージです。

このページに表示されているクライアントは、このイメージをブートするときに自動的にリストアされます。

## [共有リソースツリーの構成の完了]パネル

[完了 (Finish)]をクリックして、SRT 構成を終了します。

## SRT へのパッケージの追加または更新

共有リソースツリーに追加するリソースを選択します。

- SRT の NetBackup クライアントソフトウェアイメージを更新します。  
SRT には、保護対象のシステムと同じバージョンの NetBackup クライアントイメージが含まれている必要があります。
- SRT に Cohesity Security Services を追加します。

## SRT への NetBackup クライアントの追加

共有リソースツリーに NetBackup クライアントソフトウェアを追加する手順は次のとおりです。

- クライアントイメージを追加する共有リソースツリーを選択します。
- NetBackup クライアントインストールイメージ (NetBackup Client.msi) へのパス名を入力するか、参照してイメージを選択します。

SRT には、保護対象のシステムと同じバージョンの NetBackup クライアントイメージが含まれている必要があります。

すでに SRT に NetBackup クライアントイメージが含まれている場合、そのクライアントイメージは置き換えられます。

NetBackup クライアントを含まない SRT は、[ロック済み (Locked)]状態になります。[準備完了 (Ready)]状態は、NetBackup クライアントイメージがインストールされていることを示しています。

## SRT への NetBackup Security Services の追加

SRT に NetBackup Security Services を別途インストールする必要はありません。セキュリティサービスは、NetBackup クライアントの一部として SRT にインストールされます。古いバージョンの NetBackup クライアントを含む SRT の場合は、NetBackup Security Service を SRT に別途インストールする必要があります。NetBackup のアクセス管理を使って NetBackup 環境に対するアクセス権を管理する場合は、古いバージョンの NetBackup クライアント用に NetBackup Security Services (VxSS) ソフトウェアをインストールします。

アクセス管理のコンポーネントとアクセス管理の使用方法について詳しくは、『[NetBackup セキュリティおよび暗号化ガイド](#)』を参照してください。

SRT に NetBackup Security Service を追加するために、次のステップを実行する必要があります。

- NetBackup Security Service イメージを追加する共有リソースツリーを選択します。
- NetBackup Security Service のバージョンを選択します。
- セットアップファイル (.exe 形式) へのパスを入力するか、参照してイメージを選択します。

## SRT への NetBackup Release Update または Maintenance Pack の追加

NetBackup リリースの更新または Maintenance Pack を共有リソースツリーに追加する手順を、次に示します。

- 1 クライアントイメージを追加する共有リソースツリーを選択します。
- 2 NetBackup クライアントのインストールイメージ (Release Update.msi) のパス名を入力するか、イメージを参照して選択します。

SRT に、その特定バージョンに対応したベースとなる NetBackup クライアントのイメージが、関連するリリース更新か Maintenance Pack を適用する前に含まれている必要があります。

SRT にすでに NetBackup リリースの更新が含まれている場合は、現在のファイルが新しいファイルに置換されます。

## NetBackup 言語パックの追加

NetBackup 言語パックのソフトウェアを共有リソースツリーに追加する手順を次に示します。

- 1 クライアントイメージを追加する共有リソースツリーを選択します。
- 2 NetBackup クライアントのインストールイメージ (Language Pack.msi) のパス名を入力するか、イメージを参照して選択します。

すでに SRT に NetBackup 言語パックが含まれている場合、それは置き換えられます。

## UNIX または Linux の SRT の作成

UNIX または Linux OS クライアントの SRT を作成するには、`bmrstadm` コマンドラインを使用する必要があります。

各クライアント OS 固有の SRT の種類を作成する手順については、次を参照してください。

- p.52 の「[AIX SRT の作成](#)」を参照してください。
- p.55 の「[HP-UX SRT の作成](#)」を参照してください。
- p.58 の「[Solaris SRT の作成](#)」を参照してください。
- p.62 の「[Linux SRT の作成](#)」を参照してください。

### AIX SRT の作成

AIX SRT の作成時には、次のインストール処理の手順が示されます。

- オペレーティングシステムソフトウェア
- NetBackup クライアントソフトウェア。

#### AIX SRT を作成する方法

- 1 SRT を作成するブートサーバー上で、次のディレクトリに移動します。

```
/usr/opensv/netbackup/bin
```

- 2 次のコマンドを実行します。

```
./bmrstadm
```

- 3 プロンプトが表示されたら、新しい SRT を作成するためのオプションを選択します。

4 次の表に示すようにコマンドプロンプトを完了します。

Enter the name of the SRT to create	SRT の名前は、その SRT が存在するディレクトリにも使用されます。  英数字とアンダースコア ( <code>_</code> ) のみを使用できます。
Enter the description of the new SRT	SRT の説明。
Enter desired OS level of AIX	ブートサーバーのオペレーティングシステムのバージョンに基づいて、作成可能なレベルを入力します。
Enter desired Architecture (32/64)	64 ビット AIX オペレーティングシステムを入力します。  <b>メモ:</b> [SRT への NetBackup クライアントのインストール (NetBackup client installation into SRT)] 手順中、 <code>bmrstadm</code> は、SRT OS アーキテクチャ形式と NetBackup クライアントバージョンの間に互換性がない場合、該当するエラーメッセージを表示します。
Enter the directory in which to place the new SRT	SRT を作成するディレクトリへのパスを入力します。SRT 名を含む SRT の場所へのパス名が、SRT の root (SRT パスと呼ぶ) になります。  デフォルトは、 <code>/export/srt</code> か、SRT が最後に正常に作成されたディレクトリのいずれかになります。  このディレクトリはすでに存在している必要があります。
Source of AIX install images	オペレーティングシステムのインストールプログラムが挿入されているデバイス名を入力するか、インストールイメージへのパスを入力します。  デバイス名またはホスト:/パスを入力すると、オペレーティングシステムが SRT にインストールされます。

Enter the source of the  
NetBackup install images.

Specify a device name or an  
NFS path (host:/path form),  
or a local directory

**NetBackup** クライアントソフトウェアのインストールプログラムが挿入されているデバイス名を入力するか、インストールイメージへのパスを入力します。

デバイス名またはパスを入力すると、**NetBackup** クライアントのインストールプロセスによって、クライアントソフトウェアが **SRT** にインストールされます。

Do you want to continue? [y,n] 「y」を入力します。  
(y)

Do you want to install the 「y」を入力します。  
NetBackup client software for  
this client? [y,n] (y)

Enter the name of the  
NetBackup server:

空白以外の値を入力します。サーバー名は、リストア時に、リストア対象の **BMR** クライアントの正しい値に置き換えられます。

Would you like to use  
servername as the configured  
name of the NetBackup client?  
[y,n] (y)

デフォルトのまま使用するか、空白以外の値を入力します。クライアント名は、リストア時に、リストア対象の **BMR** クライアントの正しい値に置き換えられます。

**AIX** と **NetBackup** ソフトウェアのインストールが完了すると、`bmrstrtadm` コマンドを使用して、他のソフトウェアを **SRT** にインストールするためのオプションを指定できます。ここで他のソフトウェアを追加するか、処理を終了します (ソフトウェアは後で追加できます)。[**SRT** への **NetBackup** クライアントインストール (**NetBackup client installation into SRT**)] 手順中、オペレーティングシステムのアーキテクチャ形式と **NetBackup** クライアントのバージョンに互換性がない場合、エラーメッセージが表示されます。

他のソフトウェアの追加方法に関する詳細情報が利用可能です。

p.66 の「[共有リソースツリーへのソフトウェアの追加](#)」を参照してください。

## HP-UX SRT の作成

HP-UX SRT の作成時には、次のインストール処理の手順が示されます。

- **Ignite** ソフトウェア  
SRT を **PA-RISC2** ベースのクライアントのリストアに使用する場合は、**Ignite-UX 5.3x** 以上のものを使用して **SRT** を作成します。
- オペレーティングシステムソフトウェア
- **NetBackup** クライアントソフトウェア

## HP-UX SRT を作成するには

- 1 SRT を作成するブートサーバー上で、次のディレクトリに移動します。

```
/usr/opensv/netbackup/bin
```

- 2 次のコマンドを入力します。

```
./bmsrtdm
```

- 3 プロンプトが表示されたら、新しい SRT を作成するためのオプションを選択します。
- 4 次の表に示すようにコマンドプロンプトを完了します。

Enter the name of the SRT to create	その SRT が存在するディレクトリにも使用される SRT の名前。  英数字とアンダースコア ( _ ) のみを使用できます。
Enter the description of the new SRT	SRT の説明。
SRT OS level	ブートサーバーのオペレーティングシステムのバージョンに基づいて作成可能なレベル。
Enter desired Architecture (32/64)	64 ビット HP-UX オペレーティングシステムを入力します。  <b>メモ:</b> [SRT への NetBackup クライアントのインストール (NetBackup client installation into SRT)] 手順中、bmsrtdm は、SRT OS アーキテクチャ形式と NetBackup クライアントバージョンの間に互換性がない場合、該当するエラーメッセージを表示します。
Enter the directory in which to place the new SRT	SRT を作成するディレクトリへのパスを入力します。SRT 名を含む SRT の場所へのパス名が、SRT の root (SRT パスと呼ぶ) になります。  デフォルトは、/export/srt か、SRT が最後に正常に作成されたディレクトリのいずれかになります。  このディレクトリは存在している必要があります。

```
Location (device or directory  
path) of the Ignite install  
media.
```

BMR は、次のディレクトリを検索します ( $x.x$  は、11.00 または 11.11 のいずれかです)。

- Ignite-UX/FILE-SRV- $x.x$ /opt/ignite/data/Rel\_B. $x.x$ / (BOSdatapath)

BOSdatapath ディレクトリが検出された場合、BMR は Ignite のインストールイメージが次のいずれかのディレクトリ内に存在すると想定します (-PA は Ignite バージョン B41 を示しています)。

- 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

BOSdatapath ディレクトリが検出されなかった場合、BMR は、次のいずれかのディレクトリで提供された tar ファイルから INSTCMD5 という名前のファイルを検索します (-PA は Ignite バージョン B41 を示しています)。

- Ignite-UX/BOOT-KERNEL/opt/ignite/data
- Ignite-UX/BOOT-KERNEL-PA/opt/ignite/data

このファイルが検出されない場合、BMR は Ignite をインストールできません。

```
Enter the location (device or  
directory path) of the HP-UX  $x.x$   
install media
```

変数  $x.x$  は、SRT オペレーティングシステムのバージョンです。

```
The following patches are  
required for this SRT:  
patch_list
```

使用している Ignite のバージョンにパッチが必要な場合は、そのバージョンで必要とされる特定のパッチへのパスを入力するプロンプトが表示されます。

```
These patches can be found on  
an HPE support plus media, or  
they can be downloaded from the  
HPE web site.
```

**メモ:** HP-UX 11.11 PARISC の SRT を作成するには、新しいパッチ PHCO\_36006 が必要です。このパッチは、HP-UX 11.11 「Dec\_2009\_11i\_GoldPack」パッチバンドルから入手できます。このパッチバンドルをダウンロードし、Dec\_2009\_11i\_GoldPack の場所を指定してパッチ PHCO\_36006 をインストールする必要があります。

```
Location (device or path) of the  
media that contains patch_list:
```

Location (device or path) of the Veritas NetBackup install media	NetBackup クライアントソフトウェアのインストールメディアが挿入されているデバイス名を入力するか、インストールイメージへのパスを入力します。  デバイス名またはパスを入力すると、NetBackup クライアントのインストールプロシージャによって、クライアントソフトウェアが SRT にインストールされます。
Do you want to continue? [y,n] (y) y	y を入力します。
Do you want to install the NetBackup client software for this client? [y,n] (y)	y を入力します。
Enter the name of the NetBackup server:	空白以外の値を入力します。サーバー名は、リストア時に、リストア対象の BMR クライアントの正しい値に置き換えられます。
Would you like to use servername as the configured name of the NetBackup client? [y,n] (y)	デフォルトのまま使用するか、空白以外の値を入力します。クライアント名は、リストア時に、リストア対象の BMR クライアントの正しい値に置き換えられます。

HP-UX と NetBackup ソフトウェアのインストールが完了すると、`bmsrtdm` コマンドを使用して、他のソフトウェアを SRT にインストールするためのオプションを指定できます。ここで他のソフトウェアを追加するか、処理を終了します (ソフトウェアは後で追加できません)。

他のソフトウェアの追加方法に関する詳細情報が利用可能です。

p.66 の「[共有リソースツリーへのソフトウェアの追加](#)」を参照してください。

## Solaris SRT の作成

Solaris SRT の作成時には、次のソフトウェアのインストール手順が示されます。

- オペレーティングシステムソフトウェア
- NetBackup クライアントソフトウェア

次の追加情報の確認が必要になる場合もあります。

- p.70 の「[パッチおよびパッケージの Solaris SRT へのインストールについて](#)」を参照してください。

### Solaris SRT を作成する方法

- 1 SRT を作成するブートサーバー上で、次のディレクトリに移動します。

```
/usr/opensv/netbackup/bin
```

- 2 次のコマンドを入力します。

```
./bmrstadm
```

- 3 プロンプトが表示されたら、新しい SRT を作成するためのオプションを選択します。

#### 4 次の表に示すようにコマンドプロンプトを完了します。

Enter the name of the SRT to create	その SRT が存在するディレクトリにも使用される SRT の名前。  英数字とアンダースコア ( <code>_</code> ) のみを使用できます。
Enter the description of the new SRT	SRT の説明。
Enter desired level of Solaris/SunOS	ブートサーバーのオペレーティングシステムのバージョンに基づいて、作成可能なレベルを入力します。
Enter the directory in which to place the new SRT	SRT を作成するディレクトリへのパスを入力します。SRT 名を含む SRT の場所へのパス名が、SRT のルート (SRT パスと呼ぶ) になります。  デフォルトは、 <code>/export/srt</code> か、SRT が最後に正常に作成されたディレクトリのいずれかになります。  このディレクトリは存在している必要があります。
Enter a [hostname:/]pathname containing a suitable Solaris x.x Boot CDROM or OS image location	インストールプログラムが挿入されているデバイス名を入力するか、OS インストールイメージが抽出されるパスを入力します。

**メモ:** SRT の作成には、SRT に開発者スタジオ 12.6 のランタイムパッチが必要です。パッチは <https://www.oracle.com> からダウンロードできます

OracleDeveloperStudio12.6-solaris-<platform>-pkg.tar.bz2 から抽出されたパッチを含むローカルディレクトリパスを入力します。

プロンプトが表示されたら、マウントされる場所ではなく、ISO パスが提供されることを確認します。

パッチファイル (tar.bz2 の拡張子) を抽出するには、記事に記載されている手順に従ってください。

次のパスを指定します。

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

デバイス名またはパスを入力すると、オペレーティングシステムが SRT にインストールされます。

Enter a [hostname:]/ pathname containing NetBackup client software	NetBackup ソフトウェアのインストールメディアが挿入されているデバイス名を入力するか、install という名前のインストールプログラムへのパスを入力します。
Do you want to continue? [y,n] (y) y	デバイス名またはパスを入力すると、NetBackup のインストールプロシージャによって、クライアントソフトウェアが SRT にインストールされます。
Do you want to install the NetBackup client software for this client? [y,n] (y)	y を入力します。
Enter the name of the NetBackup server:	y を入力します。
Enter the name of the NetBackup server:	空白以外の値を入力します。サーバー名は、リストア時に、リストア対象の BMR クライアントの正しい値に置き換えられます。
Would you like to use servername as the configured name of the NetBackup client? [y,n] (y)	デフォルトのまま使用するか、空白以外の値を入力します。クライアント名は、リストア時に、リストア対象の BMR クライアントの正しい値に置き換えられます。

Solaris と NetBackup ソフトウェアのインストールが完了すると、bmrstadm コマンドを使用して、他のソフトウェアを SRT にインストールするためのオプションを指定できます。ここで他のソフトウェアを追加するか、処理を終了します (ソフトウェアは後でいつでも追加できます)。

他のソフトウェアの追加方法に関する詳細情報が利用可能です。

p.66 の「共有リソースツリーへのソフトウェアの追加」を参照してください。

## Linux SRT の作成

Linux ブートサーバーでの SRT の初回の作成時に、次のソフトウェアのインストール手順が示されます。

- オペレーティングシステムソフトウェア
- BMR のサードパーティ製品。これは、ベンダーの Linux ディストリビューションに含まれていないオープンソース製品です。Cohesity は 3PPCD のサードパーティのコンポーネントをそれぞれの最新リリースに更新します。たとえば、次の技術記事を参照してください。

[https://www.veritas.com/content/support/ja\\_JP/downloads/update.UPD238422](https://www.veritas.com/content/support/ja_JP/downloads/update.UPD238422)

### ■ NetBackup クライアントソフトウェア

この処理中に、`bmrstadm` コマンドを使用して、BMR のサードパーティインストールプログラムから次のディレクトリにファイルをコピーできます。

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

ブートサーバーに **SRT** を作成した後、`bmrstadm` では毎回それらのインストールファイルが使用されます。サードパーティ製品のイメージへのパスを再入力する必要はありません。インストールプログラムまたはイメージの場所を入力するプロンプトをもう一度表示する場合は、`bmrstadm` コマンドを実行する前に `media` ディレクトリを削除します。

BMR サードパーティ製品 **CD** は、ISO ファイルシステムイメージとして配布されます。イメージをダウンロードしてソースイメージとして使用したり、**CD** メディアに書き込むことが可能です。

### Linux SRT を作成するには

- 1 SRT を作成するブートサーバー上で、次のディレクトリに移動します。

```
/usr/opensv/netbackup/bin
```

- 2 次のコマンドを入力します。

```
./bmrstadm
```

- 3 プロンプトが表示されたら、新しい SRT を作成するためのオプションを選択します。

#### 4 次の表に示すようにコマンドプロンプトを完了します。

Enter the name of the SRT to create	その SRT が存在するディレクトリにも使用される SRT の名前。  英数字とアンダースコア ( <code>_</code> ) のみを使用できます。
Enter the description of the new SRT	SRT の説明。
Enter the directory in which to place the new SRT	SRT を作成するディレクトリへのパスを入力します。SRT 名を含む SRT の場所へのパス名が、SRT のルート (SRT パスと呼ぶ) になります。  デフォルトは、 <code>/export/srt</code> か、SRT が最後に正常に作成されたディレクトリのいずれかになります。  このディレクトリは存在している必要があります。
The following media is required: Linux distribution - disk x of x Please load the media now. Load media from:	Linux ディストリビューション (Red Hat または SuSE) および必要なディスク。  <code>bmrprtadm</code> コマンドによって、複数の Linux インストールディスクを要求するプロンプトが表示されます。  一部のシステムでは、自動的に CD ドライブにロードされたメディアのマウントを試行します (Red Hat の <code>magicdev</code> 処理など)。これらのシステム上のメディアを要求するプロンプトが表示されたら、ドライブにメディアをロードし、ドライブトレイを閉じて、ドライブの表示灯の点滅が停止するまで待ってから <b>Enter</b> キーを押します。
The following media is required: BMR third-party products CD (3PPCD) Please load the media now. Load media from:	BMR サードパーティ製品 CD が挿入されているデバイス名を入力するか、インストールイメージへのパスを入力します。  この CD には、Linux システムで BMR が使用するオープンソースコンポーネントが含まれています。

```
The following media is required: NetBackup クライアントソフトウェアのイン  
ストールメディアが挿入されているデバイス名を  
NetBackup x.x Client 入力するか、インストールイメージへのパスを  
Please load the media now. 入力します。  
Load media from: デバイス名またはパスを入力すると、  
NetBackup クライアントのインストールプロ  
シージャによって、クライアントソフトウェアが  
SRT にインストールされます。  
  
Do you want to continue? [y,n] y を入力します。  
(y) y  
  
Do you want to install the NetBackup client software for  
this client? [y,n] (y) y を入力します。  
  
Enter the name of the NetBackup server: 空白以外の値を入力します。サーバー名は、  
リストア時に、リストア対象の BMR クライアン  
トの正しい値に置き換えられます。  
  
Would you like to use servername as the configured name of the  
NetBackup client? [y,n] (y) デフォルトのまま使用するか、空白以外の値  
を入力します。クライアント名は、リストア時に、  
リストア対象の BMR クライアントの正しい値  
に置き換えられます。
```

Linux と NetBackup ソフトウェアのインストールが完了すると、`bmrprtadm` コマンドを使用して、他のソフトウェアを SRT にインストールするためのオプションを指定できます。ここで他のソフトウェアを追加するか、処理を終了します (ソフトウェアは後でいつでも追加できます)。

他のソフトウェアの追加方法に関する詳細情報が利用可能です。

p.66 の「[共有リソースツリーへのソフトウェアの追加](#)」を参照してください。

## 共有リソースツリーの管理

既存の SRT をインポート、コピー、または削除することができ、SRT にソフトウェアを追加することもできます。

## 共有リソースツリーへのソフトウェアの追加

リストア中、必要な場合にかぎり、追加ソフトウェアを既存の SRT にインストールします。追加ソフトウェアには、NetBackup クライアントソフトウェアが必要とするオペレーティングシステムのパッチやファイルセットなどがあります。SRT 内のソフトウェアは、リストア対象のシステムにインストールされることはありません。これは、保護対象のシステムをリストア

可能な元のファイルの状態に戻す場合にのみ使用されます。そのため、パッチ、メンテナンスレベル、Maintenance Pack、Service Pack、ファイルセットまたはドライバを、保護対象のシステム内にある SRT にインストールする必要はありません。

クラスタソフトウェアを SRT にインストールする必要はありません。ローカルファイルシステムのリストア後に、クライアントはクラスタを再度追加します。

次のタスクに関する詳細情報が利用可能です。

- p.67 の「UNIX または Linux SRT へのソフトウェアの追加」を参照してください。
- p.71 の「Windows SRT へのソフトウェアの追加」を参照してください。

## UNIX または Linux SRT へのソフトウェアの追加

bmrprtadm コマンドで、追加ソフトウェアを既存の UNIX または Linux SRT にインストールするためのオプションを使用できます。

すべてのシステムですべてのオプションがサポートされるわけではありませんが、次のオプションが利用可能です。

- Veritas NetBackup Maintenance Pack
- Arctera Volume Manager と Arctera File System
- Veritas Security Service
- その他のソフトウェア  
オプション名は、オペレーティングシステムによって異なります。

---

**メモ:** このリストの特別なオプションを使用してのみ、SRT に製品を追加できます。

---

SRT の作成時に必要な NetBackup ソフトウェアを追加しないと、変更オプションを選択した際に必要なソフトウェアの追加を要求するプロンプトが表示されます。

SRT の作成時に NetBackup ソフトウェアを追加すると、bmrprtadm コマンドを使用して、他のソフトウェアを SRT にインストールするためのオプションを指定できます。

### UNIX または Linux SRT にソフトウェアを追加するには

- 1 SRT が存在する BMR ブートサーバー上で、次のディレクトリに移動します。  
`/usr/opensv/netbackup/bin`
- 2 次のコマンドを入力します。  
`./bmrprtadm`
- 3 プロンプトが表示されたら、既存の共有リソースツリーを変更するためのオプションを選択します。

- 4 変更する SRT の名前を入力します。
- 5 目的のインストールオプションを選択します。

bmrstadm コマンドによって、ソフトウェアのインストール手順が示されます。通常、ソフトウェアのインストールプログラムまたはイメージへのパスを入力する必要があります。

続行するには、インストールするソフトウェアに関する次の情報を参照してください。

- p.68 の「[NetBackup Maintenance Pack の追加について](#)」を参照してください。
- p.68 の「[Arctera Volume Manager と Arctera File System の追加について](#)」を参照してください。
- p.69 の「[Veritas Security Services の追加について](#)」を参照してください。
- p.70 の「[その他のソフトウェアの追加について](#)」を参照してください。

### NetBackup Maintenance Pack の追加について

NetBackup の Maintenance Pack または Feature Pack が SRT の保護対象のクライアントにインストールされている場合は、この Maintenance Pack または Feature Pack を SRT にインストールします。

Cohesity Maintenance Pack のインストールオプションの選択時に、インストールプログラムまたはイメージの場所を要求する次のようなプロンプトが表示されます。

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

インストールプログラムまたはイメージの場所に絶対パスを入力します。

### Arctera Volume Manager と Arctera File System の追加について

次の情報は Linux システムには適用されません。

Arctera Volume Manager (VxVM) および Arctera File System (VxFS) が SRT の保護対象のシステムにインストールされている場合は、これらを SRT にインストールします。BMR はこれらを使用して、ディスクのパーティション作成およびファイルシステムの再構築を行えるようになります。

SRT 内の VxVM および VxFS のバージョンは、リストア対象のクライアントのバージョンと正確に一致している必要があります。このバージョンが一致していない場合、リストアされたクライアントソフトウェアは、ファイルシステムおよびボリュームにはアクセスできません。

保護対象のクライアントの VxVM または VxFS のバージョンが異なる場合、それらのバージョンごとに個別の SRT を作成します。ただし、VxVM および VxFS がインストールされた SRT を使用して、VxVM または VxFS がインストールされていないクライアントをリストアすることは可能です。同じオペレーティングシステムの SRT が複数必要である場合は、オペレーティングシステムと NetBackup クライアントソフトウェアだけを含む SRT を作成します(たとえば、異なるバージョンの VxVM や異なるドライバを含むクライアントをリストアする場合などです)。次に、必要な数だけコピーを作成し、そのコピーに異なるバージョンの他のソフトウェアを追加します。通常、既存の SRT をコピーした方が SRT を作成するよりも効率的です。

オペレーティングシステムのパッチなど、VxVM および VxFS に必要な前提条件を確認します。VxVM および VxFS をインストールする前に、適切な順序でこれらをインストールします。

---

**警告:** Solaris システムでは、パッチが `patchadd -c` フラグをサポートしていることを確認してください。SRT にインストールするのは `patchadd -c` フラグをサポートしているパッチのみにしてください。多くの VxFS および VxVM のパッチは `patchadd -c` フラグをサポートしていません。テストの結果には、パッチを適用しているバージョンの VxFS および VxVM を使用するクライアントが、リストアを正常に実行できることが示されます。これらのクライアントは、パッチを適用していないバージョンを含む SRT を使用する場合でもリストアを正常に実行します。

---

`bmrstadm` コマンドの [Veritas Volume Manager と Veritas File System のインストール (Install Veritas Volume Manager and Veritas File System)] オプションでは、次のようなプロンプトが表示されます。

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

これらのパッケージは、SRT にインストールする前に展開または解凍する必要はありません。各コンポーネントへのパスを要求するプロンプトが表示されたら、抽出されたパッケージへのパスを入力します。または、インストールプログラムのルートディレクトリへのパスを入力します (`file_system` および `volume_manager` ディレクトリを含むディレクトリ)。

VxVM および VxFS のオペレーティングシステムの依存関係について詳しくは、[https://www.veritas.com/support/ja\\_JP/article.100040093](https://www.veritas.com/support/ja_JP/article.100040093) で OSCL の表を参照してください

## Veritas Security Services の追加について

Bare Metal Restore バージョン 11.1 では、SRT の Veritas Security Services を個別にインストールする必要はありません。Veritas Security Services は、NetBackup クライ

アントとともに SRT にインストールされます。古いバージョンの NetBackup クライアントを含む SRT の場合は、Veritas Security を SRT に別途インストールする必要があります。アクセス管理のコンポーネントとアクセス管理の使用方法について詳しくは、『[NetBackup セキュリティおよび暗号化ガイド](#)』を参照してください。

### その他のソフトウェアの追加について

特別なオプションを使用してのみ、SRT にソフトウェアを追加できます。

他のソフトウェアで表示されるメニューオプションは、SRT のオペレーティングシステムによって異なります。

AIX	メンテナンスレベル (ML) または追加のファイルセット
HP-UX	他に必要なソフトウェアがないため、ソフトウェアを追加できません。
Linux	追加のドライバ
Solaris	追加のパッケージまたはパッチ

他のソフトウェアをインストールするときに、インストールプログラム、イメージ、パッケージ、パッチ、ファイルセットまたは RPM など (オペレーティングシステムによって異なる) の場所を入力するプロンプトが表示されます。

p.70 の「[パッチおよびパッケージの Solaris SRT へのインストールについて](#)」を参照してください。

p.70 の「[Linux SRT へのデバイスドライバのインストール](#)」を参照してください。

### パッチおよびパッケージの Solaris SRT へのインストールについて

Solaris SRT にパッチおよびパッケージをインストールする場合は、必ず `bmrstadm` コマンドを使用します。`bmrstadm` コマンドを使用すると、`pkgadd -R` フラグをサポートしていないパッケージによる破損を防ぐことができます。

miniroot にインストールされたパッチが `patchadd -c` フラグをサポートしていない場合、JumpStart サーバーと同様に BMR ブートサーバーも破損する可能性があります。そのため、`patchadd -c` フラグをサポートしていないパッチは SRT にインストールしないでください。

### Linux SRT へのデバイスドライバのインストール

Linux SRT にデバイスドライバを追加または更新するには、次の手順を実行します。

## Linux SRT にデバイスドライバをインストールする方法

- 1 メインメニューで「既存の SRT を変更する (Modify an existing SRT)」オプションを選択して変更する SRT の名前を指定します。
- 2 「追加パッチ/ドライバのインストール (Install additional patches/drivers)」オプションを選択します。

次のように表示されます。

```
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] :
```

適切なオプションを選択します。

追加の Linux のカーネルドライバ (.o、.ko) ファイルを SRT に追加するには、オプション 1 を選択します。このオプションを使用して、デフォルトでは Linux インストールメディアに存在せず、BMR リストア中に読み込む必要のあるドライバを追加できます。

## Windows SRT へのソフトウェアの追加

既存の Windows SRT には、次のものをインストールできます。

- NetBackup クライアントソフトウェア
- NetBackup Security Services

Windows SRT にソフトウェアを追加するには

- 1 SRT をホスティングする Windows BMR ブートサーバーの「スタート」メニューで、「プログラム」、「Cohesity NetBackup」、「Bare Metal Restore ブートサーバーアシスタント (Bare Metal Restore Boot Server Assistant)」の順にクリックします。
- 2 「Bare Metal Restore ブートサーバーアシスタント (Bare Metal Restore Boot Server Assistant)」で、「共有リソースツリー管理ウィザード (Shared Resource Tree Administration Wizard)」をクリックします。
- 3 共有リソースツリー管理ウィザードの「ようこそ (Welcome)」パネルで、「次へ (Next)」をクリックします。
- 4 SRT を更新するためのオプションを選択します。
  - SRT に NetBackup クライアントソフトウェアイメージを追加または更新します。SRT には、保護対象のシステムと同じバージョンの NetBackup クライアントイメージが含まれている必要があります。  
p.50 の「SRT への NetBackup クライアントの追加」を参照してください。

- SRT に **Cohesity Security Services** を追加します。  
p.51 の「[SRT への NetBackup Security Services の追加](#)」を参照してください。
- 5 プロンプトに従って、共有リソースツリーにソフトウェアを追加します。  
共有リソースツリーウィザードのヘルプページに追加情報があります。

## 共有リソースツリーのインポート

この項では、共有リソースツリーをインポートする方法についての情報を提供します。  
p.72 の「[Windows 上での SRT のインポート](#)」を参照してください。

### UNIX および Linux 上での SRT のインポート

この項では、UNIX と Linux で共有リソースツリーをインポートするための手順を示します。

UNIX および Linux のブートサーバー上では、`bmrstadm` コマンドを使用して SRT をインポートします。

#### UNIX および Linux 上で SRT をインポートする方法

- 1 次のコマンドを入力します。  

```
./bmrstadm
```
- 2 既存の共有リソースツリーをインポートするためのオプションを選択します。
- 3 次のように、必要な情報を入力します。
  - 新しい SRT の名前
  - 既存の SRT が存在するブートサーバーでのパス

### Windows 上での SRT のインポート

この項では、Windows 上で共有リソースツリーをインポートするための手順を示します。

---

メモ: NetBackup 7.6.1.2 以上のバージョンでは、Windows ブートサーバーはバージョン 6.X、6.5.X および 7.6 の SRT のインポートをサポートしません。

Windows 7.6.1.2 以降では、Windows ブートサーバーは古いレガシー SRT のインポートをサポートしません。

---

## 共有リソースツリーのコピー

別の SRT をコピーして、新しい SRT を作成できます。

新しい SRT は、`bmrstadm` コマンド (UNIX および Linux) または共有リソースツリー管理ウィザード (Windows) を実行したブートサーバー上に作成されます。既存の SRT は、ローカルまたはリモートのブートサーバーに存在する場合があります。

NFS サービスでは、リモートブートサーバーに存在する SRT をコピーする必要があります。リモートブートサーバーでは、NFS サーバーサービスを有効にする必要があります。

変更処理中の SRT はコピーできません。通常、SRT のコピーには数分かかります。ただし、ソース SRT のサイズや、別のブートサーバーにコピーする場合のネットワーク速度によっては、さらに時間がかかる場合もあります。

p.73 の「[UNIX および Linux 上での SRT のコピー](#)」を参照してください。

p.74 の「[Windows 上での SRT のコピー](#)」を参照してください。

## UNIX および Linux 上での SRT のコピー

UNIX および Linux のブートサーバー上では、`bmrstadm` コマンドを使用して SRT をコピーします。

### UNIX および Linux 上での SRT をコピーする方法

- 1 SRT を作成するブートサーバー上で、次のディレクトリに移動します。

```
/usr/opensv/netbackup/bin
```

- 2 次のコマンドを入力します。

```
./bmrstadm
```

- 3 プロンプトが表示されたら、既存の共有リソースツリーをコピーするためのオプションを選択します。
- 4 プロンプトが表示されたら、必要な情報を次のように入力します。
  - コピーする既存の SRT の名前
  - 新しい SRT の名前
  - SRT を作成するブートサーバー上のパス
  - SRT の説明
  - (Linux のみ) BMR サードパーティのオプション CD が挿入されたデバイスへのパスまたは BMR サードパーティのオプション CD のインストールイメージへのパス (SRT がまだ作成されていない Linux ブートサーバー上に SRT をコピーしている場合のみ)

## Windows 上での SRT のコピー

Windows ブートサーバー上では、共有リソースツリー管理ウィザードを使用して SRT をコピーします。

p.49 の「[SRT のコピー](#)」を参照してください。

## 共有リソースツリーの削除

bmrstadm コマンド (UNIX および Linux ブートサーバー) または共有リソースツリー管理ウィザード (Windows ブートサーバー) を使用して、SRT を削除できます。

リストアタスクに割り当てられた SRT または変更中の SRT は削除できません。

## UNIX および Linux 上での SRT の削除

UNIX および Linux のブートサーバー上では、bmrstadm コマンドを使用して SRT を削除します。

### UNIX および Linux 上での SRT を削除する方法

- 1 SRT が存在するブートサーバー上で、次のディレクトリに移動します。

```
/usr/opensv/netbackup/bin
```

- 2 次のコマンドを実行します。

```
./bmrstadm
```

- 3 プロンプトが表示されたら、既存の共有リソースツリーを削除するためのオプションを選択します。
- 4 プロンプトが表示されたら、SRT 名を入力し、Enter キーを押します。
- 5 SRT を削除したいかどうかを尋ねられたら、SRT を削除するために **y** を入力します。

SRT がロックされている場合、この処理は失敗します。

p.76 の「[共有リソースツリーの無効なロックの解除](#)」を参照してください。

## Windows 上での SRT の削除

Windows ブートサーバー上では、共有リソースツリー管理ウィザードを使用して SRT を削除します。

p.49 の「[SRT の削除](#)」を参照してください。

## SRT の排他的な使用を有効にまたは無効にする方法

次の情報は UNIX と Linux クライアントにのみ適用されます。

クライアント設定でカスタムファイルを保存する場合は、これらのカスタムファイルを SRT にコピーできます。その後、これらのファイルは、リストア中にクライアント上の一時的なオペレーティングシステム環境で使用されます。これを行うには、クライアントによる SRT の排他的な使用を有効にします。他のクライアントは、排他的な使用が無効にされるまで SRT を使用できなくなります。排他的な使用では、SRT からカスタムファイルが削除されます。

次のいずれかの処理を行う前に、排他的な使用を有効にします。

- リストア準備処理
- 検出準備処理
- ブート可能 CD/DVD を作成します (カスタムファイルが存在する SRT を含むブート可能 CD/DVD を作成する場合)。

---

**メモ:** 特定のクライアント用にカスタムファイルを保存する前に、SRT の排他的な使用を有効にすると、リストア準備処理または検出準備処理が失敗します。

---

次の追加情報の確認が必要になる場合もあります。

p.27 の「[UNIX または Linux でのカスタムファイルの保存](#)」を参照してください。

**SRT の排他的な使用を有効または無効にするには**

- 1 SRT が存在するブートサーバー上で、次のディレクトリに移動します。

```
/opt/opensrv/netbackup/bin
```

- 2 次のコマンドを入力します。

```
./bmsrtdm
```

- 3 プロンプトが表示されたら、既存の共有リソースツリーを変更するためのオプションを選択します。
- 4 プロンプトが表示されたら、変更する SRT の名前を入力します。
- 5 プロンプトが表示されたら、SRT の排他的な使用を変更するオプションを選択します。
- 6 プロンプトが表示されたら、次のどちらかを行います。
  - 排他的な使用を有効にするには、クライアント名を入力してください。
  - 排他的な使用を無効にするには、何も入力しないで **Enter** キーを押します。

## 破損した共有リソースツリーの修復

次の情報は UNIX および Linux のブートサーバーにのみ適用されます。

BMR で SRT が [DAMAGED] 状態になった場合は、SRT を修復し、[READY] 状態に戻すことが可能な場合があります。以前に実行していた `bmrstadm` コマンドを中断したために SRT が [DAMAGED] とマークされた場合は、修復の可能性は高くなります。SRT が [DAMAGED] とマークされた理由が特定できない場合は、SRT を削除して、最初から新しい SRT を作成します。

SRT の状態は、NetBackup Web UI の左側の [Bare Metal Restore]、[リソース (Resources)]、[共有 (Shared)] リソースツリーに表示されます。

### 破損した共有リソースツリーを修復する方法

- 1 SRT が存在するブートサーバー上で、次のディレクトリに移動します。

```
/usr/opensv/netbackup/bin
```

- 2 次のコマンドを実行します。

```
./bmrstadm
```

- 3 既存の共有リソースツリーを修正するためのオプションの番号を入力します。
- 4 SRT の名前を求められたら、破損した SRT の名前を入力します。
- 5 続行するかどうか尋ねられたら、`y` を入力します。

`bmrstadm` プログラムにより、SRT の修復が試行されます。このプログラムでは、不足している SRT コンポーネントのインストール手順が示されます。

修復に成功した場合は、`bmrstadm` コマンドの変更メニューが表示されます。このプログラムを終了すると、SRT が [READY] 状態になります。

## 共有リソースツリーの無効なロックの解除

次の情報は UNIX および Linux のブートサーバーにのみ適用されます。

LOCKED\_READ または LOCKED\_WRITE 状態の SRT はビジー状態で、ほとんどの処理が許可されません。ロックされた SRT を管理するには、SRT を使用する処理のロック状態が終了して解放されるまで待機してから、処理を続行する必要があります(ただし、LOCKED\_READ 状態の SRT をリストアタスクに割り当てる処理だけは実行できます)。

まれに、SRT が無効なロック状態のままになっている場合があります。たとえば、ブートサーバーが SRT 処理の途中でクラッシュまたは再ブートされた場合、SRT がロック状態のまま残る可能性があります。SRT のロックが無効であることが確実な場合は、そのロックを解除できます。

SRT の状態は、NetBackup Web UI の [Bare Metal Restore]、[リソース (Resources)]、[共有 (Shared)] リソースツリービューに表示されます。

### 無効な SRT ロックを解除する方法

- 1 SRT が存在するブートサーバー上で、次のディレクトリに移動します。

```
/usr/opensv/netbackup/bin
```

- 2 次のコマンドを実行します。

```
./bmsrtdm
```

- 3 選択を求められたら、共有リソースを変更するためのオプションの番号を入力します。次のように表示されます。

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

- 4 既存の SRT の名前を求められたら、ロックされた SRT の名前を入力して Enter キーを押します。

---

**警告:** SRT が無効であることが確実な場合以外は、SRT ロックを解除しないでください。使用中の SRT のロックを解除すると、SRT が破損する可能性があります。

---

- 5 ロックの解除を確定するかどうかを尋ねられたら、ロックを解除するために **y** を入力します。

無効なロックが解除されます。

bmsrtdm コマンドの変更メニューが表示されます。

このプログラムを終了すると、SRT が [READY] 状態になります。

## ブートメディアの管理

ブートメディアは、クライアントをブートしたり、共有リソースツリーや、共有リソースツリーをマウントするリソースを提供するために使用されます。ブートメディアには、カーネル、RAM ファイルシステム、ライブラリ、プログラムなどを含む小規模な実行時環境が格納されます。クライアントシステムのファームウェアは、メディアからカーネルをブートします。このブートメディアにも共有リソースツリーが含まれています。

メディアを使用してクライアントシステムをブートする場合、BMR を使用して適切なブートメディアを準備する必要があります。ブートメディアは、リストア前にいつでも準備できます。ただし、前提条件として、保護対象のシステムの共有リソースツリーが存在している必要があります。

ブートメディアは、SRT に格納されたリソースから作成されます。

## Windows のサポート対象のブートメディアについて

BMR のリストア処理は、BMR によって準備されたブートメディア (CD または DVD) または BMR ブートサーバーからのクライアントのネットワークブートによって開始されます。

Windows プラットフォームでは、次のオプションでのみ BMR クライアントをブートすることができます。

- ネットワークブート
- CD/DVD メディアブート

---

**メモ:** Windows プラットフォームでは、フロッピーベースのリストアは PC-DOS の廃止によりサポートされません。

---

## CD または DVD の書き込みについて

BMR が生成するメディアブートイメージのサイズは、いくつかの要因によって決まります。インストールプログラムの構造は、リリースおよびメディア形式 (CD と DVD) によって異なる可能性があります。そのため、生成された最終的なイメージのサイズは、条件が同じように見えても異なることがあります。

BMR が生成するメディアブートイメージのサイズは、次に示す要因によって決まります。

- SRT 上のオプションのソフトウェアパッケージ
- オペレーティングシステムのバージョン
- メディアブートイメージの作成中に使用するインストールメディア形式 (適用可能な場合)

すべての場合において、BMR によって生成された最終的なメディアブートイメージが CD に収まる場合は、CD または DVD にイメージを書き込みます。ただし、最終的なイメージが CD に収まらない場合は、DVD に書き込む必要があります。

CD/DVD メディアは、そのメディアを作成したシステムでブートできる必要があります。特定のシステム用にブート可能 CD/DVD を作成するための正しい方法を調べるには、CD/DVD 書き込みソフトウェアで説明されている手順を参照してください。

また、次の点に注意してください。

- AIX、Linux および Solaris で作成された CD/DVD イメージは、ISO-9660 形式を使用します。HP-UX は、ISO とは異なるバイナリ形式を使用します。
- BMR には CD/DVD 書き込みソフトウェアが含まれていません。

次をサポートする CD/DVD 書き込みソフトウェアを使って、ディスクに CD/DVD のイメージを書き込みます。

- AIX、Linux および Solaris 用の ISO 形式のイメージ

- HP-UX 用のバイナリイメージ  
CD/DVD に書き込む手順は、アプリケーションによって異なります。手順については、該当するマニュアルを参照してください。
- CD/DVD 書き込みソフトウェアによっては、末尾に `.iso` 拡張子が付いている ISO 形式またはバイナリ形式の CD/DVD イメージファイルが必要な場合があります。必要な場合は、書き込む前に CD/DVD イメージに `.iso` 拡張子を追加できます。
- BMR ブートサーバーに CD/DVD 書き込みハードウェアおよびソフトウェアが含まれていない場合は、これらが含まれているシステムに CD/DVD イメージを転送します。CD/DVD イメージファイルがバイナリファイルとして正常に転送されたかどうかを確認します。破損した CD/DVD イメージファイルを使用すると、予期しない結果が発生します。
- SRT を含む CD/DVD メディアでは、SRT の名前が CD/DVD のルートディレクトリの内容として表示されます。
- 識別しやすいように、CD/DVD にラベルを付けます。  
次の情報を含めます。
  - クライアント名 (Windows クライアント)
  - 使用する NetBackup のバージョン
  - インストールする SRT のオペレーティングシステム
  - インストールする追加のソフトウェア
- BMR は、CD/DVD イメージファイルの作成後、そのファイルを使用しません。したがって、CD/DVD に書き込んだ後は、イメージファイルの移動、ファイル名の変更、削除などを実行できます。

## UNIX および Linux のブートメディアの作成

UNIX および Linux システムでは、`bmrstadm` コマンドを使用して、SRT を含むブート可能 CD/DVD イメージを作成します。CD/DVD イメージの作成後、CD/DVD 書き込みソフトウェアを使用して CD/DVD にイメージを書き込む必要があります。

この処理では、既存の SRT を CD/DVD メディアにコピーします。そのため、クライアントをサポートする SRT が存在している必要があります。

必要な情報は次のとおりです。

- 使用する SRT の名前
- CD/DVD 上の SRT に使用する名前
- CD/DVD イメージを格納するために十分な空き領域のあるディレクトリへのパス

## UNIX および Linux のブートメディアを作成する方法

- 1 Solaris システムの場合のみ、次のコマンドを使用して、SRT が存在するブートサーバー上で `vold` プロセスを実行していないことを確認します。

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

実行している場合は、次の手順を実行します。

- ロードされている可能性がある CD/DVD を取り出すには、次のコマンドを実行します。

```
# eject
```

- `vold` プロセスを停止するには、次のコマンドを実行します。

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

- 2 SRT が存在するブートサーバー上で、次のディレクトリに移動します。

```
/usr/opensv/netbackup/bin
```

- 3 次のコマンドを実行します。

```
./bmsrtdm
```

- 4 プロンプトが表示されたら、新しい CD/DVD イメージベースの共有リソースツリーを作成するオプションを選択します。

- 5 オペレーティングシステムに関する情報を参照して続行します。

p.80 の「[AIX のブートメディアについて](#)」を参照してください。

p.81 の「[HP-UX のブートメディアについて](#)」を参照してください。

p.81 の「[Linux のブートメディアについて](#)」を参照してください。

p.81 の「[Solaris のブートメディアについて](#)」を参照してください。

## AIX のブートメディアについて

ブートメディアの作成に使用する SRT を作成した、AIX インストールプログラムを手元に用意する必要があります。(メディアのネットワークコピーから SRT を作成した場合でも、AIX インストールプログラムが必要です) インストールプログラムを含むデバイス名を入力する必要があります。

CD/DVD イメージのディレクトリを、使用する SRT が含まれているディレクトリのそのままの接頭辞にしないでください。

たとえば、SRT が `/export/srt/aix433esm` の場合は、次を使うことができます。

- 場所として、`/`、`/export`、または `/export/srt` を指定しないでください。

- `/export/srt/mb` は SRT パスのそのままの接頭辞ではないため、指定可能です。

## HP-UX のブートメディアについて

HP-UX は、ISO とは異なるバイナリ形式を使用します。CD/DVD イメージファイルは、CD/DVD のバイナリイメージであり、拡張子は含まれません。ただし、CD/DVD 書き込みソフトウェアで拡張子が必要とされる場合は、CD/DVD イメージに `.iso` 拡張子を追加できます。

HP-UX イメージに対して動作することが確認されている CD/DVD 記録プログラムは次のとおりです。

- **Sony CD/DVD Extreme** - イメージファイル名に `.iso` 拡張子を追加して[ファイル (File)]メニューオプションの[Global Image]または[Other Image]オプションを使います。
- **Nero** - イメージファイル名に `.iso` 拡張子を追加し、[Burn Image to Disc]オプションを使います。

---

**メモ:** Roxio Easy CD/DVD Creator 記録プログラムは、HP-UX イメージに対して動作しません。

---

## Linux のブートメディアについて

Linux では、`bmsrtdm` コマンドによって、SRT の名前に `.iso` 拡張子が付いたブート ISO イメージファイルが作成されます。任意の標準 CD/DVD 書き込みソフトウェアを使用して、このファイルからメディアに書き込むことができます。

## Solaris のブートメディアについて

CD/DVD にコピーする SRT の作成に使用した Solaris インストールメディア (Software 1 of 2) を手元に用意する必要があります。インストールメディアを含むデバイス名を入力する必要があります。

SRT に関する情報を入力すると、次の情報が表示されます。

- **Arctera Volume Manager (VxVM)** が BMR ブートサーバーにインストールされている場合は、次のように表示されます。

```
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] :
```

1 または 2. を入力します。次に、ディスクグループ名または **raw** パーティションのデバイスファイル名を入力します。一時的なストレージに **raw** パーティションを使用する場合、続行を確認するプロンプトが表示されます。

- **Arctera Volume Manager (VxVM)** が **BMR** ブートサーバーにインストールされていない場合は、次のように表示されます。

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

**raw** パーティションのデバイスファイル名を入力します。続行する場合は次のプロンプトに応答します。

CD/DVD イメージを作成した後で、`bmrstadm` コマンドを実行する前に `vold` プロセスを停止した場合は、このプロセスを再起動します (`/etc/init.d/volmgt start`)。

## Windows クライアントのブートメディアの作成

Windows システムでは、CD または DVD への書き込みが可能なブート ISO イメージを作成できます。

### Windows クライアントのブートメディアを作成する方法

- 1 Windows の **BMR** ブートサーバーで、Windows の [スタート]メニューから [プログラム] > [Cohesity NetBackup] > [Bare Metal Restore Boot Server Assistant] を選択します。  
[Bare Metal Restore ブートサーバーアシスタント (Bare Metal Restore Boot Server Assistant)] 画面が表示されます。
- 2 [共有リソースツリー管理ウィザード (Shared Resource Tree Administration Wizard)] をクリックします。
- 3 [共有リソースツリーからブート可能 CD/DVD を作成する。 (Create a Bootable CD/DVD from a Shared Resource Tree.)] オプションを選択します。
- 4 プロンプトに従って、ブートメディアを作成します。

# クライアントのリストア

この章では以下の項目について説明しています。

- [BMR リストア処理](#)
- [クライアントのリストアを準備する方法](#)
- [BMR ディスクリカバリ動作](#)
- [ネットワークブートによる BMR クライアントのリストアについて](#)
- [メディアブートによる BMR クライアントのリストアについて](#)
- [汎用的な BMR リストア](#)
- [ハードウェアの汎用的な検出](#)
- [指定した時点へのリストアについて](#)
- [異なるディスクへのリストアについて](#)
- [異なる システムへのリストア](#)
- [NetBackup メディアサーバーのリストアについて](#)
- [BMR ブートサーバーのリストアについて](#)
- [AWS RHEL および Windows VM クライアントのリストアについて](#)
- [外部プロシージャについて](#)
- [SAN \(ストレージエリアネットワーク\) のサポートについて](#)
- [複数のネットワークインターフェースのサポートについて](#)
- [リストア時のポートの使用](#)

# BMR リストア処理

保護対象のシステムをリストアする手順は、実行するリストア形式およびクライアントのオペレーティングシステムによって異なります。

表 6-1 リストア形式

リストア形式	手順
同じクライアントにリストアし、最新のバックアップを使用する場合	p.93 の「ネットワークブートによる BMR クライアントのリストアについて」を参照してください。 p.107 の「メディアブートによる BMR クライアントのリストアについて」を参照してください。
指定した時点にリストアする場合	p.120 の「指定した時点へのリストアについて」を参照してください。
クライアントを異なるディスクにリストアする場合	p.123 の「異なるディスクへのリストアについて」を参照してください。
新しいターゲットシステムにリストアする場合 (Windows システムでのみ)	p.128 の「異なるシステムへのリストア」を参照してください。
NetBackup メディアサーバーをリストアする場合	p.133 の「NetBackup メディアサーバーのリストアについて」を参照してください。
BMR ブートサーバーをリストアする場合	p.136 の「BMR ブートサーバーのリストアについて」を参照してください。
リストア処理をカスタマイズする場合	p.138 の「外部プロシージャについて」を参照してください。

その他の情報も利用可能です。

p.86 の「クライアントのリストアを準備する方法」を参照してください。

p.88 の「BMR ディスクリカバリ動作」を参照してください。

p.148 の「SAN (ストレージエリアネットワーク) のサポートについて」を参照してください。

p.152 の「リストア時のポートの使用」を参照してください。

NetBackup BMR マスターサーバーはリストア処理を次のように管理します。

- マスターサーバーは、リストア準備処理の実行時に、必要な構成ファイルおよびリストアスクリプト (UNIX および Linux の場合) またはリストア処理 (Windows の場合) を作成し、ブートサーバーを割り当てます。
- クライアントをネットワークブートまたはメディアブートによってブートします。

- クライアントは、ブートサーバーまたはブートメディアから共有リソースツリーにアクセスします。
- クライアントは、リストア環境とも呼ばれる一時的なオペレーティングシステム環境を実行します。リストア環境は共有リソースツリーから起動します。
- クライアントリストア環境は、マスターサーバーからリストアスクリプトおよび構成ファイルを取得します。
- クライアントリストア環境は、カスタマイズされたリストア処理を実行して、ディスクを構成します。
- クライアントリストア環境は、NetBackup クライアントソフトウェアを使用して、自動リストアを実行し、NetBackup サーバーからすべての必要なファイルおよびデータをリストアします。
- クライアントが再ブートし、リストアされたオペレーティングシステムを起動して、ブートサーバーの割り当てを解除します。
- Dissimilar System Restore タスクが完了します (Dissimilar System Restore の場合のみ)。

図 6-1 に、標準のネットワークリストアを示します。

図 6-1 ネットワークリストア

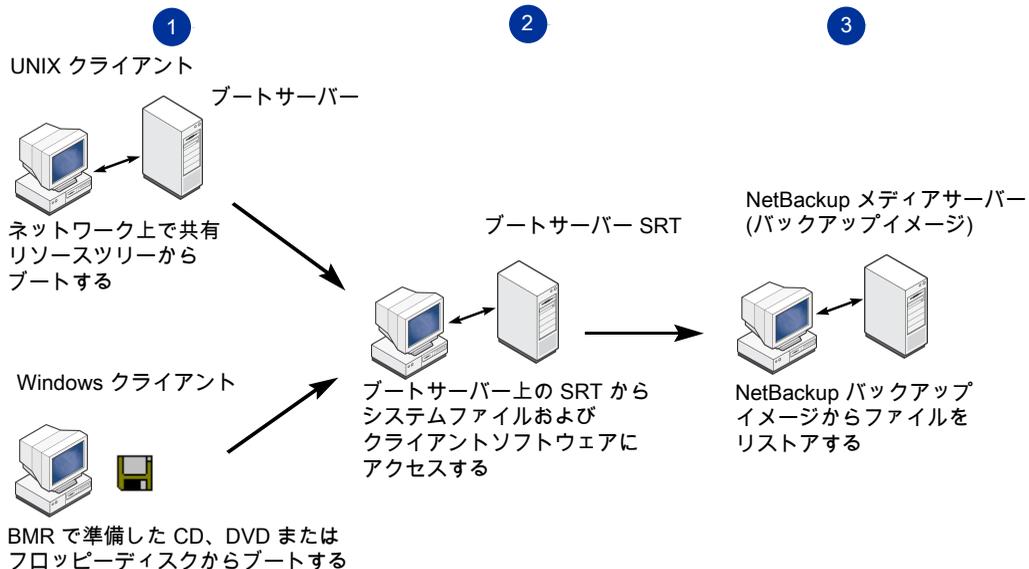
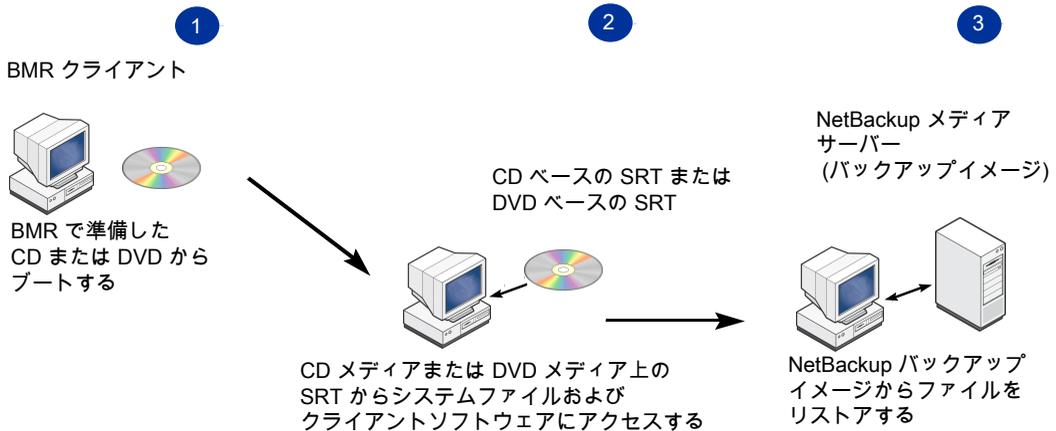


図 6-2 に、メディアリストアを示します。

図 6-2 メディアリストア



## クライアントのリストアを準備する方法

リストア準備操作を続行する前に、NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換マトリックスを確認します。

p.265 の「NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換性の表」を参照してください。

クライアントをリストアする前に、クライアントをリストア準備 (PTR) する必要があります。

リストア準備処理では、NetBackup マスターサーバーは次の処理を実行します。

- マスターサーバーデータベースからクライアント構成を取得します。
- クライアントのリストアに使用するリストアスクリプトおよび構成ファイルを作成します。
- ブートサーバーリソースを選択したクライアントリカバリに割り当てます。

クライアントをリストア準備する場合、リストアに使用する構成を次のように選択します。

- 標準リストア (セルフリストアとも言い、同じシステムにリストアする) では、現在の構成を選択します。
- 他のリストア形式では、リストア用に作成した構成を選択します。

リストアに最新データが確実に含まれるようにするために、Cohesity ではシステムをリストアする直前にリストアを準備することをお勧めします。

コマンドについては、『NetBackup コマンドリファレンスガイド』を参照してください。

### bmrprep コマンドを使用してクライアントのリストアを準備する方法

- 1 管理者としてログインします。
- 2 bpnbat コマンドを実行します。
- 3 bmrprep コマンドを実行して、リストア準備操作を開始します。

bmrprep コマンドを実行すると、SRT バージョンや構成バージョンなどのさまざまなパラメータに関連する検証チェックが実行されます。

- リストアの準備のための検証チェックが正常に実行された場合、クライアントは自動リカバリのマークが付けられます。この自動リカバリは、デフォルトでは 48 時間有効です。マスターサーバーの真正性は自動的に検証され、ホスト ID ベースの証明書は自動リカバリ処理中にこのクライアントに対して自動的に発行されます。nbhostmgmt コマンドを使用して、クライアントに自動リカバリのマークが付いているかどうかを確認します。  
自動リカバリとホスト ID ベースの証明書について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。  
[https://www.veritas.com/support/en\\_US/article.DOC5332](https://www.veritas.com/support/en_US/article.DOC5332)
- 検証チェックが失敗した場合は、適切なエラーメッセージが表示されます。メッセージに示される手順に従います。  
詳しくは、p.213 の「リストア準備および検出準備のエラーメッセージと、BMR 用の安全な通信に関連する bmrprep コマンド」を参照してください。を参照してください。

クライアントはリストアの準備ができています。

### NetBackup Web UI を使用してクライアントのリストアを準備する方法

- 1 NetBackup Web UI で、[Bare Metal Restore]、[ホスト (Hosts)]、[Bare Metal Restore クライアント (Bare Metal Restore Clients)]の順に展開します。
- 2 クライアントまたはクライアント構成を選択します。
- 3 [処理 (Actions)]、[リストア準備 (Prepare to Restore)]の順に選択します。
- 4 [クライアントのリストア準備 (Prepare to Restore Client)]ダイアログボックスで、リストアの適切な値を選択します。

クライアントとクライアント構成のいずれを選択したかによって、完了するフィールドが異なります。

他の PTR オプションが選択されている場合、p.88 の「BMR ディスクリカバリ動作」を参照してください。

- 5 [OK]をクリックします。

Bare Metal Restore によって、リストア準備のためのすべての処理が実行されます。

[リストア準備 (Prepare to Restore)]をクリックすると、SRT バージョンや構成バージョンなどのさまざまなパラメータに関連する検証チェックが実行されます。

- リストアの準備のための検証チェックが正常に実行された場合、クライアントは自動リカバリのマークが付けられます。この自動リカバリは、デフォルトでは 48 時間有効です。マスターサーバーの真正性は自動的に検証され、ホスト ID ベースの証明書は自動リカバリ処理中にこのクライアントに対して自動的に発行されます。nbhostmgmt コマンドを使用して、クライアントに自動リカバリのマークが付いているかどうかを確認します。  
自動リカバリとホスト ID ベースの証明書について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。  
[https://www.veritas.com/support/en\\_US/article.DOC5332](https://www.veritas.com/support/en_US/article.DOC5332)  
[https://www.veritas.com/support/en\\_US/article.DOC5332](https://www.veritas.com/support/en_US/article.DOC5332)
- 検証チェックが失敗した場合は、適切なエラーメッセージが表示されます。メッセージに示される手順に従います。  
詳しくは、p.213 の「リストア準備および検出準備のエラーメッセージと、BMR 用の安全な通信に関連する bmrprep コマンド」を参照してください。を参照してください。

## 6 処理が完了すると表示されるダイアログボックスで、[OK]をクリックします。

クライアントは キューへ投入済み 状態で Bare Metal Restore タスクのリストに登録されています。リストア準備は完了するまで数分間かかります。

### リストア構成をクリーンアップする方法

- 1 NetBackup Web UI で、[Bare Metal Restore]、[BMR タスク (BMR Tasks)]の順に選択します。
- 2 詳細ペインで、リストア構成をクリーンアップするクライアントを右クリックします。
- 3 ショートカットメニューから[クリーンアップ (Clean Up)]を選択します。  
タスクで使用されていたリソースの割り当てが解除され、[タスクの状態 (State)]が[完了 (Done)]に、[状態 (Status)]が[150](ユーザーにより終了)に設定されます。

## BMR ディスクリカバリ動作

リストア時に、BMR は、次のように、ディスクをリストアまたはインポートします。

- ディスクのリストアとは、BMR がディスクをフォーマットし、そのディスクにファイルをリストアすることを意味します。ディスク上のデータの保持は試行されません。
- ディスクのインポートとは、BMR がディスク上のボリュームを再利用しようとする (つまり、リストア後に自動的にファイルシステムをマウントする)ことを意味します。BMR は、ディスクをフォーマットしてそこにファイルをリストアするのではなく、再利用を試行します。

BMR は常にシステムディスクをリストアします。他のディスクについては、BMR の動作は [クライアントのリストア準備 (Prepare to Restore Client)] ダイアログボックスの次の 2 つのオプションで制御します。

- [システムディスク/ボリュームのみをリストアする (Restore system disks/volumes only)]
  - AIX および HP-UX では、ルートボリュームグループ (rootvg および vg00) がリストアされます。
  - Solaris では、ルートファイルシステム (/、/swap、/var、/usr) を含むすべてのディスクがリストアされます。
  - Windows では、%SystemRoot%、%SystemBoot% および %TEMP% を搭載したすべてのディスクがリストアされます。Active Directory サーバーでは、Active Directory システム、データベースおよびログファイルを格納するディスクもリストアされます。
  - Windows では、/、usr/、/usr/local、/var、/opt、/tmp、および /boot を搭載したすべてのディスクがリストアされます。
- [システムのリストア後に、リストアされていないディスク上のボリュームを利用可能にする (Make available volumes on non-restored disks after the system is restored)]  
このオプションを選択すると、BMR はディスクをインポートします。このオプションを選択しない場合の操作は、リストア準備オプションを実行するディスククラスによって異なります。

次に、ディスククラスを示します。

- システムディスクには、システムのブートに必要なオペレーティングシステムファイルが含まれています。
- システムディスク以外のディスクとは、次のような他のすべてのディスクです。
  - リストア可能ディスクは、一時的なリストア環境で可視であるため、リストア可能です。
  - リストア不可ディスクは、一時的なリストア環境で可視でないため、リストアできません。通常、これらは SAN デバイスです。リストアを試行するまで、これらのディスクがリストア可能かどうかは不明です。これらのディスクのリストアが必要な場合は、Dissimilar Disk Restore (DDR) を強制的に実行します。
  - 共有ディスクは、クラスタソフトウェアを使用して別のシステムと共有されています。リストア時またはリストア後にクライアントから制御できない場合があります。
  - 不明ディスクは、使用されていなかった場合もありますが、すでにシステムから接続解除されているディスクです。これらのディスクはリストア構成に含まれます。不明ディスクに対して実行する処理に関する詳細情報が利用可能です。  
p.90 の「リストア準備オプションによる BMR のディスククラスの処理」を参照してください。

- 新しいディスクは、システムで使用されていない場所に接続され、任意のボリュームまたはボリュームグループによって使用されます。新しいディスクは元の構成に含まれていません。

BMR はリストア時に処理されないように一部のディスクを制限します。たとえば、クラスタ内の共有ディスクや Solaris システム上の未使用の VxVM ディスクが制限されます。また、BMR によって処理されないように、ユーザーがディスクを手動で制限することもできます。

## リストア準備オプションによる BMR のディスクの処理

表 6-2 に、2 つのリストア準備オプションに応じた BMR のディスクの処理方法を示します。

リストアオプションの列については、次の点に注意してください。

- [システムのみ (System Only)] はリストア準備の [システムディスク/ボリュームのみをリストアする (Restore system disks/volumes only)] オプションです。
- [インポート (Import)] はリストア準備の [システムのリストア後に、リストアされていないディスク上のボリュームを利用可能にする (Make available volumes on non-restored disks after the system is restored)] オプションです。

表 6-2 BMR のディスク処理

リストアオプション	システムディスク	システムディスク以外のディスク 制限 = false	システムディスク以外のディスク 制限 = true
システムのみ = true および インポート = true	リストア (Restore)	インポート	処理なし
システムのみ = true および インポート = false	リストア (Restore)	処理なし	処理なし
システムのみ = false および インポート = true	リストア (Restore)	可能な場合はリストア、 可能でない場合はインポート	処理なし
システムのみ = false および インポート = false	リストア (Restore)	リストア (Restore)	処理なし

## リストア準備オプションによる BMR のディスククラスの処理

表 6-3 に、BMR がシステムディスクに実行する処理を示します。

表 6-4 に、BMR がシステムディスク以外のディスクに対して実行する処理およびユーザーが実行する必要がある操作を示します。

表の[リストアオプション (Restore options)]の列については、次の点に注意してください。

- [システムのみ (System Only)]はリストア準備の [システムディスク/ボリュームのみをリストアする (Restore system disks/volumes only)]オプションです。
- [インポート (Import)]はリストア準備の [システムのリストア後に、リストアされていないディスク上のボリュームを利用可能にする (Make available volumes on non-restored disks after the system is restored)]オプションです。

リストア時に残りの共有ディスクの使用に対して、クラスタノード間で競合が発生する場合があります。これを回避するには、共有ディスクを制限したままにするか、マッピングを解除するか、共有されていないリストア可能な別の場所に再マッピングする必要があります。リストア時に他のクラスタノードがディスクを共有していない場合にも、共有ディスクを制限なしで所定の場所にリストアします。

表 6-3 システムディスクの処理

リストアオプション	処理
システムのみ = true およびインポート = true	リストア (Restore)
システムのみ = true およびインポート = false	リストア (Restore)
システムのみ = false およびインポート = true	リストア (Restore)
システムのみ = false およびインポート = false	リストア (Restore)

表 6-4 システムディスク以外のディスクの処理

リストアオプション	リストア可能	リストア不可	共有	不明	新規
システムのみ = true およびインポート = true	インポート	インポート	処理なし	ディスクを制限ありとマークするか、リストア可能なディスクに再マッピングするか、リストア構成からディスクを削除します。	インポートされない
システムのみ = true およびインポート = false	処理なし	処理なし	処理なし	処理なし	処理なし
システムのみ = false およびインポート = true	リストア (Restore)	インポート	処理なし	ディスクを制限ありとマークするか、リストア可能なディスクに再マッピングするか、リストア構成からディスクを削除します。	インポートされない

リストアオプション	リストア可能	リストア不可	共有	不明	新規
システムのみ = false およびインポート = false	リストア (Restore)	リストア構成からディスクを削除するか、ディスクを制限ありとマークします。	処理なし	ディスクを制限ありとマークするか、リストア可能なディスクに再マッピングするか、リストア構成からディスクを削除します。	処理なし

## オペレーティングシステムまたは Volume Manager のインポート処理

表 6-5に、各オペレーティングシステムまたは Volume Manager のインポート処理を示します。

インポート処理について、次の点に注意してください。

- HP-UX Logical Volume Manager は自動仮想インポートです。HP システムでは、VxVM 管理ルートディスクおよび LVM 管理ディスクを使用できます。システムのためのリストアでは、LVM データベース (/etc/lvmtab ファイル) がリストアされます。これらのディスクおよびボリュームは、BMR による処理を必要とせずに使用できます。ファイルシステムの /etc/fstab ファイルにエントリが残っている場合は、そのファイルシステムを使用できます。
- Solaris システムまたは VxVM での結合時に、BMR は /etc/fstab ファイルまたは /etc/vfstab ファイルのエントリをコメント化して削除する場合があります。
- Veritas Volume Manager は自動インポートです。VxVM にはディスクグループを自動的にインポートする機能 (ディスクグループオプション) があります。/etc/fstab および /etc/vfstab ファイルにエントリがある場合は、BMR による処理を必要とせずにファイルシステムを使用できます。
- Windows インポートの場合は、次の点に注意してください。
  - インポートしない場合は、再作成されたドライブ文字のみがリストア後に割り当てられます。
  - インポートする場合は、信頼できるディスク上のボリュームに割り当てられたドライブ文字が、リストア後に同じ場所に割り当てられます。ボリュームが存在しないか、移動された場合は、MountedDevices レジストリキーを編集する必要があります。

表 6-5 インポート処理

OS および Volume Manager	インポートの意味
AIX Logical Volume Manager	リストア時または初回ブート時に importvg を実行する

OS および Volume Manager	インポートの意味
HP-UX Logical Volume Manager	lvmtab を結合して、fstab を結合する
Linux	fstab を結合する
Solaris	vfstab を結合する
Veritas Storage Foundation for Windows	MountedDevices を使用してドライブ文字を割り当て、vxdg インポートを実行する
Veritas Volume Manager	vxdg のインポートを実行し、fstab を結合する
Windows の場合	MountedDevices を使用してドライブ文字を割り当てる

## ネットワークブートによる BMR クライアントのリストアについて

**メモ:** Linux、Windows、Solaris、AIX、および HP-UX 環境のサポート対象マスター、ブートサーバー、クライアント、および SRT バージョンについて詳しくは、BMR の安全な通信互換性の表を確認してください。p.265 の「[NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換性の表](#)」を参照してください。

標準リストア (セルフリストアとも言い、同じシステムおよびディスクにリストアする) では、次に示す手順を実行します。

**メモ:** NetBackup がアクセス制御を使っている環境では、NetBackup がクライアントファイルをリストアするときに適切なクレデンシャルを入力するように求められます。BMR Windows クライアントまたは UNIX クライアントをリストアするには、クライアントをリストアする前にマスターサーバー上で `bpbmat -addmachine` を実行する必要があります。

追加されたマシンの名前を表示するには、マスターサーバー上で `bpbmat -ShowMachines` コマンドを使用します。

メディアブートを使用したリストアには、まずブートメディアの作成に関するセクションを参照してください。

標準リストアを行う前に、現在保存されている構成を使用して、リストア準備処理を実行する必要があります。p.86 の「[クライアントのリストアを準備する方法](#)」を参照してください。

- クライアントシステムをリストアする手順は、製造元およびモデルによって異なります。
- p.94 の「ネットワークブートによる AIX クライアントのリストア」を参照してください。
  - p.103 の「ネットワークブートによる Solaris クライアントのリストア」を参照してください。
  - p.98 の「ネットワークブートによる HP-UX クライアントのリストア」を参照してください。
  - p.101 の「ネットワークブートによる Linux クライアントのリストア」を参照してください。
  - p.105 の「ネットワークブートによる Windows クライアントのリストア」を参照してください。
- クライアントのリストアに関するその他の情報が利用可能です。
- p.138 の「外部プロシージャについて」を参照してください。
  - p.26 の「完全バックアップの実行について」を参照してください。
  - p.26 の「リストア後の完全バックアップの実行について」を参照してください。
  - p.26 の「正常なバックアップの保障」を参照してください。

## ネットワークブートによる AIX クライアントのリストア

---

**メモ:** Linux、Windows、Solaris、AIX、および HP-UX 環境のサポート対象マスター、ブートサーバー、クライアント、および SRT バージョンについて詳しくは、BMR の安全な通信互換性の表を確認してください。p.265 の「NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換性の表」を参照してください。

---

**メモ:** NetBackup アクセス制御管理が使用されている環境では、NetBackup がクライアントファイルをリストアするときに適切なクレデンシャルを入力するように求められます。

---

AIX ブート (ネットワークブートまたはメディアブート) では、ネットワークインターフェース構成、速度、二重モードを、自動ネゴシエーションまたは 10 M 半二重に設定できます。この設定により、BMR のリストアが非常に低速になることがあります。通常のリストアのパフォーマンスを実現するには、BMR のリストア前に、ネットワークインターフェース構成をファームウェア上から手動で設定します。

AIX システムのリストアには、特定の情報およびリソースが必要です。

ファームウェアで構成される情報はアーキテクチャによって異なりますが、次の情報が含まれます。

- ネットワークアダプタの種類
- **BMR** クライアント IP アドレス
- **BMR** クライアントサブネットマスク
- **BMR** ブートサーバー IP アドレス
- **BMR** クライアントゲートウェイアドレス

次のサンプル画面ショットでは、ネットワークブート時に **BMR** が自動的にリストアされるように、リストア先のハードウェアファームウェアで構成される必須のエンティティを示します。

図 6-3 サンプル AIX ファームウェアの設定

```
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 █
```

```
Version EL350_108
SMS 1.7 (c) Copyright IBM Corp. 2000,2008 All rights reserved.
-----
Network Parameters
Port 2 - IBM 4 PORT PCIe 10/100/1000 Base-TX Adapter: U789C.001.DQDN266-P1-C1-I2
1.  IP Parameters
2.  Adapter Configuration
3.  Ping Test
4.  Advanced Setup: BOOTP
-----
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.
-----
IP Parameters
PORT - 2 IBM Host Ethernet Adapter: U789C.001.DQDN266-P1-C7-I2
1.  Client IP Address          [000.000.000.000]
2.  Server IP Address         [000.000.000.000]
3.  Gateway IP Address        [000.000.000.000]
4.  Subnet Mask                [000.000.000.000]
-----
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: █
```

ネットワークブート手順を実行したら、残りのリストア処理は自動的に行われるため、手動の操作は必要ありません。リストアが終了し、クライアントが自動的に再ブートすると、完全にリストアされています。

AIX をインストール済みの AIX システムはネットワークブートできます。ネットワークブートでは、次の処理が行われます。

- BMR ブートサーバー、クライアントおよびゲートウェイの正しいアドレスで NVRAM が更新されます。
- BMR ブートサーバーから bootp によってブートされます。ブートサーバーが bootp 要求に応答しない場合、コンピュータはハードドライブからブートします。

ネットワークブートは、BMR クライアントが正しくリストア準備されている場合にのみ機能します。

---

**警告:** リストアする予定がない場合は、この手順を実行しないでください。リストアのためにクライアントを準備すると、最終的にリストアされる場合があります。

---

## ネットワークブートで AIX クライアントをリストアする方法

- 1 クライアントのリストアを準備します。

p.86 の「クライアントのリストアを準備する方法」を参照してください。

- 2 IBM のハードウェアマニュアルの手順に従って、ネットワークインターフェースからブートします。

リストアの準備中に設定された自動リカバリパラメータにより、リストア操作はホスト ID ベースの証明書の取得と、認証局 (CA) 証明書の検証を試行します。このリカバリは期限が定められています。リストア準備中の自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください。

---

**メモ:** リストア操作を中止する、またはリストア操作が失敗した場合は、リストア準備操作を再度実行して自動リカバリを再開するか、NetBackup Web UI を使用して [セキュリティ (Security)]、[ホストマッピング (Host mappings)]、[ホスト (Hosts)]、メニューボタン、[証明書の自動再発行を許可する (Allow auto reissue certificate)] オプションを手動で設定するか、コマンドラインインターフェースを使用して手動で設定します。

[証明書の自動再発行を許可する (Allow Auto Reissue Certificate)] オプションの手動設定について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「証明書の自動再発行の許可」を参照してください

[https://www.veritas.com/support/ja\\_JP/article.DOC5332](https://www.veritas.com/support/ja_JP/article.DOC5332)

---

リストアが開始されます。

リストアが正常に完了した後、リストアされたクライアント上でホスト ID ベースの証明書がコピーされます。自動リカバリパラメータがリセットされます。自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください

## ネットワークブートによる HP-UX クライアントのリストア

---

**メモ:** Linux、Windows、Solaris、AIX、および HP-UX 環境のサポート対象マスター、ブートサーバー、クライアント、および SRT バージョンについて詳しくは、BMR の安全な通信互換性の表を確認してください。p.265 の「NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換性の表」を参照してください。

---



---

**メモ:** NetBackup アクセス制御管理が使用されている環境では、NetBackup がクライアントファイルをリストアするときに適切なクレデンシャルを入力するように求められます。

---

HP-UX システムのリストアには、個別に詳細な情報およびリソースが必要です。  
 この情報はアーキテクチャによって異なりますが、次の情報が含まれます。

- BMR クライアント IP アドレス
- BMR クライアントゲートウェイアドレス
- BMR クライアントサブネットマスク
- Ignite サーバーアドレス (通常、BMR ブートサーバー)

ネットワークブート手順を実行したら、残りのリストア処理は自動的に行われるため、手動の操作は必要ありません。リストアが終了し、クライアントが自動的に再ブートすると、完全にリストアされています。

#### ネットワークブートで HP-UX IA クライアントをリストアする方法

- 1 クライアントのリストアを準備します。  
 p.86 の「クライアントのリストアを準備する方法」を参照してください。
- 2 リストアするクライアントをブートします。

```

EFI Boot Manager ver 2.00 [14.62]
IS might use only the primary console set via boot manager or conconfig command

/-----\
|          Boot Menu          |
| HP-UX Primary Boot: 0/1/1/0... |
| iLO Virtual Media          |
| Core LAN A                  |
| Core LAN B                  |
| EFI Shell [Built-in]       |
| Internal Bootable DVD      |
|-----|
| Boot Configuration         |
| System Configuration      |
| Security Configuration    |
|-----|
\-----/

/-----\
|          System Overview          |
| hp server rx2660                  |
| Serial #: SGH474905V              |
|-----|
| System Firmware: 4.11 [4842]     |
| BMC Version: 5.25                 |
| MP Version: F.02.23               |
| Installed Memory: 2048 MB        |
|-----|
|          CPU Logical              |
| Module CPUs  Speed  Status      |
| 0    4    1.4 GHz  Active       |
|-----|
\-----/

Use <^|v> to scroll  <ENTER> to Select  <ESC> or <X/x> for Previous Menu
    
```

- 3 クライアントがワークステーションの場合は、オペレーティングシステムの言語を番号で選択します。たとえば、US 英語は 61 です。
- 4 言語の選択を入力したら、Enter キーを 2 回押して選択し、選択を確認します。HP-UX Ignite メニューが表示されます。
- 5 矢印キーを使用して、[Run a Recovery Shell]までスクロールします。DHCP 検索が実行され、[ネットワーク構成 (Network Configuration)]メニューが開くまで、待機します。DHCP 検索を中断すると、BMR のリストアが失敗する場合があります。
- 6 次のプロンプトに応答します。
  - Hostname:
  - Internet Protocol Address:
  - Subnet mask:
  - Ignite Server Address (typically the BMR boot server):

- 7 矢印キーを使用して[OK]までスクロールし、Enter キーを押します。

システムがネットワークからブートします。

リストアの準備中に設定された自動リカバリパラメータにより、リストア操作はホスト ID ベースの証明書の取得と、認証局 (CA) 証明書の検証を試行します。このリカバリは期限が定められています。リストア準備中の自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください。

---

**メモ:** リストア操作を中止する、またはリストア操作が失敗した場合は、リストア準備操作を再度実行して自動リカバリを再開するか、NetBackup Web UI を使用して [セキュリティ (Security)]、[ホストマッピング (Host mappings)]、[ホスト (Hosts)]、メニューボタン、[証明書の自動再発行を許可する (Allow auto reissue certificate)] オプションを手動で設定するか、コマンドラインインターフェースを使用して手動で設定します。

[証明書の自動再発行を許可する (Allow Auto Reissue Certificate)] オプションの手動設定について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「証明書の自動再発行の許可」を参照してください。

[https://www.veritas.com/support/ja\\_JP/article.DOC5332](https://www.veritas.com/support/ja_JP/article.DOC5332)

---

- 8 リストアが開始されます。

リストアが正常に完了した後、リストアされたクライアント上でホスト ID ベースの証明書がコピーされます。自動リカバリパラメータがリセットされます。自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください。

## ネットワークブートによる Linux クライアントのリストア

---

**メモ:** Linux、Windows、Solaris、AIX、および HP-UX 環境のサポート対象マスター、ブートサーバー、クライアント、および SRT バージョンについて詳しくは、BMR の安全な通信互換性の表を確認してください。p.265 の「NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換性の表」を参照してください。

---

**メモ:** NetBackup アクセス制御管理が使用されている環境では、NetBackup がクライアントファイルのリストアするときに適切なクレデンシャルを入力するように求められます。

---

Linux クライアントをネットワークブートする場合、BMR には次が必要です。

- PXE

- DHCP
- TFTP
- NFS

Linux のネットワークブートに必要なすべての情報は、リストア準備処理時に収集されます。Linux クライアントのネットワークベースのリカバリでは、上記のサービスが BMR ブートサーバーで設定され、動作していることを確認する必要があります。これらのサービス構成ファイルで、クライアントの特定の設定をする必要があります。BMR はリストア準備中に、選択されたクライアントの必須ネットワークブートサービス構成を処理します。必須のネットワークサービス構成について詳しくは、

p.251 の「[BMR ブートサーバーに対するネットワークサービスの設定](#)」を参照してください。

リストア準備後、クライアントをブートしてリストアを開始します。

### Linux クライアントをネットワークブートする方法

- 1 クライアントのリストアを準備します。

p.86 の「[クライアントのリストアを準備する方法](#)」を参照してください。

- 2 BMR ブートサーバーで実行されているものを除き、他の DHCP サービスが同じサブネットで動作していないことを確認してください。そうでない場合、クライアント DHCP ブートの要求は、意図しない DHCP サーバーに送信され、PXE ネットワークブートが失敗する可能性があります。

---

**メモ:** これは、最初の DHCP 応答エラーによりネットワークブート処理が停止されてしまうという PXE と DHCP ブートプロトコルの制限事項です。このため、実行中のブートサーバーでは、Linux DHCP サービスのみを保持することを推奨します。

---

- 3 リストアするクライアントをブートします。

#### 4 ハードウェアベンダーの指示に従って、クライアントを PXE ブートします。

システムによっては、キーを押すことによって PXE ブートを開始できるという BIOS メッセージが表示されます。また、デフォルトのブート順序にネットワークカードが追加されるように、BIOS の設定を変更する必要がある場合もあります。詳しくは、ハードウェアのマニュアルを参照してください。

リストアの準備中に設定された自動リカバリパラメータにより、リストア操作はホスト ID ベースの証明書の取得と、認証局 (CA) 証明書の検証を試行します。このリカバリは期限が定められています。リストア準備中の自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください。

---

**メモ:** リストア操作を中止する、またはリストア操作が失敗した場合は、リストア準備操作を再度実行して自動リカバリを再開するか、NetBackup Web UI を使用して [セキュリティ (Security)]、[ホストマッピング (Host mappings)]、[ホスト (Hosts)]、メニューボタン、[証明書の自動再発行を許可する (Allow auto reissue certificate)] オプションを手動で設定するか、コマンドラインインターフェースを使用して手動で設定します。

[証明書の自動再発行を許可する (Allow Auto Reissue Certificate)] オプションの手動設定について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「証明書の自動再発行の許可」を参照してください

[https://www.veritas.com/support/ja\\_JP/article.DOC5332](https://www.veritas.com/support/ja_JP/article.DOC5332)

---

#### 5 プロンプトが表示されたら、Enter キーを押すか、またはシステムがブートするまで待機します。

システムがブートし、リストアが開始されます。ユーザーの操作は必要ありません。

#### 6 クライアントの正常なリカバリ後、BMR は自動的にリストア準備中に DHCP 構成のクライアントに追加されるネットワークブート設定をクリーンアップします。

リストアが正常に完了した後、リストアされたクライアント上でホスト ID ベースの証明書がコピーされます。自動リカバリパラメータがリセットされます。自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください

## ネットワークブートによる Solaris クライアントのリストア

---

**メモ:** Linux、Windows、Solaris、AIX、および HP-UX 環境のサポート対象マスター、ブートサーバー、クライアント、および SRT バージョンについて詳しくは、BMR の安全な通信互換性の表を確認してください。p.265 の「NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換性の表」を参照してください。

---

---

**メモ:** NetBackup アクセス制御管理が使用されている環境では、NetBackup がクライアントファイルをリストアするときに適切なクレデンシャルを入力するように求められます。

---

Solaris クライアントをネットワークブートする場合、BMR には次が必要です。

- PXE (Solaris-x64 プラットフォームベースのクライアントリカバリの場合)
- DHCP
- TFTP
- NFS

必須のネットワークサービス構成について詳しくは、

p.251 の「[BMR ブートサーバーに対するネットワークサービスの設定](#)」を参照してください。

Solaris システムのリストアには、クライアントに正しい BMR ブートサーバーを指示するネットワークデバイスの名前が必要です。

ネットワークブート手順を実行したら、残りのリストア処理は自動的に行われるため、手動の操作は必要ありません。リストアが終了し、クライアントが自動的に再ブートすると、完全にリストアされています。

### ネットワークブートで Solaris クライアントをリストアする方法

- 1 クライアントのリストアを準備します。  
p.86 の「[クライアントのリストアを準備する方法](#)」を参照してください。
- 2 BMR Solaris ブートサーバーで実行されているものを除き、他の DHCP サービスが同じサブネットで動作していないことを確認してください。そうでない場合、クライアント DHCP ブートの要求は、意図しない DHCP サーバーに送信され、ネットワークブートが失敗する可能性があります。

---

**メモ:** これは、最初の DHCP 応答エラーによりネットワークブート処理が停止してしまうという DHCP と PXE ブートプロトコルの制限事項です。このため、実行中のブートサーバーでは、Solaris DHCP サービスのみを保持することを推奨します。

---

- 3 リストアするクライアントをブートします。
- 4 `sc>` プロンプトに戻り、[OK]プロンプトを取得するために `sc>` プロンプトから `break` コマンドを送信し、`#.` コマンドを使用してブートプロセスを終了します。

5 次のコマンドを入力してネットワークブートを開始します

(net[id] is the device that points to the BMR boot server): boot net[id] の [id] は 1、2、3 のインターフェースカードです。

6 次のコマンドを入力してネットワークブートを開始します (**net[id]** は BMR ブートサーバーを指すデバイスです): boot net [id] (id は 1、2、3 のインターフェースカードです)。

リストアの準備中に設定された自動リカバリパラメータにより、リストア操作はホスト ID ベースの証明書の取得と、認証局 (CA) 証明書の検証を試行します。このリカバリは期限が定められています。リストア準備中の自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください。

---

**メモ:** リストア操作を中止する、またはリストア操作が失敗した場合は、リストア準備操作を再度実行して自動リカバリを再開するか、NetBackup Web UI を使用して [セキュリティ (Security)]、[ホストマッピング (Host mappings)]、[ホスト (Hosts)]、メニューボタン、[証明書の自動再発行を許可する (Allow auto reissue certificate)] オプションを手動で設定するか、コマンドラインインターフェースを使用して手動で設定します。

[証明書の自動再発行を許可する (Allow Auto Reissue Certificate)] オプションの手動設定について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「証明書の自動再発行の許可」を参照してください。

[https://www.veritas.com/support/ja\\_JP/article.DOC5332](https://www.veritas.com/support/ja_JP/article.DOC5332)

---

リストアが正常に完了した後、リストアされたクライアント上でホスト ID ベースの証明書がコピーされます。自動リカバリパラメータがリセットされます。自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください

## ネットワークブートによる Windows クライアントのリストア

---

**メモ:** Linux、Windows、Solaris、AIX、および HP-UX 環境のサポート対象マスター、ブートサーバー、クライアント、および SRT バージョンについて詳しくは、BMR の安全な通信互換性の表を確認してください。p.265 の「NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換性の表」を参照してください。

---

**メモ:** NetBackup アクセス制御管理が使用されている環境では、NetBackup がクライアントファイルのリストアするときに適切なクレデンシャルを入力するように求められます。

---

Windows システムのネットワークブートでは、PXE プロトコルを使用します。BMR ブートサーバーは PXE ネットワークサービスを提供および管理しますが、DHCP サービスを使用できる環境である必要があります。DHCP サービスは同じブートサーバーにまたはサブネットのあらゆる場所に存在できます。

### ネットワークブートで Windows クライアントをリストアする方法

- 1 クライアントのリストアを準備します。  
p.86 の「[クライアントのリストアを準備する方法](#)」を参照してください。
- 2 BMR ブートサーバーで PXE および TFTP サービス構成が 1 度行われることを確認してください。

BMR PXE 構成がブートサーバーで行われていない場合、Windows BMR ブートサーバーの[スタート]メニューにある、[BMR Boot server assistant]で利用可能な PXE サービスの構成ウィザードを実行してください。

このためには、[プログラム]、NetBackup Web UI、[Windows]、[Veritas NetBackup]、[BMR Boot Server Assistant]の順に選択します。この BMR PXE サービス設定は Windows ブートサーバーで 1 回のみ実行する必要があります。DHCPサーバーの場所を後から変更する場合、このウィザードを再度実行する必要があります。

---

**メモ:** 同じ BMR ブートサーバーで実行中の他の非 BMR PXE または TFTP サービスは、BMRリカバリで使うことができません。クライアントネットワークがリカバリのためにブートする間、これらのサービスは必ず停止してください。そうでない場合、クライアント PXE ブートの要求は、意図しないサーバーに送信され、PXE ネットワークブートが失敗する可能性があります。これは PXE、DHCP ブートプロトコルの制限事項であり、ネットワークベースのリカバリでクライアントをブートしている間、Cohesity は正しい PXE、DHCP、TFTP サーバーのみを実行し続けることをお勧めします。

---

- 3 BMR PXE および TFTP サービスが起動し、実行中であることを確かめてください。
- 4 リストアするクライアントをブートします。

- 5 ハードウェアベンダーの指示に従って、クライアントを PXE ブートします。システムによっては、キーを押すことによって PXE ブートを開始できるという BIOS メッセージが表示されます。また、デフォルトのブート順序にネットワークカードが追加されるように、BIOS の設定を変更する必要がある場合もあります。詳しくは、ハードウェアのマニュアルを参照してください。

リストアの準備中に設定された自動リカバリパラメータにより、リストア操作はホスト ID ベースの証明書の取得と、認証局 (CA) 証明書の検証を試行します。このリカバリは期限が定められています。リストア準備中の自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください。

---

**メモ:** リストア操作を中止する、またはリストア操作が失敗した場合は、リストア準備操作を再度実行して自動リカバリを再開するか、NetBackup Web UI を使用して [セキュリティ (Security)]、[ホストマッピング (Host mappings)]、[ホスト (Hosts)]、メニューボタン、[証明書の自動再発行を許可する (Allow auto reissue certificate)] オプションを手動で設定するか、コマンドラインインターフェースを使用して手動で設定します。

[証明書の自動再発行を許可する (Allow Auto Reissue Certificate)] オプションの手動設定について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「証明書の自動再発行の許可」を参照してください

[https://www.veritas.com/support/ja\\_JP/article.DOC5332](https://www.veritas.com/support/ja_JP/article.DOC5332)

---

- 6 メッセージが表示されたら、F12 キーを押してシステムをブートし、リストアを開始します。

リストアが正常に完了した後、リストアされたクライアント上でホスト ID ベースの証明書がコピーされます。自動リカバリパラメータがリセットされます。自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください

## メディアブートによる BMR クライアントのリストアについて

---

**メモ:** Linux、Windows、Solaris、AIX、および HP-UX 環境のサポート対象マスター、ブートサーバー、クライアント、および SRT バージョンの詳細については、BMR の安全な通信互換性の表を確認してください。p.265 の「NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換性の表」を参照してください。

---

標準リストア (セルフリストアとも言い、同じシステムおよびディスクにリストアする) では、次に示す手順を実行します。

- |  |   |
|--|---|
| メディアブートを使用したリストアには、まずブートメディアを作成する必要があります。          | ブートメディアの作成に関するセクションを参照してください。   |
| 標準リストアを行う前に、現在保存されている構成を使用して、リストア準備処理を実行する必要があります。 | p.86 の「 <a href="#">クライアントのリストアを準備する方法</a> 」を参照してください。  |
| クライアントシステムをリストアする手順は、製造元およびモデルによって異なります。           | p.109 の「 <a href="#">メディアブートによる AIX クライアントのリストア</a> 」を参照してください。<br>p.110 の「 <a href="#">メディアブートによる HP-UX クライアントのリストア</a> 」を参照してください。<br>p.112 の「 <a href="#">メディアブートによる Linux クライアントのリストア</a> 」を参照してください。<br>p.114 の「 <a href="#">メディアブートによる Solaris クライアントのリストア</a> 」を参照してください。<br>p.116 の「 <a href="#">メディアブートによる Windows クライアントのリストア</a> 」を参照してください。 |
| クライアントのリストアに関するその他の情報が利用可能です。                      | p.138 の「 <a href="#">外部プロシージャについて</a> 」を参照してください。<br>p.26 の「 <a href="#">完全バックアップの実行について</a> 」を参照してください。<br>p.26 の「 <a href="#">リストア後の完全バックアップの実行について</a> 」を参照してください。<br>p.26 の「 <a href="#">正常なバックアップの保障</a> 」を参照してください。   |

## メディアブートによる AIX クライアントのリストア

---

**メモ:** Linux、Windows、Solaris、AIX、および HP-UX 環境のサポート対象マスター、ブートサーバー、クライアント、および SRT バージョンについて詳しくは、BMR の安全な通信互換性の表を確認してください。p.265 の「[NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換性の表](#)」を参照してください。

---

**メモ:** NetBackup アクセス管理を使っている環境では、NetBackup がクライアントファイルのリストアできるように適切なクレデンシャルを入力するように求められます。

---

AIX ブート (ネットワークブートまたはメディアブート) では、ネットワークインターフェース構成、速度、二重モードを、自動ネゴシエーションまたは 10 M 半二重に設定できます。この設定により、BMR のリストアが非常に低速になることがあります。通常のリストアのパフォーマンスを実現するには、BMR のリストア前に、ネットワークインターフェース構成をファームウェア上から手動で設定します。

### メディアブートで AIX クライアントをリストアする方法

- 1 ブートメディア上に作成した SRT を使用して、クライアントのリストアを準備します。  
p.86 の「[クライアントのリストアを準備する方法](#)」を参照してください。
- 2 作成したブートメディアからクライアントをブートします。CD または DVD からのブート手順については、IBM のハードウェアマニュアルを参照してください。
- 3 BMR の処理の次のプロンプトで必要な情報を入力します。
  - Client name (検出ブートの場合は、検出準備処理の[タスク (Tasks)]ビューに表示されているクライアント名を入力します)
  - Client IP address
  - Network mask
  - Default gateway
  - NetBackup master server name
  - NetBackup master server IP address
  - NetBackup master server gateway IP address

リストアの準備中に設定された自動リカバリパラメータにより、リストア操作はホスト ID ベースの証明書の取得と、認証局 (CA) 証明書の検証を試行します。このリカバリは期限が定められています。リストア準備中の自動リカバリについて詳しくは、「[p.86 の「クライアントのリストアを準備する方法](#)」を参照してください。」を参照してください

リストアが開始されます。

---

**メモ:** リストア操作を中止する、またはリストア操作が失敗した場合は、リストア準備操作を再度実行して自動リカバリを再開するか、NetBackup Web UI を使用して [セキュリティ (Security)]、[ホストマッピング (Host mappings)]、[ホスト (Hosts)]、メニューボタン、[証明書の自動再発行を許可する (Allow auto reissue certificate)] オプションを手動で設定するか、コマンドラインインターフェースを使用して手動で設定します。

[証明書の自動再発行を許可する (Allow Auto Reissue Certificate)] オプションの手動設定について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「証明書の自動再発行の許可」を参照してください

[https://www.veritas.com/support/ja\\_JP/article.DOC5332](https://www.veritas.com/support/ja_JP/article.DOC5332)

---

リストアが正常に完了した後、リストアされたクライアント上でホスト ID ベースの証明書がコピーされます。自動リカバリパラメータがリセットされます。自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください。

## メディアブートによる HP-UX クライアントのリストア

---

**メモ:** Linux、Windows、Solaris、AIX、および HP-UX 環境のサポート対象マスター、ブートサーバー、クライアント、および SRT バージョンについて詳しくは、BMR の安全な通信互換性の表を確認してください。p.265 の「NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換性の表」を参照してください。

---

**メモ:** NetBackup アクセス管理を使っている環境では、NetBackup がクライアントファイルのリストアできるように適切なクレデンシャルを入力するように求められます。

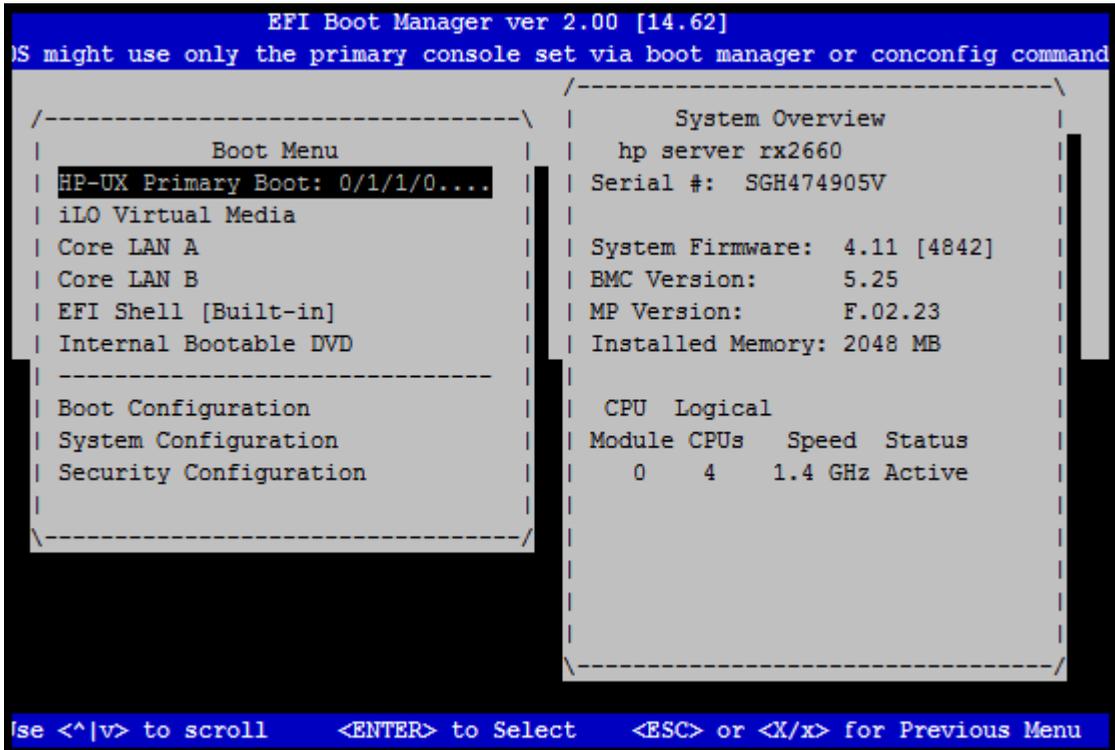
---

HP-UX クライアントをメディアブートするには、次の手順を実行します。

### メディアブートで HP-UX IA クライアントをリストアする方法

- 1 ブートメディア上に作成した SRT を使用して、クライアントのリストアを準備します。  
p.86 の「クライアントのリストアを準備する方法」を参照してください。
- 2 ブート可能 CD またはブート可能 DVD を CD-ROM ドライブに挿入します。

- 3 リストアするクライアントをブートします。



- 4 Run a Recovery Shell プロンプトに対して Yes と入力します。
- 5 Start Networking プロンプトに対して Yes と入力します。
- 6 Choose the Network Interface プロンプトに対して、ブートするデフォルトの LAN デバイスを入力します。  
 ファームウェアが Ignite サーバーからのブートにデフォルトの LAN のアドレスを使用するため、デフォルトの LAN を入力する必要があります。SRT またはバックアップへのアクセスには任意のネットワークインターフェースカードを使用できますが、ブートにはデフォルトの LAN を使用する必要があることに注意してください。
- 7 入力が必要であれば、次の情報を入力します。
  - Hostname
  - IP address
  - Default gateway
  - Subnet mask

- 8 Is this network information temporary プロンプトで No と入力します。
- 9 矢印キーを使用して OK までスクロールし、Enter キーを押します。
- 10 BMR の処理の次のプロンプトで必要な情報を入力します。
  - Client name (検出ブートの場合は、検出準備処理の[タスク (Tasks)]ビューに表示されているクライアント名を入力します)
  - NetBackup master server name
  - NetBackup master server IP address
  - NetBackup master server gateway IP address

リストアの準備中に設定された自動リカバリパラメータにより、リストア操作はホスト ID ベースの証明書の取得と、認証局 (CA) 証明書の検証を試行します。このリカバリは期限が定められています。リストア準備中の自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください

リストアが開始されます。

---

**メモ:** リストア操作を中止する、またはリストア操作が失敗した場合は、リストア準備操作を再度実行して自動リカバリを再開するか、NetBackup Web UI を使用して [セキュリティ (Security)]、[ホストマッピング (Host mappings)]、[ホスト (Hosts)]、メニューボタン、[証明書の自動再発行を許可する (Allow auto reissue certificate)] オプションを手動で設定するか、コマンドラインインターフェースを使用して手動で設定します。

[証明書の自動再発行を許可する (Allow Auto Reissue Certificate)] オプションの手動設定について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「証明書の自動再発行の許可」を参照してください

[https://www.veritas.com/support/ja\\_JP/article.DOC5332](https://www.veritas.com/support/ja_JP/article.DOC5332)

---

リストアが正常に完了した後、リストアされたクライアント上でホスト ID ベースの証明書がコピーされます。自動リカバリパラメータがリセットされます。自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください。

## メディアブートによる Linux クライアントのリストア

---

**メモ:** Linux、Windows、Solaris、AIX、および HP-UX 環境のサポート対象マスター、ブートサーバー、クライアント、および SRT バージョンについて詳しくは、BMR の安全な通信互換性の表を確認してください。p.265 の「NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換性の表」を参照してください。

---

---

**メモ:** NetBackup アクセス管理を使っている環境では、NetBackup がクライアントファイルをリストアできるように適切なクレデンシャルを入力するように求められます。

---

Linux クライアントに対して次の手順を実行します。

#### メディアブートで Linux クライアントをリストアする方法

- 1 ブートメディア上に作成した SRT を使用して、クライアントのリストアを準備します。  
 p.86 の「[クライアントのリストアを準備する方法](#)」を参照してください。
- 2 ブート可能 CD またはブート可能 DVD を CD-ROM ドライブに挿入します。  
 システムによっては、CD-ROM ドライブからシステムがブートするように、BIOS の設定を変更する必要がある場合があります。詳しくは、ハードウェアのマニュアルを参照してください。
- 3 リストアするクライアントをブートします。
- 4 BMR の処理の次のプロンプトに必要な情報を入力します。
  - Client name (検出ブートの場合は、検出準備処理の[タスク (Tasks)]ビューに表示されているクライアント名を入力します)
  - 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

リストアの準備中に設定された自動リカバリパラメータにより、リストア操作はホスト ID ベースの証明書の取得と、認証局 (CA) 証明書の検証を試行します。このリカバリは期限が定められています。リストア準備中の自動リカバリについて詳しくは、「[p.86 の「クライアントのリストアを準備する方法](#)」を参照してください。」を参照してください

リストアが開始されます。

---

**メモ:** リストア操作を中止する、またはリストア操作が失敗した場合は、リストア準備操作を再度実行して自動リカバリを再開するか、NetBackup Web UI を使用して [セキュリティ (Security)]、[ホストマッピング (Host mappings)]、[ホスト (Hosts)]、メニューボタン、[証明書の自動再発行を許可する (Allow auto reissue certificate)] オプションを手動で設定するか、コマンドラインインターフェースを使用して手動で設定します。

[証明書の自動再発行を許可する (Allow Auto Reissue Certificate)] オプションの手動設定について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「証明書の自動再発行の許可」を参照してください

[https://www.veritas.com/support/ja\\_JP/article.DOC5332](https://www.veritas.com/support/ja_JP/article.DOC5332)

---

リストアが正常に完了した後、リストアされたクライアント上でホスト ID ベースの証明書がコピーされます。自動リカバリパラメータがリセットされます。自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください。

## メディアブートによる Solaris クライアントのリストア

---

**メモ:** Linux、Windows、Solaris、AIX、および HP-UX 環境のサポート対象マスター、ブートサーバー、クライアント、および SRT バージョンについて詳しくは、BMR の安全な通信互換性の表を確認してください。p.265 の「NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換性の表」を参照してください。

---

**メモ:** NetBackup アクセス管理を使っている環境では、NetBackup がクライアントファイルのリストアできるように適切なクレデンシャルを入力するように求められます。

---

Solaris クライアントに対して次の手順を実行します。

### メディアブートで Solaris クライアントをリストアする方法

- 1 ブートメディア上に作成した SRT を使用して、クライアントのリストアを準備します。  
p.86 の「クライアントのリストアを準備する方法」を参照してください。
- 2 ブート可能 CD またはブート可能 DVD を CD-ROM ドライブに挿入します。
- 3 リストアするクライアントをブートします。
- 4 ブートプロセスを終了します。これには、# コマンドを押して `sc>` プロンプトに戻り、`sc>` プロンプトから `break` コマンドを送信して [OK] プロンプトを取得します。

5 次のコマンドを入力します。

```
boot cdrom
```

Solaris OS インストールにより、ネットワーク ID の入力が必要になります。

6 ネットワーク ID を入力します。

7 BMR の処理の次のプロンプトで必要な情報を入力します。

- Client name (検出ブートの場合は、検出準備処理の[タスク (Tasks)]ビューに表示されているクライアント名を入力します)
- NetBackup master server name
- NetBackup master server IP address
- NetBackup master server gateway IP address

リストアの準備中に設定された自動リカバリパラメータにより、リストア操作はホスト ID ベースの証明書の取得と、認証局 (CA) 証明書の検証を試行します。このリカバリは期限が定められています。リストア準備中の自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください

必要な情報を入力すると、リストアが開始されます。

---

**メモ:** リストア操作を中止する、またはリストア操作が失敗した場合は、リストア準備操作を再度実行して自動リカバリを再開するか、NetBackup Web UI を使用して [セキュリティ (Security)]、[ホストマッピング (Host mappings)]、[ホスト (Hosts)]、メニューボタン、[証明書の自動再発行を許可する (Allow auto reissue certificate)] オプションを手動で設定するか、コマンドラインインターフェースを使用して手動で設定します。

[証明書の自動再発行を許可する (Allow Auto Reissue Certificate)] オプションの手動設定について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「証明書の自動再発行の許可」を参照してください

[https://www.veritas.com/support/ja\\_JP/article.DOC5332](https://www.veritas.com/support/ja_JP/article.DOC5332)

---

リストアが正常に完了した後、リストアされたクライアント上でホスト ID ベースの証明書がコピーされます。自動リカバリパラメータがリセットされます。自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください。

## メディアブートによる Windows クライアントのリストア

---

**メモ:** Linux、Windows、Solaris、AIX、および HP-UX 環境のサポート対象マスター、ブートサーバー、クライアント、および SRT バージョンについて詳しくは、BMR の安全な通信互換性の表を確認してください。p.265 の「[NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換性の表](#)」を参照してください。

---

**メモ:** NetBackup アクセス管理を使っている環境では、NetBackup がクライアントファイルのリストアできるように適切なクレデンシャルを入力するように求められます。BMR Windows クライアントをリストアするには、クライアントをリストアする前にマスターサーバーの `bpnbat -addmachine` を実行する必要があります。

追加されたマシンの名前を表示するには、マスターサーバー上で `bpnbat -ShowMachines` コマンドを使用します。

---

Windows クライアントをメディアブートするには、次の手順を実行します。

### メディアブートで Windows クライアントをリストアする方法

- 1 クライアントのリストアを準備します。  
p.86 の「[クライアントのリストアを準備する方法](#)」を参照してください。
- 2 リストア準備時に使用した SRT からブート可能 CD/DVD を作成します。

### 3 ブート可能 CD/DVD を CD-ROM/DVD-ROM ドライブに挿入します。

システムによっては、CD-ROM ドライブからシステムがブートするように、BIOS の設定を変更する必要がある場合があります。詳しくは、ハードウェアのマニュアルを参照してください。

リストアの準備中に設定された自動リカバリパラメータにより、リストア操作はホスト ID ベースの証明書の取得と、認証局 (CA) 証明書の検証を試行します。このリカバリは期限が定められています。リストア準備中の自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください。

---

**メモ:** リストア操作を中止する、またはリストア操作が失敗した場合は、リストア準備操作を再度実行して自動リカバリを再開するか、NetBackup Web UI を使用して [セキュリティ (Security)]、[ホストマッピング (Host mappings)]、[ホスト (Hosts)]、メニューボタン、[証明書の自動再発行を許可する (Allow auto reissue certificate)] オプションを手動で設定するか、コマンドラインインターフェースを使用して手動で設定します。

[証明書の自動再発行を許可する (Allow Auto Reissue Certificate)] オプションの手動設定について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「証明書の自動再発行の許可」を参照してください

[https://www.veritas.com/support/ja\\_JP/article.DOC5332](https://www.veritas.com/support/ja_JP/article.DOC5332)

---

### 4 リストアするクライアントをブートします。

次のメッセージが表示されます。

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

### 5 システムがブートし、リストアが開始されます。操作は必要ありません。

リストアが正常に完了した後、リストアされたクライアント上でホスト ID ベースの証明書がコピーされます。自動リカバリパラメータがリセットされます。自動リカバリについて詳しくは、「p.86 の「クライアントのリストアを準備する方法」を参照してください。」を参照してください。

## 汎用的な BMR リストア

NetBackup Bare Metal Restore (BMR) は、リストア準備 (PTR) 操作を実行せずに Windows クライアントをリストアする機能を備えています。この機能は、汎用的な BMR リストアと呼ばれます。

### 汎用的な BMR を使用して Windows クライアントをリストアする方法

- 1 Windows SRT を使用してクライアントをブートします。図に示すように、表示される画面で Windows SRT を使用してクライアントをブートした後、任意のキーを押して Veritas System Recovery Disk ウィザードに移動します。
- 2 Veritas System Recovery Disk ウィザードで、[汎用的な BMR リストア (Generic BMR Restore)]をクリックします。
- 3 図に示すように、表示される画面で以下のネットワークの詳細を入力します。

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

次に、[マスターサーバーに接続する (Contact Master Server)]をクリックします。

- 4 クライアントが通信を確立しようとしている、選択したプライマリサーバーが、信頼できるサーバーであるかどうかを検証して確認する必要があります。

プライマリサーバーが信頼できる場合は、[はい (Yes)]をクリックします。

認証局 (CA) のハッシュ証明書の検証方法については、『*NetBackup セキュリティおよび暗号化ガイド*』の「*CA 証明書の指紋の検索と通信*」を参照してください。

<http://www.veritas.com/docs/DOC5332>

- 5 [再発行 (Reissue)]トークンを入力し、[OK]をクリックします。

NetBackup Web UI の[証明書管理 (Certificate Management)]ノードを使用してトークンを生成します (左側の[ホストマッピング (Host mappings)]、[ホスト (Hosts)]、メニューボタン、[再発行トークンの生成 (Generate reissue token)]の順に選択)。

再発行タイプの認証トークンを生成する方法については、NetBackup Web UI のヘルプまたは『*NetBackup セキュリティおよび暗号化ガイド*』の「再発行トークンの作成」を参照してください。

[https://www.veritas.com/support/en\\_US/article.DOC5332](https://www.veritas.com/support/en_US/article.DOC5332)

- 6 クライアント構成ドロップダウンリストで、リストアするクライアント構成を選択して[クライアントのリストア (Restore Client)]をクリックします。

---

**メモ:** このリストに、指定した再発行トークンが関連付けられている特定クライアントのみの構成が表示されます。

再発行トークンを指定したクライアントに関連付けられているすべての構成のリストを表示する場合は、[すべての構成を表示する (Show all configurations)]を選択します。

---

- 7 リストアが始まります。これ以上ユーザーが操作する必要はありません。
- 8 リストアが正常に完了した後、リストアされたクライアント上でホスト ID ベースの証明書がコピーされます。

## ハードウェアの汎用的な検出

NetBackup Bare Metal Restore (BMR) は、検出準備 (PTD) 操作を実行せずに Windows クライアントを検出する機能を備えています。この機能は、ハードウェアの汎用的な検出と呼ばれます。

### 汎用的な検出を使用して Windows クライアントを検出する方法

- 1 Windows SRT を使用してクライアントをブートします。図に示すように、表示される画面で Windows SRT を使用してクライアントをブートした後、任意のキーを押して Veritas System Recovery Disk ウィザードに移動します。
- 2 Veritas System Recovery Disk ウィザードで、[ハードウェアの汎用的な検出 (Generic Discovery of Hardware)]をクリックします。
- 3 構成の詳細を指定します。  
(省略可能) 検出した構成をローカルシステム上に保存する場合は、[検出された構成をローカルに保存する (Save a discovered configuration locally)]チェックボックスを選択します。検出済みの構成を XML 形式で保存します。
- 4 [検出を実行 (Do Discover)]をクリックします。  
[検出された構成をローカルに保存する (Save a discovered configuration locally)]チェックボックスを選択し、[検出を実行 (Do Discover)]をクリックすると、検出はさらにユーザーが操作する必要なく続行します。
- 5 [検出された構成をローカルに保存する (Save a discovered configuration locally)]チェックボックスを選択せずに[検出を実行 (Do Discover)]をクリックすると、表示される画面に、次のネットワーク詳細を入力する必要があります。

- IP Address

- Netmask
  - Gateway
  - NetBackup master server IP address
  - NetBackup master server name
- 6 手順 5 に示されているすべての詳細を入力したら、[マスターサーバーに接続する (Contact Master Server)]をクリックします。
- 7 (手順 5 と手順 6 で該当する場合) クライアントが通信を確立しようとしている、選択したプライマリサーバーが、信頼できるサーバーであるかどうかを検証して確認する必要があります。
- プライマリサーバーが信頼できる場合は、[はい (Yes)]をクリックします。
- 認証局 (CA) のハッシュ証明書の検証方法について詳しくは、『*NetBackup セキュリティおよび暗号化ガイド*』の「*CA 証明書の指紋の検索と通信*」を参照してください。
- <http://www.veritas.com/docs/DOC5332>
- 8 (手順 5 と手順 6 で該当する場合) 左側の[ホストマッピング (Host mappings)]、[ホスト (Hosts)]、メニューボタン、[再発行トークンの生成 (Generate reissue token)]の順に選択し、[OK]をクリックします
- NetBackup Web UI の[証明書管理 (Certificate Management)]ノードを使用してトークンを生成します (左側の[ホストマッピング (Host mappings)]、[ホスト (Hosts)]、メニューボタン、[再発行トークンの生成 (Generate reissue token)]の順に選択)。
- 再発行タイプの認証トークンを生成する方法について詳しくは、NetBackup Web UI のヘルプまたは『*NetBackup セキュリティおよび暗号化ガイド*』の「再発行トークンの作成」を参照してください。
- [https://www.veritas.com/support/en\\_US/article.DOC5332](https://www.veritas.com/support/en_US/article.DOC5332)
- 9 [OK]をクリックします。検出は、さらにユーザーが操作する必要なく完了します。
- 検出が正常に完了すると、検出された構成は、NetBackup Web UI の[Bare Metal Restore]、[リソース (Resources)]、[検出された構成 (Discovered configurations)]、[Bare Metal Restore]、[リソース (Resources)]、[検出された構成 (Discovered configurations)] の下の一覧に表示されます。

## 指定した時点へのリストアについて

NetBackup が BMR クライアントをバックアップする際に、現在保存されている構成もバックアップします。その構成には、特定の日時 of クライアントに関する情報が含まれています。そのため、BMR クライアントのバックアップが存在する任意の時点にリストアできます。

指定した時点へのリストアの場合、リストアに指定した時点のリストア構成を作成する必要があります。

## 指定した時点へのリストア処理について

BMR は、通常、最新のバックアップからリストアします。指定した時点へのリストアでは、最後の完全バックアップ以前の状態にシステムをリストアできます。

システムを任意の時点にリストアするには、リストア構成を作成するときにその時点のバックアップを選択します。

指定した時点へのリストアは、最近のソフトウェアの変更によって、システムが使用できなくなった場合に役立ちます。**Bare Metal Restore** では、以前の既知の稼働状態にシステムをリストアできます。

指定した時点へのリストアは、次のようなシナリオで使用します。

- ハードウェアの変更によって、システムが不安定になった。ハードウェアに関連付けられているソフトウェアを完全に削除できない場合があります。関連付けられているすべてのドライブおよびソフトウェアを削除する代わりに、指定した時点へのリストアによって、システムを既知の稼働状態にリストアできます。
- ソフトウェアの追加によって、システムが不安定になった。ソフトウェアのアンインストールでは、ソフトウェアをインストールする前の状態にシステムを戻すことができない場合がありますが、指定した時点へのリストアによってシステムをリカバリできます。
- システムがウイルスの攻撃を受けた。
- 重要なシステムまたはアプリケーションファイルが削除された。

## 指定した時点へのリストア構成の作成

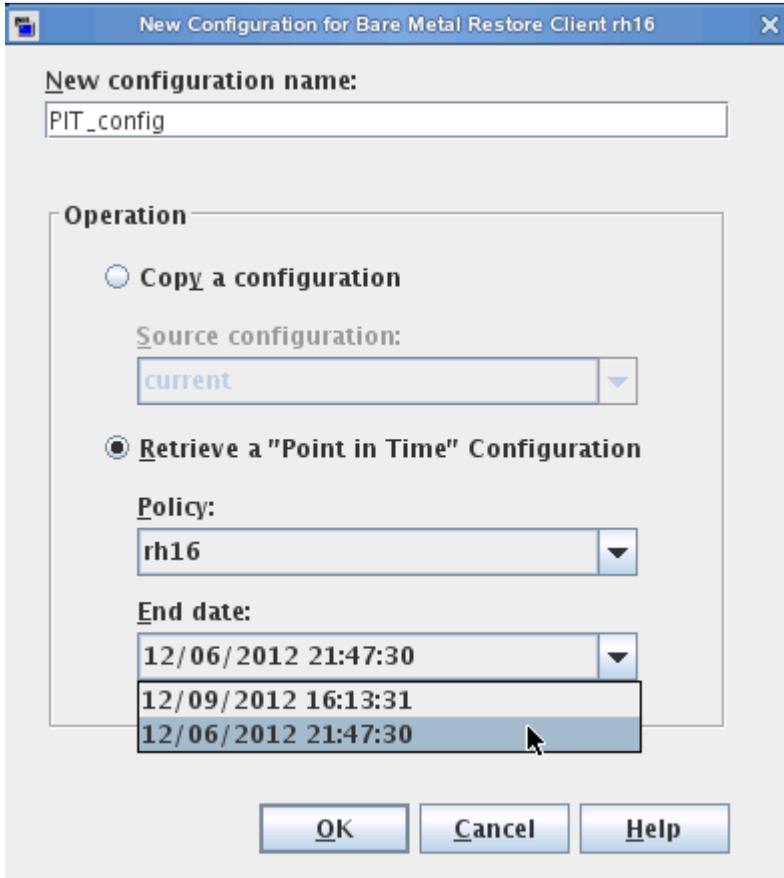
次の手順では、すべてのクライアント形式を対象とした、指定した時点へリストアするためのリストア構成を作成します。クライアントの標準的なリストア手順を次に示します。

指定した時点へのリストア構成を作成する方法

- 1 NetBackup Web UI で、[Bare Metal Restore]、[ホスト (Hosts)]、[Bare Metal Restore クライアント (Bare Metal Restore Clients)]の順に展開します。
- 2 [すべての Bare Metal Restore クライアント (All Bare Metal Restore Clients)] ペインで、クライアントの保存された構成 (現在のものと表示されている構成) を右クリックし、ショートカットメニューから [新規 (New)] を選択します。

- 3 [Bare Metal Restore クライアントの新しい構成 (New Configuration for Bare Metal Restore Client)]ダイアログボックスで、新しい構成の名前を入力します。

リカバリのための特定時点の設定の作成方法を示すサンプル画面ショットは次のとおりです。



- 4 [NetBackup から取得する (Retrieve from NetBackup)] をクリックします。
- 5 リストアの[ポリシー (Policy)]および[終了日時 (End date)]を選択します。

バックアップポリシーで複数のデータストリームを使ってクライアントをバックアップする場合は、バックアップジョブごとのすべてのデータストリームが[終了日時 (End Date)]ドロップダウンメニューに表示されます。リストアする日付の最新のバックアップジョブのストリームを選択します。通常、同じバックアップジョブ内の複数の日数とデータストリームで発生するバックアップジョブは、秒または分単位で区別されます。

**6** [OK]をクリックします。

クライアントの構成のリストに新しい構成が表示されます。これで、リストア準備処理の構成が完了しました。

**7** クライアントをリストアします。

p.93 の「ネットワークブートによる **BMR** クライアントのリストアについて」を参照してください。

p.107 の「メディアブートによる **BMR** クライアントのリストアについて」を参照してください。

## 異なるディスクへのリストアについて

ディスクドライブが交換された場合でも、保護対象のクライアントをリストアできます。また、ボリュームレイアウトやサイズを変更したり、一部のディスクやボリュームのみをリストアする場合に、Dissimilar Disk Restore (DDR) を実行できます。

### Dissimilar Disk Restore 処理について

標準リストアでは、BMR は現在のクライアント構成を使用して元のシステムを再作成します。元のシステムが元のディスク構成に移動されるため、ユーザーの操作は、ほとんど、またはまったく必要ありません。

Dissimilar Disk Restore では、保護対象のクライアントから、新しいディスクにボリューム構成をマッピングする必要があるため、ユーザーの操作が必要です。(ディスクとは物理ディスクを表し、ボリュームとは 1 つ以上の物理ディスク上のディスク領域の論理的区分を表します。)

マッピングは次のように行います。

- リストア前: 編集可能な構成 (編集可能なリストア構成) を作成し、新しいディスクレイアウトでその構成を初期化できます。次に、元のボリューム構成を新しいディスクにマッピングします。マッピングが完了したら、そのリストア構成を使用してクライアントをリストアします。
  - クライアント上の新しいディスクのレイアウト。たとえば、検出処理を実行する場合に必要です。
  - 同じディスクが別の保護対象のクライアントにもあるかどうか。
- リストア中: 標準リストアを実行し、BMR でディスクが異なることが検出されます。BMR が DDR モードになり、編集可能なリストア構成を作成するため、ディスクをマッピングできます。
  - UNIX または Linux クライアントの場合は、マスターサーバー上での NetBackup Web UI の BMR ディスクマッピングユーティリティを使用します。

- Windows クライアントの場合は、リカバリ中に、クライアント上でマッピングするか、NetBackup Web UI の BMR ディスクマッピングユーティリティを使って、マスターサーバー上でマッピングできます。

Dissimilar Disk Restore は次の状況で使用する必要があります。

- 物理ディスクが交換される
- 1 つ以上のディスクのサイズが小さくなったため、同じボリューム配置を格納できない
- 1 つ以上のディスクの場所が変更される
- ディスクの数が減ったため、必要なボリューム配置をリストアできない
- リストア対象のシステムのレイアウトおよびボリュームを変更する必要がある
- システムの一部のディスクのみをリストアする

---

**警告:** ディスクの場所の変更により、リストア後に、クラスタ構成のリソースがオンラインにできなくなる場合があります。BMR は、Dissimilar Disk Restore に対応して、クラスタ構成のリソース属性を調整しようとしません。

---

## DDR 用のリストア構成の作成

表 6-6 に、リストアを開始する前に、編集可能なリストア構成を作成し、ディスクマッピングを実行する手順の概要を示します。

Windows クライアントリカバリの場合、リストアを開始する前に、DDR 構成を作成する必要はありません。リストアを開始してから、リストア中にディスクマッピングを実行することができます。BMR Windows リカバリは、リカバリ中に利用可能なディスクに元のディスクをマッピングできない場合、ディスクマッピング GUI を自動的に開きます。UNIX または Linux クライアントの場合には、ディスク照合に失敗した場合にリカバリ処理が対象ハードウェア検出モードになります。

p.125 の「異なるディスクへのクライアントのリストア」を参照してください。

表 6-6 リストア構成を作成する方法

手順	作業	手順詳細
手順 1	新しいディスクの構成を検出します。	p.159 の「構成の検出」を参照してください。
手順 2	現在の構成をコピーして、編集可能なリストア構成を作成します。	p.158 の「構成のコピー」を参照してください。
手順 3	リストア構成用の[構成の変更 (Change Configuration)]ダイアログボックスを開きます。	p.162 の「構成の変更」を参照してください。

手順	作業	手順詳細
手順 4	検出された構成のディスク情報でリストア構成を初期化し、元のボリューム構成を新しいディスクにマッピングします。	p.178 の「[ボリューム (Volumes)] プロパティについて」を参照してください。
手順 5	マッピングが完了したら、DDR リストア手順を実行します。	p.125 の「異なるディスクへのクライアントのリストア」を参照してください。

## 異なるディスクへのクライアントのリストア

表 6-7 に、異なるディスクにリストアする手順の概要を示します。事前にリストア構成を作成しなかった場合は、リストア処理中に BMR が編集可能なリストア構成を自動的に作成します。

UNIX および Linux の DDR では、次の点に注意してください。

- クラスタ内の共有ディスクは、制限ありとマークされます。
- Solaris クライアント上の未使用の VxVM ディスクは、制限ありとマークされます。制限されたままの状態にしておきます。
- 物理ボリュームがマルチデバイス上に作成された Linux LVM ボリュームグループは、同じ構成にマッピングできません。物理ボリュームは、マルチデバイスにはなく、ディスクまたはパーティションにマッピングされます。

表 6-7 Dissimilar Disk Restore を実行する方法

手順	作業	手順詳細
手順 1	クライアントのリストアを準備します。	リストア構成を事前に準備した場合は、準備操作時にその構成を選択します。  p.86 の「クライアントのリストアを準備する方法」を参照してください。

手順	作業	手順詳細
手順 2	ネットワークブートまたはメディアブートを使用してクライアントをブートし、リストアを開始します。	<p>保護対象のシステムのボリューム構成が新しいディスクにすでにマッピングされている構成を使用する場合は、標準リストアが実行されます。ユーザーの操作は必要ありません。</p> <p>ディスクが異なっていて、まだマッピングされていないことが検出されると、<b>BMR</b> が <b>DDR</b> モードになります。<b>Windows</b> の場合には、自動ポップアップ表示される <b>BMR</b> 構成マッピング <b>GUI</b> を使用して、この時点でボリュームをリカバリ時間ディスクにマッピングできます。</p> <p><b>p.84</b> の「<b>BMR</b> リストア処理」を参照してください。</p>
手順 3	編集可能なリストア構成を保存します。	<p>編集不可能な構成のみ。</p> <p>編集できない構成を使用する場合は、<b>BMR</b> が編集可能なリストア構成を作成します。<b>BMR</b> は現在の構成をコピーし、次のように、その構成の名前を入力するように求めます。</p> <pre>Current configuration name for restore is 'current'. Please enter the name for a new editable configuration:</pre>

手順	作業	手順詳細
手順 4	検出された構成を保存します。	<p>新しいディスクのレイアウトを取得するため、<b>BMR</b> がクライアントのハードウェアを検出します。次のように、検出された構成の名前を入力するように求められます。</p> <p>Please enter the name for a new discovered configuration:</p> <p>検出された構成が保存されます。後で、<b>BMR</b> 構成マッピング GUI で、[初期化 (Initialize)] オプションを使用して、この検出された構成のディスクレイアウトをリストア構成にインポートします (手順 6 を参照)。</p>
手順 5	[構成の変更 (Change Configuration)]を開く	<p>検出された構成が保存されたら、マスターサーバーの <b>NetBackup Web UI</b> で、リストア構成に対して左側の [Bare Metal Restore]、[ホスト (Hosts)]、[Bare Metal Restore クライアント (Bare Metal Restore clients)] の順に選択します。</p> <p>p.162 の「構成の変更」を参照してください。</p>
手順 6	リストア構成を初期化します。	<p>検出された構成からの新しいディスクレイアウトでリストア構成を初期化します。次に、元のボリューム構成を新しいディスクにマッピングします。</p> <p>p.178 の「[ボリューム (Volumes)] プロパティについて」を参照してください。</p>

手順	作業	手順詳細
手順 7	編集されたリストア構成を使ってリストアを準備し、クライアントをリストアします。	<p>p.86 の「<a href="#">クライアントのリストアを準備する方法</a>」を参照してください。</p> <p>p.93 の「<a href="#">ネットワークブートによる BMR クライアントのリストアについて</a>」を参照してください。</p> <p>p.107 の「<a href="#">メディアブートによる BMR クライアントのリストアについて</a>」を参照してください。</p>
手順 8	リストア構成のディスクマッピングがまだ完了していない場合は、ボリュームをディスクにマッピングできるように、BMR が再度 DDR モードになります。	p.178 の「 <a href="#">[ボリューム (Volumes)] プロパティについて</a> 」を参照してください。

## 異なるシステムへのリストア

表 6-8 に、異なるシステムにリストアする手順を示します。

ターゲットシステムのディスクが保護対象のシステムのディスクと異なる場合は、ディスクおよびボリュームのマッピングが必要になります (Dissimilar Disk Restore と同様)。

表 6-8 Dissimilar System Restore の概要

手順	作業	手順
手順 1	Dissimilar System Restore についての理解を深めます。	p.129 の「 <a href="#">Dissimilar System Restore について</a> 」を参照してください。
手順 2	ターゲットシステムの構成を検出します。	p.130 の「 <a href="#">新しいシステムの構成の検出について</a> 」を参照してください。
手順 3	リストアに使用する構成を作成します。	p.130 の「 <a href="#">編集可能な DSR 構成の作成</a> 」を参照してください。
手順 4	リストア構成システムに NIC ドライバと MSD ドライバを追加します。	p.130 の「 <a href="#">NIC ドライバと MSD ドライバの追加について</a> 」を参照してください。

手順	作業	手順
手順 5	リストア構成のネットワークインターフェースとネットワーク識別情報を変更します。	p.131 の「ネットワークインターフェースの変更について」を参照してください。
手順 6	リストア構成にディスクをマッピングします。	p.132 の「リストア構成でのディスクのマッピングについて」を参照してください。
手順 7	ブートメディアを作成します。	p.132 の「ブートメディアの作成について」を参照してください。
手順 8	クライアントをリストアします。	p.133 の「クライアントのリストアについて」を参照してください。
手順 9	リストアされたシステムへの最初のログオンで DSR の変更を完了します。	p.133 の「システムのリストア後の最初のログオン」を参照してください。

## Dissimilar System Restore について

Dissimilar System Restore (DSR) は、保護対象の Windows クライアントをハードウェア構成が異なる新しいシステムにリストアします。

---

**メモ:** ハードウェア構成の変更により、リストア後に、クラスタ構成のリソースがオンラインにできなくなる場合があります。BMR は、Dissimilar System Restore に対応して、クラスタ構成のリソース属性を調整しようとしません。

---

DSR は、次のような場合に効果的です。

- 企業内のシステムの階層で優先されるベンダーを変更する。
- 古いハードウェアから新しいハードウェアにアプリケーションを移行する。
- システムで重大なハードウェア障害が発生し、交換できる類似のハードウェアがない。
- ディザスタリカバリのプロバイダが、ディザスタリカバリサイトで同じハードウェアを提供していない。
- 本番サイトとハードウェアが異なるテストサイトで、アプリケーションのステージングおよび検証を行っている。(アプリケーションをテストから本番に移行できる。)

次の状況が当てはまる場合は、DSR を使用します。

- ターゲットシステムに、保護対象のシステムに含まれていないディスクコントローラがある。
- ターゲットシステムに、保護対象のシステムに含まれていないネットワークカードがある。

- ターゲットシステムで、保護対象のシステムと異なる HAL (ハードウェア抽象シミュレーションレイヤ) またはカーネルが必要である。
- ターゲットシステムと保護対象のシステムの TCP/IP 設定が異なる。(TCP/IP プロパティのみがリストアされます。IPX (Internetwork Packet eXchange) などの他のネットワークプロパティはリストアされないため、リストア後に構成する必要があります。)

## 新しいシステムの構成の検出について

異なるハードウェアへのリストアで行う最初の手順は、新しいシステムに含まれるハードウェアの検出です。

p.159 の「[構成の検出](#)」を参照してください。

## 編集可能な DSR 構成の作成

保護対象のクライアントのリストアに使用する構成を作成する必要があります。次の表は構成を作成する手順をリストしたものです。

表 6-9 編集可能な DSR 構成を作成するプロセス

手順	処理	関連項目
手順 1	保護対象のクライアントの既存の構成をコピーして、DSR 構成を作成します。  たとえば、クライアント「protected」をシステム「target」にリストアする場合は、クライアント「protected」の現在の構成をコピーして、「dsr_to_target」という名前の構成を作成します。	p.158 の「 <a href="#">構成のコピー</a> 」を参照してください。
手順 2	DSR 構成を作成したら、[構成の変更 (Change Configuration)] ダイアログボックスを開き、次の項の説明に従って構成を変更します。	p.164 の「 <a href="#">クライアント構成プロパティ</a> 」を参照してください。

## NIC ドライバと MSD ドライバの追加について

この項は、Windows オペレーティングシステムの場合にのみ該当します。

DSR 構成には、ターゲットシステムで必要な NIC ドライバおよび MSD ドライバが含まれている必要があります。

ターゲットシステムのドライバは、構成を検出するいずれかの手順を実行した際に、パッケージプールに追加されています。

p.159 の「構成の検出」を参照してください。

ドライバは DSR 構成に追加することができます。ドライバを追加するには、構成の [ドライバ (Drivers)] ダイアログボックスの [利用可能なドライバ (Available drivers)] ウィンドウで、追加するドライバを選択します。次に、[リストアに使用するドライバ (Drivers to be used during restore)] ウィンドウに選択したドライバを追加します。

p.167 の「[デバイスおよびドライバ (Devices & Drivers)] プロパティ」を参照してください。

次の方法でドライバをパッケージプールに追加した場合は、ドライバの説明にターゲットシステムの名前が含まれます。

- ターゲットシステムの構成を保存する
- ターゲットシステムからドライバを抽出する

ドライバの説明によって、ターゲットシステムに必要なドライバを識別しやすくなります。保護対象のシステムで使用されているが、ターゲットシステムでは使用されていないドライバを DSR 構成から削除します。

---

**メモ:** TCP/IP プロパティのみがリストアされます。IPX (Internetwork Packet eXchange) などの他のネットワークプロパティはリストアされないため、リストア後に構成する必要があります。

---

## ネットワークインターフェースの変更について

DSR 構成のネットワークインターフェースおよびネットワーク識別情報を変更する必要があります。

変更を正しく反映させるには、構成の検出の一部である手順に従ってターゲットシステムをバックアップする必要があります。

p.159 の「構成の検出」を参照してください。

ターゲットシステムにクライアントをインストールし、前述の手順に従ってクライアントをバックアップしたら、次の操作を実行できます。

- 構成から NIC 情報をインポートする
- 保護対象のクライアントのネットワーク識別情報 (IP アドレス、ネットマスクおよびドメイン名) をターゲットシステムの NIC にマッピングする

ターゲットシステムの構成を保存しなかった場合は、ターゲットシステムの NIC の MAC アドレスを確認する必要があります。その後、ネットワークインターフェース情報を手動で DSR 構成に追加します。

インターフェースをインポートしてマッピングする手順、またはインターフェースを手動で変更する手順に関する詳細情報が利用可能です。

p.172 の「[\[ネットワークインターフェース \(Network Interfaces\)\]プロパティ](#)」を参照してください。

## リストア構成でのディスクのマッピングについて

Dissimilar System Restore は、Dissimilar Disk Restore であるとも言えます。ターゲットシステムのディスクが保護対象のクライアントのディスクと異なる場合、元のシステムのボリューム構成を新しいディスクにマッピングする必要があります。(Dissimilar Disk Restore の場合と同様にマッピングします) システムパーティションまたはボリュームのサイズを縮小または拡大することもできます。ベンダーパーティション (存在する場合) を保護対象のクライアントからターゲットシステムのディスクにマッピングする必要はありません。

変更を正しく反映させるには、構成の検出の一部である手順に従ってターゲットシステムをバックアップする必要があります。

p.159 の「[構成の検出](#)」を参照してください。

ターゲットシステムにクライアントをインストールし、前述の手順に従ってクライアントをバックアップしたら、次の操作を実行できます。

- この構成からディスクレイアウトをインポートします。
- リストアの前にディスクをマッピングします。

Cohesity リストアする前にディスクをマッピングすることは、特に、保護対象のクライアントのシステムパーティションがターゲットシステムのシステムディスクに収まらない場合にお勧めします。

ターゲットシステムの構成を保存しなかった場合は、リストア時に DDR マッピングを実行する必要があります。

Dissimilar Disk Restore に関する詳細情報が利用可能です。

p.123 の「[異なるディスクへのリストアについて](#)」を参照してください。

Windows クライアントのリカバリ中に、クライアントオペレーティングシステムをリカバリしているターゲットシステムのディスク上に、BMR リカバリ処理によってベンダーパーティションが検出された場合、BMR は検出されたベンダーパーティションを保持するオプションを表示します。

## ブートメディアの作成について

ターゲットシステムを開始するためにメディアを使う場合、メディアが利用可能でなければメディアを作成します。

p.77 の「[ブートメディアの管理](#)」を参照してください。

## クライアントのリストアについて

DSR 構成を使用してクライアントのリストアを準備し、Dissimilar System Restore 処理を開始します。

p.93 の「ネットワークブートによる BMR クライアントのリストアについて」を参照してください。

p.107 の「メディアブートによる BMR クライアントのリストアについて」を参照してください。

## システムのリストア後の最初のログオン

この項は、Windows オペレーティングシステムの場合にのみ該当します。

システムのリストア後、DSR の変更を完了するには、ローカル管理者でのログインが必要です。bmrcleanup ユーティリティが起動して、実行中の処理について説明する状態ボックスが表示されます。

状態ボックスが表示されたときに、Windows で多数の新しいハードウェアの検出ウィザードが表示される場合があります。

システムリストアの後、はじめてログオンするには、表示されるウィザードまたはメッセージ画面に従って、次の処理を実行してください。

- [デジタル署名未検出]パネルでは、[はい]または[続行]をクリックします。
- [新しいハードウェアの検出ウィザード]パネルでは、[キャンセル]をクリックします。
- [新しいドライバがインストールされました。再ブートしますか?]パネルでは、[いいえ]をクリックします。

---

メモ: bmrcleanup 状態ボックスが完了するまで、システムを再ブートしないでください。

---

## NetBackup メディアサーバーのリストアについて

NetBackup メディアサーバーは、BMR クライアントとして保護する場合にリストアできます (ただし、NetBackup マスターサーバーと同じ場所にあるメディアサーバーはリストアできません)。

NetBackup メディアサーバーのリストアには、次のオプションがあります。

- メディアサーバーを別のメディアサーバーにバックアップする場合、保護対象のクライアントと同様に保護対象のメディアサーバーをリストアします。

p.93 の「ネットワークブートによる BMR クライアントのリストアについて」を参照してください。

p.107 の「メディアブートによる BMR クライアントのリストアについて」を参照してください。

- メディアサーバーは、**SCSI 接続ストレージデバイス**または **SAN 接続ストレージデバイス**を使って、自身のデータをバックアップできます。この場合、代替メディアサーバーを使用するように **NetBackup** を構成してから、**BMR** を使ってメディアサーバーをリストアします。

詳細情報を参照できます。

p.134 の「[代替メディアサーバーの構成について](#)」を参照してください。

p.135 の「[メディアサーバーのリストア](#)」を参照してください。

## 代替メディアサーバーの構成について

**NetBackup** に代替メディアサーバーを構成する方法が 2 つあります。

次のどちらかを実行する必要があります。

- 自動メディアサーバーフェールオーバーの構成。この方法では、メディアサーバーが利用できない場合にのみ、リストア先が変更されます。この方法は、メディアを含むライブラリが、障害が発生したメディアサーバーと代替メディアサーバーの両方に接続されている場合に、最も有用です。通常、障害が発生する前に、自動メディアサーバーフェールオーバーを構成しておきます。これにより、リストア時の時間と労力を削減できます。
- 元のメディアサーバーの手動上書き。この方法では、元のメディアサーバーの状態に関係なく、強制的に代替メディアサーバーへのリストアが行われます。
  - 障害が発生する前に自動メディアサーバーフェールオーバーを構成しなかった場合。
  - 元のメディアサーバーをリストアできるように一時的にメディアサーバーを再割り当てする場合。

(BMR リストアだけでなく)バックアップとリストアのすべての要求が代替メディアサーバーに送信されます。

詳細情報を参照できます。

p.135 の「[元のメディアサーバーの手動上書き](#)」を参照してください。

p.135 の「[代替サーバーへの自動メディアサーバーフェールオーバーの有効化](#)」を参照してください。

代替メディアサーバーを使用するように **NetBackup** を構成する方法に関する詳細情報が利用可能です。

『[NetBackup Web UI 管理者ガイド](#)』を参照してください。

## 代替サーバーへの自動メディアサーバーフェールオーバーの有効化

通常、元のメディアサーバーで障害が発生する前に、自動メディアサーバーフェールオーバーを構成しておきます。

UNIX および Linux システムでは、bp.conf ファイルの

FAILOVER\_RESTORE\_MEDIA\_SERVERS パラメータでこのオプションを設定します。

### 代替メディアサーバーへの自動フェールオーバーを有効にする方法

- 1 プライマリサーバーの[リストアのフェールオーバー (Restore failover)]ホストプロパティを開きます。
- 2 [代替リストア用のフェールオーバーマシン (Alternate Restore Failover Machines)] リストにエンTRIESを追加し、メディアサーバーおよびリストア用のフェールオーバーサーバーの名前を入力します。
- 3 プライマリサーバー上で、NetBackup Request Manager デーモンまたはサービスを停止してから再起動します。

## 元のメディアサーバーの手動上書き

メディアサーバーを物理的に上書きする前に、必要に応じて、メディアを新しいメディアサーバーのライブラリに移動します。次に、NetBackup データベースを更新して、その移動を反映します。

リストアを実行したら、[メディアホストの上書き (Media host override)]リストから代替サーバーのエンTRIESを削除して、NetBackup 構成の変更を元に戻します。元のサーバーは NetBackup とリストアの要求を再度実行します。

UNIX および Linux システムでは、bp.conf ファイルの FORCE\_RESTORE\_MEDIA\_SERVER パラメータでこのオプションを設定します。

### 手動リストアで元のサーバーを上書きする方法

- 1 プライマリサーバーの[一般的なサーバー (General server)]ホストプロパティを開きます。
- 2 [メディアホストの上書き (Media host override)]リストにエンTRIESを追加し、元のバックアップサーバーおよびリストアサーバーの名前を入力します。
- 3 マスターサーバー上で、NetBackup Request Manager デーモンまたはサービスを停止してから再起動します。

## メディアサーバーのリストア

メディアサーバーで障害が発生する前に、(多くの場合、自動フェールオーバーの方法で) 代替メディアサーバーを構成した場合、代替メディアサーバーは元のメディアサー

バーの BMR クライアント構成にホストとして保存されます。これにより、標準リストアを実行できるようになります。

障害が発生する前に NetBackup 代替メディアサーバーを構成しなかった場合は、リストア時に使用するリストア構成を作成および変更します。

表 6-10                   メディアサーバー処理のリストア

手順	作業	手順詳細
手順 1	リストア構成を作成します。	p.158 の「構成のコピー」を参照してください。
手順 2	代替メディアサーバーをホストとして追加します。	p.162 の「構成の変更」を参照してください。 p.170 の「[[ホスト (Hosts)]プロパティ」を参照してください。
手順 3	リストア構成を作成および変更したら、標準リストアを実行します。	p.93 の「ネットワークブートによる BMR クライアントのリストアについて」を参照してください。 p.107 の「メディアブートによる BMR クライアントのリストアについて」を参照してください。

## BMR ブートサーバーのリストアについて

BMR ブートサーバーは、BMR クライアントとして保護する場合にリストアできます。最初に BMR ブートサーバーをバックアップします。その後で、保護対象のブートサーバーを再構築するためのリソースを格納する別のブートサーバーまたは BMR メディアベースの共有リソースツリーを使用します。

ブートサーバーが同じシステムに NetBackup マスターサーバーとしてインストールされている場合は、それを BMR クライアントとして保護することはできません。NetBackup マスターサーバーへの NetBackup カタログ (BMR データベースを含む) のリカバリは可能です。ただし、マスターサーバーに NetBackup および BMR ソフトウェアを再インストールする必要があります。

詳しくは、『NetBackup トラブルシューティングガイド』のディザスタリカバリ手順を参照してください。

# AWS RHEL および Windows VM クライアントのリストアについて

BMR (Bare Metal Recovery) は、RHEL および Windows オペレーティングシステムプラットフォームで実行されている AWS 仮想マシンのバックアップとリカバリを容易にします。

BMR でサポートされる RHEL および Windows OS プラットフォームについて詳しくは、[BMR SCL](#) を参照してください。

この機能は、スナップショット機能が利用できない AWS ローカルゾーンで特に役立ちます。

NetBackup Web UI では、AWS 仮想マシンで RHEL および Windows EC2 を実行している BMR クライアントの構成に新しいオプションが表示されるようになりました。このオプションは[クラウドにリストア (Restore to Cloud)]です。

## 開発要件

NetBackup プライマリサーバーは、オンプレミスまたは AWS EC2 に配置できます。NetBackup RHEL または Windows クライアントとメディアサーバーは、AWS EC2 で構成する必要があります。NetBackup プライマリサーバーとともに、NBSM (NetBackup Snapshot Manager) がインストールおよび構成されている必要があります。さらに、保護対象の AWS VM が NBSM によってすでに検出されている必要があります。

## AWS RHEL VM の BMR バックアップ

BMR バックアップ処理は、標準の BMR バックアップデータとともに、必要なインスタンスの詳細をキャプチャします。

## BMR AWS RHEL および Windows VM リストアの前提条件

- AWS 仮想マシンのバックアップをリストアする場合、SRT (共有リソースツリー) は不要であるため、ブートサーバーは不要になります。
- 代わりに、バックアップと同じ OS バージョンの AMI (Amazon マシンイメージ) が必要です。Windows のリストアの場合は、Windows 2019 以降のバージョンの AMI が必要です。この AMI には NetBackup クライアントがインストールされている必要がありますが、証明書は含まれません。
- ダウンロードセンターで利用可能なスクリプトは、基本 AMI や NetBackup クライアントインストーラへのパスなどの入力を受け入れます。このスクリプトは、リストアに必要な AMI を作成します。  
[https://www.veritas.com/content/support/ja\\_JP/downloads/update.UPD985473](https://www.veritas.com/content/support/ja_JP/downloads/update.UPD985473)
- さらに、このスクリプトでは、ターゲット仮想マシンの作成時に使用される、キーファイル (公開鍵と秘密鍵のペアを含む .pem ファイル) とキー名の入力が必要です。

### BMR AWS 仮想マシンをリストアするには

- 1 BMR バックアップ中に収集されたインスタンスデータとユーザー入力を利用して、指定した AMI ID から新しい仮想マシンがインスタンス化されます。
- 2 BMR バックアップでキャプチャされた適切なサイズと形式のディスクは、手順 1 で作成したターゲット仮想マシンに接続されます。
- 3 NetBackup CA 証明書とホスト証明書が取得され、ターゲット仮想マシンにインストールされます。
- 4 リストア操作はターゲット仮想マシンで開始されます。
- 5 ターゲット仮想マシンで BMR リストアが完了すると、AMI OS ブートディスクが BMR 操作からリストアされたブートディスクで切り替えられます。

---

**メモ:** 元のインスタンスが削除され、IP アドレスとホスト名の両方をターゲット仮想マシンに割り当てることができる場合、ユーザーは[元の IP とホスト名を使用してリストア (Restore with original IP and hostname)]オプションを選択できます。

---

## 制限事項および考慮事項

- ユーザーが[元の IP とホスト名を使用してリストア (Restore with original IP and hostname)]オプションを選択しない場合、ソース仮想マシンのバックアップが異なる IP とホスト名でリストアされることがあります。その結果、リストアされたクライアントは新しい ID を採用し、どのポリシーでも構成されません。
- ユーザーは、保護とバックアップを確実にするために、リストアされたクライアントを必要なポリシーで構成する必要があります。

## 外部プロシージャについて

外部プロシージャは、ユーザーの終了時にリストア処理と対話するスクリプトです。外部プロシージャの使用によって、自動化されていないリストアに必要なユーザーの操作を最小限に抑えられます。

次に、外部プロシージャの種類を示します。

- 特定のクライアントのクライアント固有プロシージャ
- 特定のオペレーティングシステムの種類すべてのクライアントのオペレーティングシステム固有プロシージャ

クライアント固有プロシージャはオペレーティングシステムプロシージャより優先されます。

外部プロシージャは、次のいずれかの操作を行った場合にのみ開始されます。

- [クライアントのリストア準備 (Prepare to Restore Client)]または[検出準備 (Prepare To Discover)]ダイアログボックスで、[外部プロシージャを実行する (Run External Procedures)]を選択する。
- `bmrprep -runep` コマンドを使用して外部プロシージャを指定する。

外部プロシージャは、リストア環境 (リストア処理時の制限されたオペレーティングシステム環境) で実行します。リストア環境では、完全なオペレーティングシステムで利用可能な多くのコマンドと機能が使用できません。

UNIX 外部プロシージャは `root` として実行します。Windows 外部プロシージャは管理者として実行します。

外部プロシージャは、NetBackup マスターサーバー上の BMR データベースに保存されます。マスターサーバーで `bmrepadm` コマンドを使用して、外部プロシージャを管理します。

---

メモ: 外部プロシージャの使用には、スクリプトに関する一般的な知識が必要です。

---

## 外部プロシージャのポイントと名前

BMRは、次の順序で、リストア処理時に次のユーザーの出口ポイントで外部プロシージャを実行できます。

<code>prediscover</code>	ハードウェアの検出が BMR サーバーに報告される前 (UNIX クライアントのみ)。
<code>preformat</code>	ディスクのフォーマットおよびパーティション作成前。Windows システムでは、システムドライブのフォーマット後、かつシステム以外のドライブのフォーマット前に、 <code>preformat</code> が実行されます。
<code>prerestore</code>	ファイルのリストア開始前。
<code>postrestore</code>	ファイルのリストア後。
<code>first boot</code>	リストアの完了後およびリストアされたクライアントの初回ブート時。Windows システムでは、クライアントのリストア後、最初のユーザーがログオンしたときに、初回ブートの外部プロシージャが実行されます。

外部プロシージャポイント名は、ユーザーが作成する各外部プロシージャスクリプトの名前の一部として使用されます。クライアント固有の外部プロシージャの命名規則は、オペレーティングシステム固有の外部プロシージャと異なります。

---

メモ: Microsoft Windows システム用の外部プロシージャには、`.cmd` 拡張子を追加しないでください。BMR は、リストア準備処理時にスクリプトを生成する際に、適切なファイル名拡張子を追加します。

---

クライアント固有の外部プロシージャ名      クライアント固有の外部プロシージャ名は次の形式になります。

*clientname\_externalprocedure*

たとえば、sol123\_prerestore 外部プロシージャは、クライアント sol123 でファイルがリストアされる前に開始されます (プロシージャは、リストア時に [外部プロシージャを実行する (Run External Procedures)] を指定した場合に開始されます)。

オペレーティングシステム固有の外部プロシージャ名      オペレーティングシステム固有の外部プロシージャ名は次の形式になります。

*externalprocedure.ostype*

**ostype** には、次のいずれかを指定します。

- aix  
AIX
- hp  
HP-UX システム
- linux  
Linux システム
- sol  
Solaris システム
- win  
Windows システム

たとえば、preformat.linux 外部プロシージャは、ドライブがフォーマットされる前に、Linux クライアント上で開始されます (プロシージャは、リストア時に [外部プロシージャを実行する (Run External Procedures)] を指定した場合に開始されます)。

## 外部プロシージャの管理について

bmrepadm コマンドを使用して、次の操作を実行します。

- リストア時に使用できるように外部プロシージャを追加する
- データベースから外部プロシージャを削除する

- データベースから外部プロシージャを抽出する
- データベース内のすべての外部プロシージャを一覧表示する

たとえば、sol123 という名前のクライアントの **prerestore** 外部プロシージャを追加するには、BMR データベースが構成された **NetBackup** マスターサーバーで次のコマンドを実行します。

```
bmrepadm -add sol123_prerestore
```

bmrepadm コマンドではクライアント名が検証されません (すなわち、存在しないクライアントの外部プロシージャを追加できます)。

他の例として、ListStorageGroups.vbs という名前の外部プロシージャ補助ファイルを追加するには、次のコマンドを実行します。

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

bmrepadm コマンドについて詳しくは、『**NetBackup コマンドリファレンスガイド**』を参照してください。

## 外部プロシージャの指定

外部プロシージャを実行するリストア準備処理時に指定する必要があります。BMR マスターサーバーは、適切な外部プロシージャスクリプトを作成し、それらをリストア時に使用します。

---

**メモ:** 外部プロシージャは、リストア準備処理または検出準備処理が開始される前に、BMR データベースに存在している必要があります。

---

外部プロシージャを指定するには

- [検出準備 (Prepare To Discover)] または [クライアントのリストア準備 (Prepare to Restore Client)] ダイアログボックスで、[外部プロシージャを実行する (Run External Procedures)] を選択します。  
p.159 の「**構成の検出**」を参照してください。  
p.86 の「**クライアントのリストアを準備する方法**」を参照してください。
- または、bmrprep コマンドの `-runep` オプションを使用して、外部プロシージャを指定します。

## 外部プロシージャのデータ転送について

bmrc コマンドを使用して、リストア時に BMR マスターサーバーからクライアントにファイルを転送できます。

UNIX システムでは、/tmp ファイルシステムまたは /tmp にマウントされているファイルシステムにデータを格納します。他のすべてのファイルシステムはリストア時に読み取り専用になります。

Windows システムでは、デフォルトで転送されたファイルが現在のディレクトリに格納されます。このディレクトリは、リストア時は %SystemDrive% です。first boot プロシージャ実行時は、%HOMEPATH% です。コマンドラインで他のパス名またはファイル名を指定できます。

次に、bmrc コマンドを使用して、マスターサーバーからクライアントにファイルを転送する例を示します。

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

外部プロシージャで bmrc コマンドを開始する場合は、次のようにリストア環境でフルパスを指定します。

- UNIX クライアントと Linux クライアントの場合: /usr/opensv/NetBackup/bin
- Microsoft Windows クライアントの場合: %SystemDrive%\BMR\NBU\bin  
first boot 外部プロシージャポイントでの bmrc コマンドのパスは、Microsoft Windows クライアントでは *install\_path*\NetBackup\bin になります。

bmrc コマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

## 外部プロシージャとの対話について

### UNIX および Linux システムの場合

リストア時にコマンドを入力して外部プロシージャと対話できます。これを行うには、外部プロシージャスクリプト内から bmrShell 関数を実行します。bmrShell 関数を使用すると、デフォルトのコンソールキーボードから入力し、コンソールモニターに出力できます。

リダイレクトを使用して、特殊デバイスに出力をリダイレクトし、外部プロシージャから画面に送ることもできます。これを行うには、/dev/console を使用します (例: echo "Hello World" >> /dev/console)。

UNIX および Linux システムでは、初回ブート時に bmrShell を使用できません。

## Windows システム

リストア時にコマンドを入力して外部プロシージャと対話できます。これを行うには、外部プロシージャスクリプト内から **Windows** コマンドインタプリタ `cmd` を実行します。

**Windows** システムでは、制限されたリストア環境に **DLL** が含まれていなかったり、または元のクライアントシステムで使用されていたものと同じバージョンの **DLL** が含まれていない場合があります。リストア時に `bmrc` を使用してそれらの **DLL** を `C:\BMR\WINNT\SYSTEM32` ディレクトリに転送します。または、その **DLL** の場所を **PATH** 環境変数に追加します。

## 外部プロシージャのログ 例

リストア処理時に、**BMR** マスターサーバーで次のログが作成されます。

```
/usr/opensv/netbackup/logs/bmrrst/client_name/log.mmddyy (UNIX)
install_path¥NetBackup¥logs¥bmrrst¥client_name¥log.mmddyy (Windows)
```

**UNIX** および **Linux** システムでは、**BMR** リストア処理によって、外部プロシージャの開始および終了メッセージがログに書き込まれます。**(Windows** システムでは、**BMR** リストア処理で開始および終了の記録は行われません。)**外部プロシージャスクリプトで `bmrc` コマンドを使用して、メッセージをログに書き込むこともできます。**

外部プロシージャは、開始および終了時にメッセージを書き込みます。メッセージには、プロシージャが開始された日時、クライアント名、外部プロシージャ名の説明が含まれます。次に例を示します。

```
2005/08/02 12:10:38.180 w2k200,sol1157 INFO: Executing External
Procedure: sol1123,sol1123_prerestore.
2005/08/02 12:10:38.350 w2k200,sol1157 INFO: Completed executing
External Procedure: sol1123,sol1123_prerestore.
```

`bmrc` コマンドを使用して、メッセージをリストアログに書き込むことができます。次に、クライアント **sol1123** のリストア時にメッセージを書き込む `bmrc` コマンドの例を示します。

```
bmrc -operation create -resource message -client sol1123 -msg "
message text to log"
```

または、次の例に示すように、パイプを介して `bmrc` コマンドにデータを書き込むことができます。

```
echo "Hello World" | bmrc -operation create -resource log -client
sol1123
```

次に、前述のコマンドのログエントリを示します。

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

外部プロシージャで `bmrc` コマンドを開始する場合は、次のようにリストア環境でフルパスを指定します。

- UNIX クライアントと Linux クライアントの場合: `/usr/openv/netbackup/bin`
- Microsoft Windows クライアントの場合: `%SystemDrive%\¥BMR¥NBU¥bin`  
`first boot` 外部プロシージャポイントでの `bmrc` コマンドのパスは、Microsoft Windows クライアントでは `install_path¥NetBackup¥bin` になります。

`bmrc` コマンドについて詳しくは、『[NetBackup コマンドリファレンスガイド](#)』を参照してください。

## 外部プロシージャの操作状態

外部プロシージャの操作中、次の操作状態が[タスク (Tasks)]ビューに表示されます。

検出の外部プロシージャ (Discovery External Procedure)	外部プロシージャは <code>prediscover</code> フェーズで実行中です。
初回ブートの外部プロシージャ (First Boot External Procedure)	外部プロシージャは <code>first boot</code> フェーズで実行中です。
リストア後の外部プロシージャ (Post-restore External Procedure)	外部プロシージャは <code>postrestore</code> フェーズで実行中です。
フォーマット前の外部プロシージャ (Pre-format External Procedure)	外部プロシージャは <code>preformat</code> フェーズで実行中です。
リストア前の外部プロシージャ (Pre-restore External Procedure)	外部プロシージャは <code>prerestore</code> フェーズで実行中です。

## 外部プロシージャの終了コードについて

外部プロシージャが戻りコード `0` で終了していることを確認します。外部プロシージャが `0` 以外のコードで終了している場合は、リストアが入力のために一時停止します。

リストア時に外部プロシージャが失敗してもかまわない場合 (システム機能に不可欠でない場合)、外部プロシージャから `0` で終了するようにします。

## 外部プロシージャのエラー処理について

デフォルトで、外部プロシージャは `0` 以外の戻りコードを返す場合に、リストア処理を停止し、ユーザーの操作を待機します。

UNIX および Linux のリストアの場合、次のメニューが表示されます。

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.

[再試行 (Retry)]を選択すると、外部プロシージャを実行する前に、BMR サーバーから外部プロシージャを再度転送するかどうかを尋ねられます。このプロンプトの段階で、外部プロシージャを再実行する前に、マスターサーバー上で編集することができます。

---

**メモ:** ターミナルを定義せずに UNIX で初回ブートの外部プロシージャを実行し、このプロシージャが 0 以外を返した場合、Bare Metal Restore 処理は終了します。

---

Windows のリストアの場合、次の選択肢を含むダイアログボックスが表示されます。

- [キャンセル (Cancel)]はリストアを停止します。
- [再試行 (Try Again)]は外部プロシージャを再実行します。
- [続行 (Continue)]はエラーを無視し、リストアを続行します。

[再試行 (Try Again)]を選択すると、外部プロシージャを実行する前に、BMR サーバーから外部プロシージャを再度転送するかどうかを尋ねられます。このプロンプトの段階で、外部プロシージャを再実行する前に、マスターサーバー上で編集することができます。

## 外部プロシージャの環境変数について

BMR は、リストア処理時に、特定の環境変数を設定し、エクスポートします。それらの中には、汎用環境変数と BMR に固有の環境変数があります。

### UNIX と Linux の環境変数

UNIX および Linux システムでは、次の環境変数がエクスポートされます。

表 6-11 UNIX と Linux の環境変数

システムによって異なる	説明
\$BMRC	bmrc 実行可能ファイルのパス名 (/usr/openv/NetBackup/bin/bmrc)
\$bootServerAddress	ブートサーバー IP アドレス
\$clAddress	クライアントの IP アドレス

システムによって異なる	説明
<code>\$clAddressHex</code>	16 進数に変換されたクライアント IP アドレス
<code>\$client_firstboot</code>	クライアント固有の <b>first boot</b> 外部プロシージャの名前
<code>\$client_postrestore</code>	クライアント固有の <b>postrestore</b> 外部プロシージャの名前
<code>\$client_prediscover</code>	クライアント固有の <b>discover</b> 外部プロシージャの名前
<code>\$client_preformat</code>	クライアント固有の <b>preformat</b> 外部プロシージャの名前
<code>\$client_prerestore</code>	クライアント固有の <b>prerestore</b> 外部プロシージャの名前
<code>\$clName</code>	クライアントの名前。
<code>\$clOs</code>	BMR の簡略な OS 仕様
<code>\$configName</code>	構成の名前
<code>\$default_firstboot</code>	OS のデフォルトの <b>first boot</b> 外部プロシージャの名前
<code>\$default_postrestore</code>	OS のデフォルトの <b>postrestore</b> 外部プロシージャの名前
<code>\$default_prediscover</code>	OS のデフォルトの <b>prediscover</b> 外部プロシージャの名前
<code>\$default_preformat</code>	OS のデフォルトの <b>preformat</b> 外部プロシージャの名前
<code>\$default_prerestore</code>	OS のデフォルトの <b>prerestore</b> 外部プロシージャの名前
<code>\$defaultGateway</code>	デフォルトゲートウェイの名前
<code>\$extProcName</code>	現在の外部プロシージャの名前
<code>\$importNonRootVgs</code>	システム以外のボリュームおよびディスクグループのインポート
<code>\$logging</code>	リストアのログ。 <b>yes</b> = はい、 <b>no</b> = いいえ
<code>\$newConfig</code>	検出する構成名

システムによって異なる	説明
\$onEpError	外部プロシージャエラーに対するリストアの動作 0 = キャンセル 1 = 確認 2 = 無視
\$runEp	外部プロシージャが検出された場合に実行する。0 = いいえ、1 = はい
\$runMode	BMR プロセスの検出またはリストアのモード
\$serverAddress	NetBackup サーバー IP アドレス
\$serverGateway	NetBackup サーバーへのゲートウェイ
\$serverName	NetBackup サーバー名

## AIX の環境変数

```
$BMR_BOSINST_DATA      $MNT
$RC_CONFIG              $ROUTES
```

次のエクスポートされるオペレーティングシステム環境変数は、リストア時に設定されます。

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

## HP-UX の環境変数

次のエクスポートされるオペレーティングシステム環境変数は、リストア時に設定されます。

```
$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 の環境変数

次のエクスポートされるオペレーティングシステム環境変数は、リストア時に設定されます。

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

## Windows の環境変数

リストア時に Windows コマンドラインインタプリタを起動するには、CMD を使用します。

次のエクスポートされるオペレーティングシステム環境変数は、リストア時に使用できます。

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

# SAN (ストレージエリアネットワーク) のサポートについて

Bare Metal Restore (BMR) では、ストレージエリアネットワーク (SAN) に接続されているシステムをリストアできます。Windows、AIX、Linux、Solaris および HP-UX システムでは、ホストバスアダプタ (HBA) ドライバが使用できる場合に、BMR は SAN に接続されたボリュームを自動的にリストアします。

---

**メモ:** BMRリカバリ中、同じ SAN LUN 上でオペレーティングシステムを復元し、コンピュータを再度 SAN ブート可能な状態にする BMR DDR (Dissimilar Disk Restore) サポートを使用するか、ローカルディスク上のオペレーティングシステムを移動して、コンピュータをローカルディスクからブート可能にすることができます。同じロジックはローカルディスクベースのシステムを持っているコンピュータを復元している間に適用可能です。DDR を使用して、ユーザーは SAN LUN にオペレーティングシステムボリュームをマッピングし、復元されたコンピュータの SAN をブート可能にさせることができます。

---

p.149 の「Solaris の SAN に接続されたボリュームがマッピングされていないままの場合にそれらをリストアする方法」を参照してください。

p.149 の「Windows クライアントでの SAN と Dissimilar System Restore について」を参照してください。

## Solaris の SAN に接続されたボリュームがマッピングされていないままの場合にそれらをリストアする方法

次の説明は、Solaris クライアントだけに適用されます。

Dissimilar Disk Restore 機能を使用して Solaris システムをリカバリした後は、マップされていないままの (非リストア対象としてマーク付けされている) SAN に接続されたボリュームに対し、次の手順を実行する必要がある場合があります。

**Solaris の SAN に接続されたボリュームがマッピングされていないままの場合にそれらをリストアする方法**

- 1 現在と以前の `vfstab` ファイルの違いを判断します。

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

- 2 違いを確認します。

- 3 `/etc/vfstab.old.bmr.dmr` ファイルの SAN デバイスに関するエントリをコピーします。コピーしたエントリを `/etc/vfstab` ファイルに追加するか、`vfstab` の結合時にコメントアウトされた行をコメント解除します。

- 4 SAN に接続されているファイルシステムをマウントします。

- 5 NetBackup のバックアップ、アーカイブおよびリストアインターフェースを使用して、SAN ファイルシステムを手動でリストアします。

## Windows クライアントでの SAN と Dissimilar System Restore について

次の説明は、Windows クライアントだけに適用されます。

Windows で Dissimilar System Restore を実行し、SAN ディスクにリストアする場合は、次の手順を実行する必要があります。

- HBA ドライバをリストア構成に追加します。HBA ドライバは、他の大容量記憶装置デバイスドライバと同様に追加できます。
- ターゲットシステムの HBA がソースシステムに存在していた HBA と同じデバイスを認識するように、SAN を構成します。

ドライバの追加に関する詳細情報が利用可能です。

p.130 の「NIC ドライバと MSD ドライバの追加について」を参照してください。

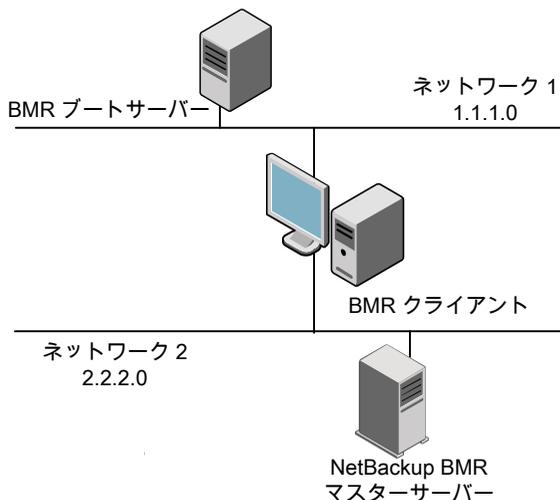
## 複数のネットワークインターフェースのサポートについて

BMRリカバリは、ブート段階およびファイルのリストア段階の 2 つの主な段階で実行されます。ブート段階では、1 つのネットワークインターフェースを使って、BMR ブートサーバーと通信します。リストア環境がブートサーバーからロードされると、BMR は、ファイルのリストア段階で使用するすべてのネットワークインターフェースを構成して有効にします。

**メモ:** 複数のネットワークインターフェースを持つシステムは、マルチホームシステムとも呼ばれます。BMR では、マルチホームクライアントが完全にサポートされています。

図 6-4 に、マルチホームクライアントで実行可能な構成を示します。この構成では、クライアントをネットワークブートするときに、ネットワーク 1 のネットワークインターフェースを指定します。

図 6-4 マルチホームの簡単な例



## ゲートウェイを使ったクライアント構成について

BMR クライアントは、リストア処理時に、ゲートウェイを使用して BMR サーバーおよび NetBackup サーバーと通信できます。

表 6-12 に、リストア時に使用されるゲートウェイ属性を示します。

表 6-12 ネットワークゲートウェイ

ゲートウェイ	説明
デフォルトゲートウェイ	リストア時にクライアントのデフォルトのネットワークゲートウェイを定義します。
マスターサーバーゲートウェイ	クライアントから NetBackup マスターサーバーへのゲートウェイを定義します。
メディアサーバーゲートウェイ	クライアントから NetBackup メディアサーバーへのゲートウェイを定義します。これは、ファイルのリストアに使用されます。

すべてのゲートウェイを指定する必要はありません。クライアントがデフォルトゲートウェイを使用してすべてのホストと通信できる場合、指定する必要があるのはデフォルトゲートウェイのみです。

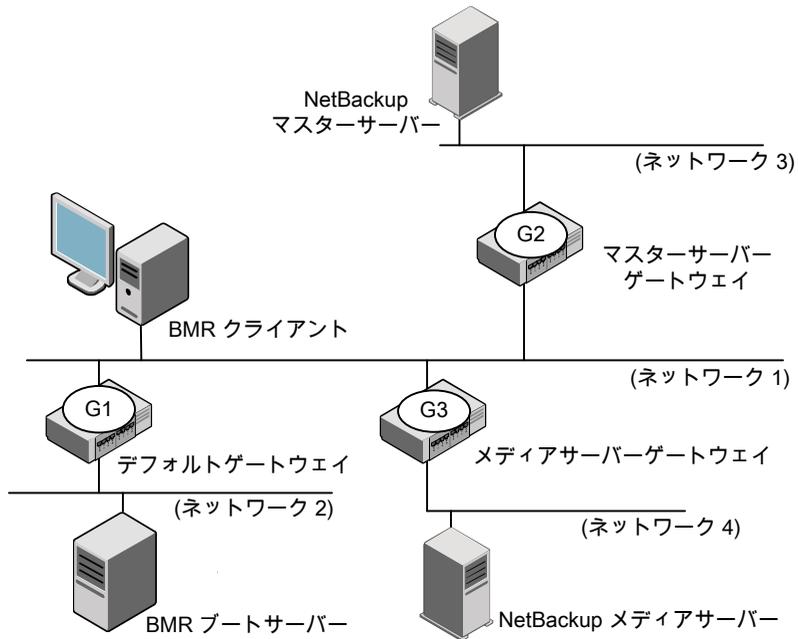
ネットワークブートの場合は、次のように指定します。

- リストア構成の[ホスト (Hosts)]ダイアログボックスで NetBackup マスターサーバーおよびメディアサーバーのゲートウェイを指定します。
- [ネットワークルート (Network Routes)]ダイアログボックスでデフォルトゲートウェイを指定します。

メディアブートの場合は、ブートメディアの作成時またはリストア時にこれらの値を指定するように求められます。

図 6-5に、BMR クライアントリストア時のゲートウェイの使用方法を示します。

図 6-5 ゲートウェイの例



この図のクライアントは、デフォルトゲートウェイのみを使用してすべての必要なサーバーと通信することはできません。このような構成の場合、デフォルトゲートウェイを G1 に、マスターサーバーゲートウェイを G2 に、メディアサーバーゲートウェイを G3 に指定する必要があります。

## リストア時のポートの使用

リストア時に、クライアントは特定のサービスおよびポートを通じて、BMR マスター、BMR ブート、および NetBackup プライマリサーバーまたはメディアサーバーと通信します。ブートサーバーがファイアウォールで保護されている場合は、これらのポートを使用して、クライアントサーバーとブートサーバー間の通信を許可する必要があります。

表 6-13 に、リストア時に使用するポートとサービスを示します。

表 6-13 リストア時のポートの使用

サービス	ポート	UNIX の場合	Linux	Windows の場合
bootp/DHCP	67, 68	X	X	X
ping			X	

サービス	ポート	UNIX の場合	Linux	Windows の 場合
lockd	可変	X	X	
mountd	可変	X	X	
nfsd	2049	X	X	
portmapper	111	X	X	
rpcbind		X ( bootparam Solaris のみ)		
statd	可変	X	X	
tftp	69	X	X	X
vnetd	13724	X	X	X
bpcd	13782	X	X	X
Windows ファイル 共有	445			X

# Windows ドライバパッケージの管理

この章では以下の項目について説明しています。

- [Windows ドライバパッケージについて](#)
- [Windows ドライバパッケージの追加](#)
- [Windows ドライバパッケージの削除](#)

## Windows ドライバパッケージについて

Windows パッケージとは、ネットワークインターフェースカード (NIC) ドライバおよび大容量記憶装置デバイス (MSD) ドライバのことです。パッケージは NetBackup マスターサーバーの BMR データベースに格納されています。パッケージプールは、データベースに格納されたパッケージで構成されています。パッケージプールは、リストア構成に追加可能なパッケージの共通プールです。

パッケージは、別のシステムにリストアする際に、リストア構成に追加する必要がある場合があります。[パッケージ (Packages)] ウィンドウに、Dissimilar System Restore に必要なドライバがない場合は、Bare Metal Restore に追加します。SRT を作成した Windows インストールメディアにドライバがある場合は、ドライバをリストア構成に追加しないでください。

Dissimilar System Restore に必要なパッケージが [パッケージ (Packages)] ウィンドウにすでに表示されている場合、リストア構成にそのパッケージを追加します。

p.164 の「[クライアント構成プロパティ](#)」を参照してください。

p.167 の「[\[デバイスおよびドライバ \(Devices & Drivers\)\] プロパティ](#)」を参照してください。

## Windows ドライバパッケージの追加

次の手順でパッケージを追加します。

- 任意の Windows ブートサーバーでドライバパッケージウィザードを使用して、ネットワークインターフェースカード (NIC) ドライバまたは大容量記憶装置デバイス (MSD) ドライバを追加します。
- または、ターゲットシステムに NetBackup クライアントソフトウェアをインストールし、BMR バックアップを実行します。ドライバがそのクライアントの構成に保存され、Dissimilar System Restore の実行時に使用できるようになります。

パッケージを追加する前に、パッケージのインストールファイルを用意する必要があります。ファイルをベンダーの Web サイト、NIC デバイスまたは MSD デバイスに付属のインストールプログラム、または環境内の別の BMR Windows クライアントのいずれかから入手します。

---

**メモ:** 追加できるのは、NIC ドライバと MSD ドライバのみです。他のすべての種類のドライバ (オーディオ、ビデオ、モデムなど) は、リストアの完了後にシステムにインストールする必要があります。

---

p.156 の「[Windows がインストールされている場合の正しいドライバの検索](#)」を参照してください。

ドライバパッケージウィザードを使用してドライバパッケージを追加するには

- 1 Windows ブートサーバーの [スタート]メニューで、[プログラム]、[Cohesity NetBackup]、[Bare Metal Restore ブートサーバーアシスタント (Bare Metal Restore Boot Server Assistant)]の順にクリックします。
- 2 Bare Metal Restore ブートサーバーアシスタントで、[ドライバパッケージウィザード (Driver Package Wizard)]をクリックします。
- 3 [ドライバパッケージウィザード (Driver Package Wizard)]で、プロンプトに従ってソフトウェアパッケージを追加します。
  - パッケージのインストールファイルへのパス
  - パッケージの説明
  - パッケージを使用できる Windows のバージョン
  - パッケージインストールファイルからの特定のドライバ (インストールファイルには、複数のドライバが含まれている場合があります)

## Windows がインストールされている場合の正しいドライバの検索

ドライバ情報ファイル (.inf または txtsetup.oem) には、複数のドライバに関する情報が含まれていることがあります。そのため、大容量記憶装置デバイス (MSD) ドライバまたはネットワークインターフェースカード (NIC) のドライバを追加する際に、複数のオプションから選択する必要がある場合もあります。

デバイスについては、コンピュータに付属のマニュアルで説明されています。説明されていない場合は、ドライバオプションの製造元にお問い合わせください。

または、Windows がインストールされている場合は、次の手順を使用して、ドライバの正しい名前を判別します。

### Windows がインストールされている場合に正しいドライバを検索する方法

- 1 大容量記憶装置デバイスアダプタを含むコンピュータで、Windows の [デバイス マネージャ] を開きます。
- 2 アダプタのカテゴリ (たとえば、[ネットワーク アダプタ]) を展開します。
- 3 ここで表示されるデバイス名を記録しておきます。.inf ファイルでのオプション名は、このデバイス名と同じか、似ている名前になっています。

## Windows ドライバパッケージの削除

ドライバパッケージを削除するには、次の手順を実行します。

---

**警告:** リストアに必要なドライバを削除しないでください。

---

### Windows ドライバパッケージを削除する方法

- 1 NetBackup マスターサーバーの NetBackup Web UI で、[Bare Metal Restore]、[リソース (Resources)]、[パッケージ (Packages)] の順に選択します。
- 2 詳細ペインで、削除するドライバを右クリックします。
- 3 ショートカットメニューから [削除 (Delete)] を選択します。
- 4 確認のパネルで、[はい (Yes)] をクリックします。  
選択したパッケージが削除されます。

# クライアントおよび構成の管理

この章では以下の項目について説明しています。

- [クライアントと構成について](#)
- [構成のコピー](#)
- [構成の検出](#)
- [構成の変更](#)
- [構成の削除](#)
- [クライアントの削除](#)
- [クライアント構成プロパティ](#)

## クライアントと構成について

論理的に、BMRクライアントは構成の集合です。構成は、システムに関する情報の集合で、保護対象のシステムの再構築にテンプレートとして使用されます。

次の情報が含まれています。

- ディスクドライブの数
- ボリューム情報
- ファイルシステム情報
- ネットワークアダプタの数と形式
- ネットワークのプロパティ
- ドライバ

- その他のシステムソフトウェアコンポーネント

BMR の操作の多くは構成上で実行されます。

BMR で保護されたクライアントをバックアップすると、クライアントの構成は **current** という名前で保存されます。クライアントがバックアップされるたびに、以前に保存された構成は新しく保存される構成に置き換えられます。

現在保存されている構成は読み取り専用です。現在の構成は、保護対象のシステムを最新バックアップ (標準またはセルフリストア) 時の状態にリストアする場合に使用します。

別の指定した時点にリストアする場合、または別のディスクやシステム上にリストアする場合は、現在の構成をコピーしてリストア構成を作成します。その後、そのリストア構成を変更します。

## 構成のコピー

次の操作を実行できるように構成をコピーします。

- 最後のバックアップより前のバックアップで保存された状態にクライアントをリストアする。  
p.120 の「[指定した時点へのリストアについて](#)」を参照してください。
- ディスクが変更されたクライアントをリストアする。  
p.123 の「[異なるディスクへのリストアについて](#)」を参照してください。
- Windows クライアントを別のシステムにリストアする。  
p.128 の「[異なるシステムへのリストア](#)」を参照してください。
- クライアントを同じハードウェアに、別のネットワークプロパティでリストアする。

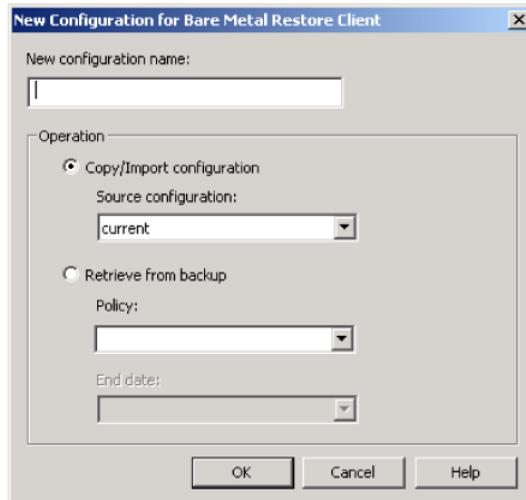
リストア用にコピーした構成をリストア構成と言います。

リストア構成の作成後に、ターゲットハードウェアのプロパティと一致するようにリストア構成を変更します。

構成をコピーするには

- 1 NetBackup Web UI で、[Bare Metal Restore]、[ホスト (Hosts)]、[Bare Metal Restore クライアント (Bare Metal Restore Clients)]の順に選択します。
- 2 [すべての Bare Metal Restore クライアント (All Bare Metal Restore Clients)] ツリーペインで、コピーする構成を含むクライアントのビューを展開します。
- 3 コピーする構成を右クリックします。

- 4 ショートカットメニューから、[新規 (New)]を選択します。



- 5 [Bare Metal Restore クライアントの新しい構成 (New Configuration for Bare Metal Restore Client)]ダイアログボックスで、フィールドに入力します。
- 6 [OK]をクリックします。
- 7 必要であれば構成を修正します。  
p.162 の「[構成の変更](#)」を参照してください。

## 構成の検出

検出準備操作を続行する前に、BMR 用の安全な通信の互換マトリックスを確認します。

p.265 の「[NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換性の表](#)」を参照してください。

新しいシステムの構成を検出することができます。システムが NetBackup クライアントである必要はありません。検出された構成には、ホストのハードウェア情報およびソフトウェア情報が含まれています。

元のマシンとは異なるターゲットシステムにクライアントをリカバリするときには、主にハードウェア検出が必要です。ターゲットシステムは、NIC (ネットワークインターフェースカード) やディスクの詳細など、ハードウェア詳細の元のコンピュータとは異なります。BMR は、リストアが始まる前にそれらの詳細を理解する必要があります。したがって、BMR 検出準備操作を使用して、対象のハードウェアのハードウェア検出を実行し、元のクライアント構成を検出された構成とマッピングする必要があります。

検出された構成は、BMRによって専用のプールに追加されます。これによって、Dissimilar Disk Restore などの処理を実行する場合に、構成の要素（ディスクのレイアウトなど）を使用できるようになります。

検出処理が終了すると、クライアントでは次の変更が表示され、構成が[検出された構成 (Discovered Configurations)]ビューに表示されます。

- AIX クライアントでは LED 画面に B55 と表示されます。
- HP-UX、Linux および Solaris クライアントでは、次のメッセージが表示されます。  
The Bare Metal Restore hardware discovery boot has concluded.
- Windows クライアントでは検出が終了したことと[OK]をクリックするとシステムを再起動できることを示すポップアップボックスが表示されます。

コマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください

[https://www.veritas.com/support/en\\_US/article.DOC5332](https://www.veritas.com/support/en_US/article.DOC5332)

自動リカバリまたは検出とホスト ID ベースの証明書について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

#### bmrprep コマンドを使用して構成を検出する方法

- 1 管理者としてログオンします。
- 2 bpnbat コマンドを実行します。
- 3 bmrprep コマンドを実行して、検出準備操作を開始します。

bmrprep コマンドを実行すると、検証チェックが実行されます。これらのチェックは、SRT のバージョン、構成バージョンなどのさまざまなパラメータに関係します。

- 検出準備のための検証チェックが正常に実行された場合、クライアントは自動検出のマークが付けられます。この自動検出は、デフォルトでは 48 時間有効です。プライマリサーバーの真正性は自動的に検証され、ホスト ID ベースの証明書は自動検出処理中にこのクライアントに対して自動的に発行されます。  
nbhostmgmt コマンドを使用して、クライアントに自動検出のマークが付いているかどうかを確認します。
- 検証チェックが失敗した場合は、適切なエラーメッセージが表示されます。メッセージに示される手順に従います。

詳しくは、p.213 の「リストア準備および検出準備のエラーメッセージと、BMR 用の安全な通信に関連する bmrprep コマンド」を参照してください。を参照してください。

クライアントは検出の準備ができています。

## NetBackup Web UI を使用して構成を検出する方法

- 1 左側の[Bare Metal Restore]、[Host (Hosts)]、[Bare Metal Restore クライアント (Bare Metal Restore clients)]の順に選択します
- 2 フィールドに入力し、必要に応じてデータを入力します。  
[Host (Host)]、[Bare Metal Restore クライアント (Bare Metal Restore Clients)]ビューでクライアントを選択すると、そのクライアントの値がダイアログボックスに表示されます。

---

**メモ:** クライアントが DDR (Dissimilar Disk Restore) の対象であり、保護対象のクライアントのディスクが VxVM で管理されている場合は、VxVM がインストールされている SRT を指定します。

---

- 3 [OK]をクリックします。  
[検出準備 (Prepare to Discover)]をクリックすると、検証チェックが実行されます。これらのチェックは、SRT のバージョン、構成バージョンなどのさまざまなパラメータに関係します。
  - 検証チェックが正常に実行された場合、クライアントは自動検出のマークが付けられます。この自動検出は、デフォルトでは 48 時間有効です。プライマリサーバーの真正性は自動的に検証され、Host ID ベースの証明書は自動検出処理中にこのクライアントに対して自動的に発行されます。  
クライアントは検出の準備ができています。  
nbhostmgmt コマンドを使用して、クライアントに自動検出のマークが付いているかどうかを確認します。  
自動リカバリまたは検出と Host ID ベースの証明書について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。
  - 検証チェックが失敗した場合は、適切なエラーメッセージが表示されます。メッセージに示される手順に従います。  
詳しくは、p.213 の「リストア準備および検出準備のエラーメッセージと、BMR 用の安全な通信に関連する bmrprep コマンド」を参照してください。を参照してください。
- 4 クライアントをブートして、ハードウェア検出処理を開始します。  
メディアブートを使用した場合は、BMR でクライアント名を入力するように求められます。検出準備処理の[タスク (Tasks)]ビューに表示されているクライアント名を入力する必要があります。  
ターゲットシステムの検出が自動的に行われて、検出が完了すると通知を受信します。検出操作が正常に完了すると、[Bare Metal Restore 管理 (Metal Restore Management)]、[リソース (Resources)]、[検出された構成 (Discovered Configurations)]メニューの下で指定された名前の検出済み構成を参照できます。

---

**メモ:** 検出操作を停止する、または検出操作が失敗した場合は、検出準備操作を再度実行して自動検出を再開するか、NetBackup Web UI またはコマンドラインインターフェースを使用して[セキュリティ (Security)]、[ホストマッピング (Host mappings)]、[ホスト (Hosts)]、メニューボタン、[証明書の自動再発行を許可する (Allow auto reissue certificate)] オプションを手動で設定します。

[証明書の自動再発行を許可する (Allow Auto Reissue Certificate)] オプションの手動設定について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「証明書の自動再発行の許可」セクションを参照してください

[https://www.veritas.com/support/ja\\_JP/article.DOC5332](https://www.veritas.com/support/ja_JP/article.DOC5332)

---

## 構成の変更

次の操作を実行できるように構成を変更します。

- 最後のバックアップより前のバックアップで保存された状態にクライアントをリストアする。  
p.120 の「[指定した時点へのリストアについて](#)」を参照してください。
- ディスクが変更されたクライアントをリストアする。  
p.123 の「[異なるディスクへのリストアについて](#)」を参照してください。
- Windows クライアントを別のシステムにリストアする。  
p.128 の「[異なるシステムへのリストア](#)」を参照してください。
- クライアントを同じハードウェアに、別のネットワークプロパティでリストアする。
- 目的の非 OS データボリュームまたはディスクをスキップして、クライアントをリストアする。
- SAN LUN に OS ボリュームをマッピングして、クライアント SAN をブート可能にする。

current という名前の構成は変更できません。編集可能な構成を作成する必要があります。

p.158 の「[構成のコピー](#)」を参照してください。

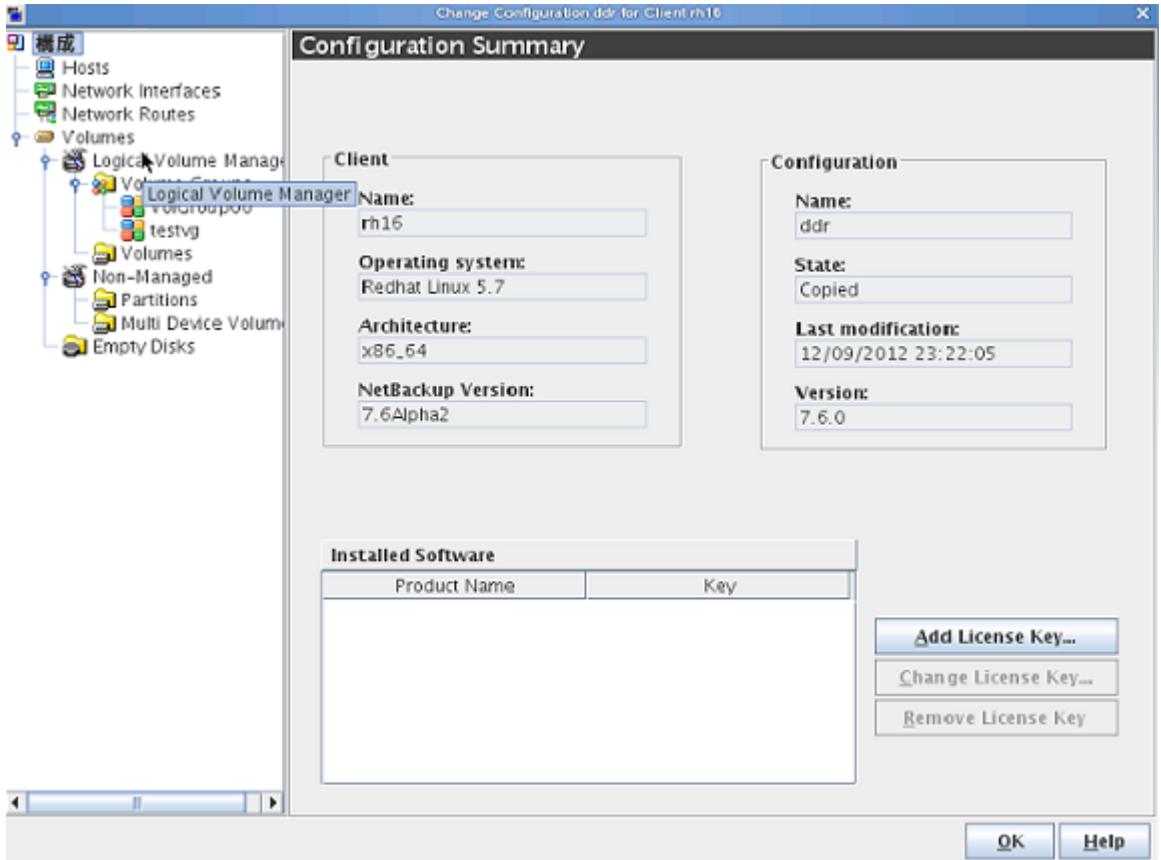
構成を変更するには

- 1 NetBackup Web UI で、[Bare Metal Restore]、[ホスト (Hosts)]、[Bare Metal Restore クライアント (Bare Metal Restore Clients)] の順に選択します。
- 2 [すべての Bare Metal Restore クライアント (All Bare Metal Restore Clients)] ペインで、変更する構成を含むクライアントのビューを展開します。
- 3 変更する構成を右クリックします。

- 4 ショートカットメニューから、[変更 (Change)]を選択します。
- 5 [構成の変更をする (Change Configuration)]ダイアログボックスで、必要に応じてプロパティを変更します。

p.164 の「クライアント構成プロパティ」を参照してください。

図 8-1 [構成の変更 (Change Configuration)]ダイアログボックス



## 構成の削除

読み取り専用であるため現在の構成は削除できません。カスタム作成された構成のみ削除できます。

構成を削除するには

- 1 NetBackup Web UI で、[Bare Metal Restore]、[ホスト (Hosts)]、[Bare Metal Restore クライアント (Bare Metal Restore Clients)]の順に選択します。
- 2 [すべての Bare Metal Restore クライアント (All Clients)]ペインで、削除する構成を含むクライアントのビューを展開します。
- 3 削除する構成を右クリックします。
- 4 [削除 (Delete)]、[はい (Yes)]の順に選択します。

## クライアントの削除

クライアントを削除すると、BMR データベースからクライアントとその BMR 構成のみが削除されます。クライアント上の NetBackup ソフトウェアの削除、NetBackup からのクライアントの削除、またはクライアントのバックアップの削除は行われません。

クライアントを削除することはできますが、クライアントをバックアップする NetBackup ポリシーからは削除できません。この場合、次のバックアップ時にそのクライアントが BMR に再登録され、[Bare Metal Restore クライアント (Bare Metal Restore Clients)]ビューに表示されます(クライアントをバックアップする NetBackup ポリシーは、BMR 情報を収集するポリシーです)。

クライアントを削除するには

- 1 NetBackup Web UI で、[Bare Metal Restore]、[ホスト (Hosts)]、[Bare Metal Restore クライアント (Bare Metal Restore Clients)]の順に選択します。
- 2 削除するクライアントを右クリックします。
- 3 ショートカットメニューから、[削除 (Delete)]を選択します。
- 4 確認のダイアログボックスで、[はい (Yes)]をクリックします。

## クライアント構成プロパティ

[構成の変更 (Change Configuration)]ダイアログボックスを使用して、保護対象のシステムにおけるクライアント構成の属性をリストア構成にマッピングします。構成をマッピングすると、指定した時点へのリストア、Dissimilar Disk Restore または Dissimilar System Restore が有効になります。

[構成の変更 (Change Configuration)]ダイアログボックスは複数のプロパティシートを含んでいます。

p.165 の「[構成の概略 プロパティ](#)」を参照してください。

p.167 の「[\[デバイスおよびドライバ \(Devices & Drivers\)\]プロパティ](#)」を参照してください。

p.170 の「[ホスト (Hosts)]プロパティ」を参照してください。

p.172 の「[ネットワークインターフェース (Network Interfaces)]プロパティ」を参照してください。

p.177 の「[ネットワークルート (Network Routes)]プロパティ」を参照してください。

p.178 の「[ボリューム (Volumes)]プロパティについて」を参照してください。

## 構成の概略 プロパティ

[構成の変更 (Change Configuration)]ダイアログボックスの [構成の概略 (Configuration Summary)]プロパティシートを使用して、次の処理を実行します。

- 構成の概略を表示する
- 保護対象のシステム上のライセンスキーが必要なソフトウェアのライセンスキーを変更する
- リストアに適したソフトウェアを含む共有リソースツリーを選択できるように、リストア構成のコンポーネントを判断する

図 8-2 構成の概略

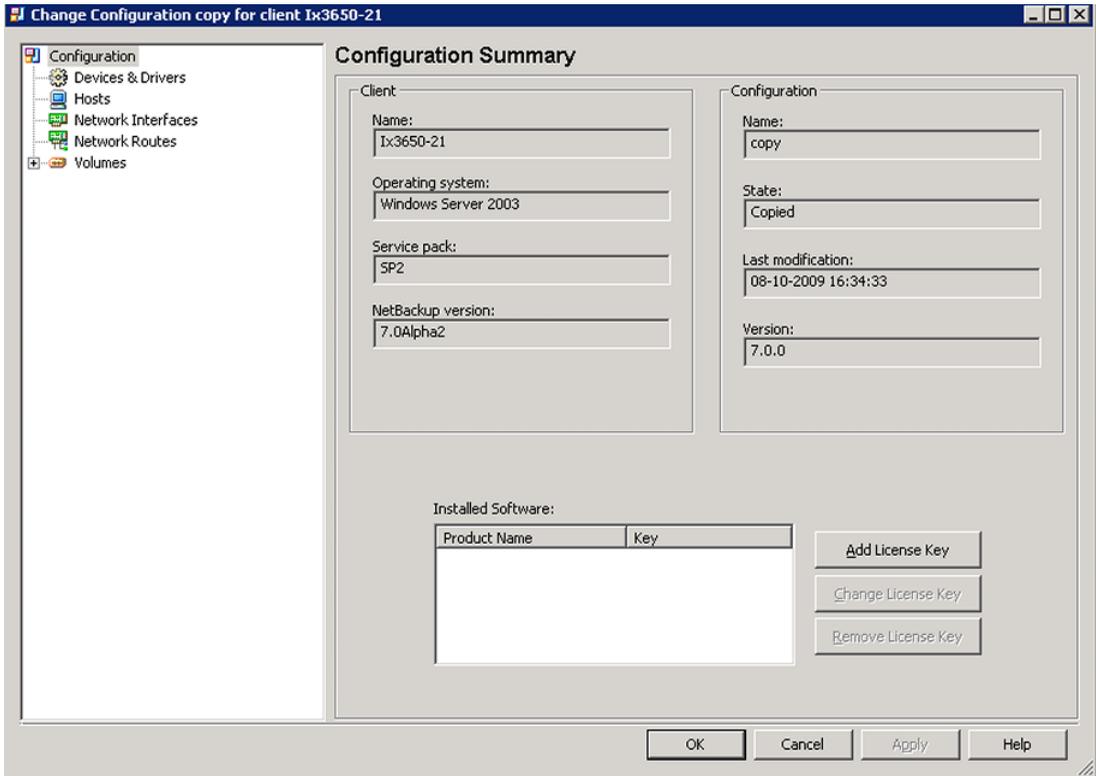


表 8-1に、ライセンスキーに関して開始できる処理を示します。

表 8-1 ライセンスキーの処理

処理	説明
ライセンスキーを追加する	選択したソフトウェアのライセンスキーを追加するためのダイアログボックスを開きます。
ライセンスキーを変更する	選択したソフトウェアのライセンスキーを変更するためのダイアログボックスを開きます。
ライセンスキーを削除する	選択したライセンスキーを削除します。

表 8-2に、ダイアログボックスに表示されるクライアントフィールドを示します。

表 8-2 クライアントの項目

フィールド	説明
名前 (Name)	クライアントの名前。
オペレーティングシステム (Operating system)	クライアントのオペレーティングシステム。
Service Pack	(Windows クライアントのみ) クライアントの Service Pack のバージョン。
アーキテクチャ (Architecture)	(UNIX および Linux クライアントのみ) クライアントのアーキテクチャ。
NetBackup バージョン (NetBackup version)	クライアントの NetBackup ソフトウェアのバージョン。
Veritas Volume Manager のバージョン (Veritas Volume Manager Version)	Arctera Volume Manager または Storage Foundation for Windows (存在する場合) のバージョン。

表 8-3に、ダイアログボックスに表示される構成フィールドを示します。

表 8-3 構成フィールド

フィールド	説明
名前 (Name)	構成の名前。
状態 (State)	構成の状態。[保存済み (Saved)]の場合は構成を編集できません。[コピー済み (Copied)]の場合は構成を編集できます。
前回の変更 (Last modification)	構成が最後に変更された日付および時刻。
バージョン (Version)	構成のバージョン。

## [デバイスおよびドライバ (Devices & Drivers)] プロパティ

この項は、Windows オペレーティングシステムの場合にのみ該当します。

[デバイスおよびドライバ (Devices & Drivers)] プロパティシートは Microsoft Windows クライアントにのみ適用されます。Windows クライアントが元のシステムとは異なるハードウェアにリストアされ、リストア先のハードウェアの大容量記憶装置デバイス (MSD) のドライバやネットワークインターフェースカード (NIC) が異なる場合には、デバイスドライバマッピングの変更が必要です。

[構成の変更 (Change Configuration)] ダイアログボックスの [デバイスおよびドライバ (Devices & Drivers)] プロパティシートを使用して、次の処理を実行します。

- この構成内のデバイスを、検出された新しいハードウェア構成または別のクライアントの構成を使用して初期化します。
- リストに示されているデバイスに対応する正しい大容量記憶装置デバイス (MSD) ドライバおよびネットワークインターフェースカード (NIC) ドライバを自動的に選択します。
- 構成に MSD と NIC ドライバを手動で追加します。

また、BMR で検出されたドライバだけを使用するかどうかを指定できます。

図 8-3 [デバイスおよびドライバ (Devices & Drivers)] ダイアログボックス

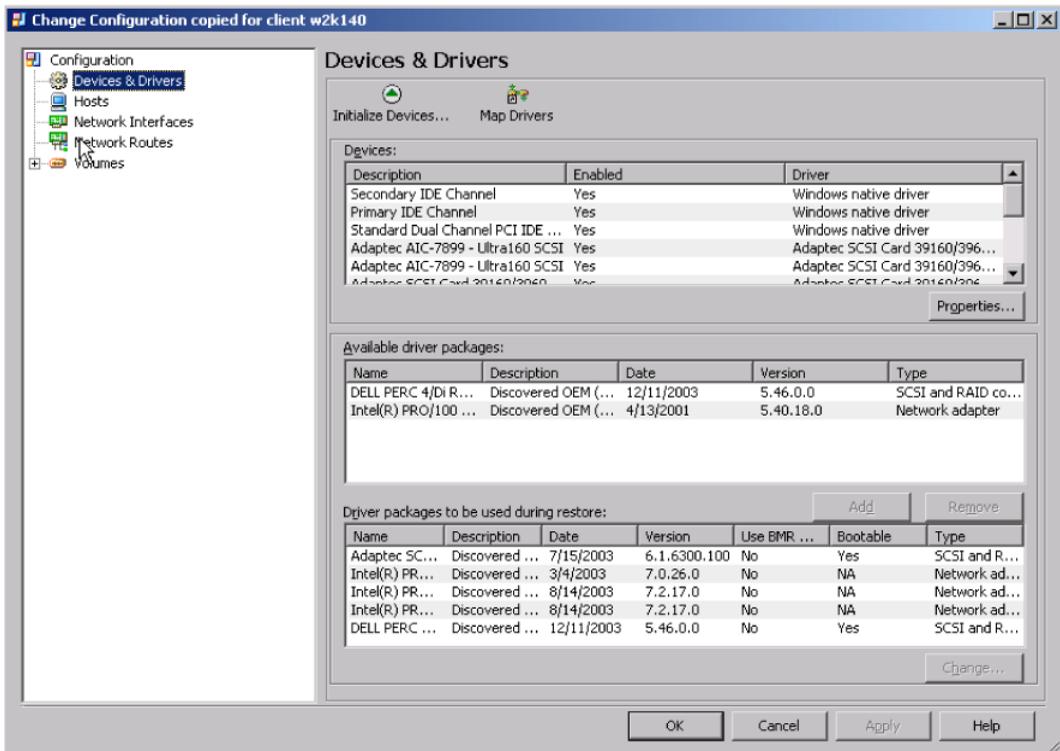


表 8-4に、利用可能なオプションおよびそれらのオプションによって開始される処理を示します。

表 8-4 [デバイスおよびドライバ (Devices & Drivers)] オプション

オプション	処理
デバイスの初期化 (Initialize Devices)	デバイスのインポート元となる他の構成を指定するプロンプトが表示されます。検出された構成を選択するか、または他のクライアントから選択できます。初期化処理によって [リストアで使用するドライバパッケージ (Driver packages to be used during restore)] ウィンドウが更新され、このハードウェアに必要なドライバが含まれるようになります。
ドライバのマッピング (Map Drivers)	<p>ドライバのないデバイスに対して、ドライバを自動的に割り当てます。最後の初期化処理後にドライバが BMR に追加された場合は、この操作を繰り返してください。[追加 (Add)] オプションを使って特定のドライバを手動で選択し、自動選択されたドライバを上書きすることが有効である場合があります。</p> <p>ドライバのないデバイスは、[デバイス (Devices)] ウィンドウの [有効 (Enabled)] 列に [一致するドライバが見つかりません (No matching driver)] と示されます。これらのデバイスは、リストア時に利用できません。</p>
追加 (Add)	選択したドライバを [利用可能なドライバパッケージ (Available driver packages)] ウィンドウから [リストアで使用するドライバパッケージ (Driver packages to be used during restore)] ウィンドウに移動します。
削除 (Remove)	選択したドライバを [リストアで使用するドライバパッケージ (Driver packages to be used during restore)] ウィンドウから [利用可能なドライバパッケージ (Available driver packages)] ウィンドウに移動します
変更 (Change)	<p>選択したドライバの次の属性を変更できます。</p> <ul style="list-style-type: none"> <li>■ [Windows で提供されるドライバまたはより新しいドライバの代わりにこのドライバを強制的にインストールする (Force installation of this driver instead of Windows supplied or newer driver)] チェックボックスは選択されたドライバが強制的に使用されるかどうかを制御します。</li> <li>■ MSD ドライバの場合には、[インストールのテキストモードの部分で使用するブート可能ドライバ (Bootable driver to be used during text mode portion of the installation)] オプションは、Windows レガシーリストア方式のみに適用されます。Windows レガシーリストアのインストールの段階でこのドライバが使用されるかを判断します。Windows Fast Restore には影響しません。</li> </ul>

## Windows 提供または最新のドライバの代わりにこのドライバのインストールを強制する

BMR が保護対象のシステムからサードパーティドライバを保存した場合に、ドライバの署名が失われます。(サードパーティドライバとは、Windows で配布されていないドライバで

す) 保護対象のシステムからのドライバには署名がないため、BMR リストア中に、インストール処理で標準のドライバが一時的な修復環境にインストールされます。

標準の Windows ドライバではなく、検出されたドライバを一時修復環境に強制インストールするように、構成を編集できます。このオプションは特定のドライババージョンを選択する際にも有用です。

#### 検出されたドライバをリストア時に使用する方法

- 1 [デバイスおよびドライバ (Devices & Drivers)] プロパティシートで、ウィンドウ下部のドライバリストから目的のドライバを選択し、[変更 (Change)] をクリックします。
- 2 [Windows で提供されるドライバまたはより新しいドライバの代わりにこのドライバを強制的にインストールする (Force installation of this driver instead of Windows supplied or newer driver)] チェックボックスにチェックマークを付けます。
- 3 [OK] をクリックします。

## [ホスト (Hosts)] プロパティ

[構成の変更 (Change Configuration)] ダイアログボックスの [ホスト (Hosts)] プロパティシートを使用して、リストア処理に関与するすべてのホストの属性を追加、削除または変更します。

別の構成を含むネットワーク (ディザスタリカバリサイトなど) にリストアできるように、属性を変更できます。

図 8-4 [ホスト (Hosts)] プロパティシート

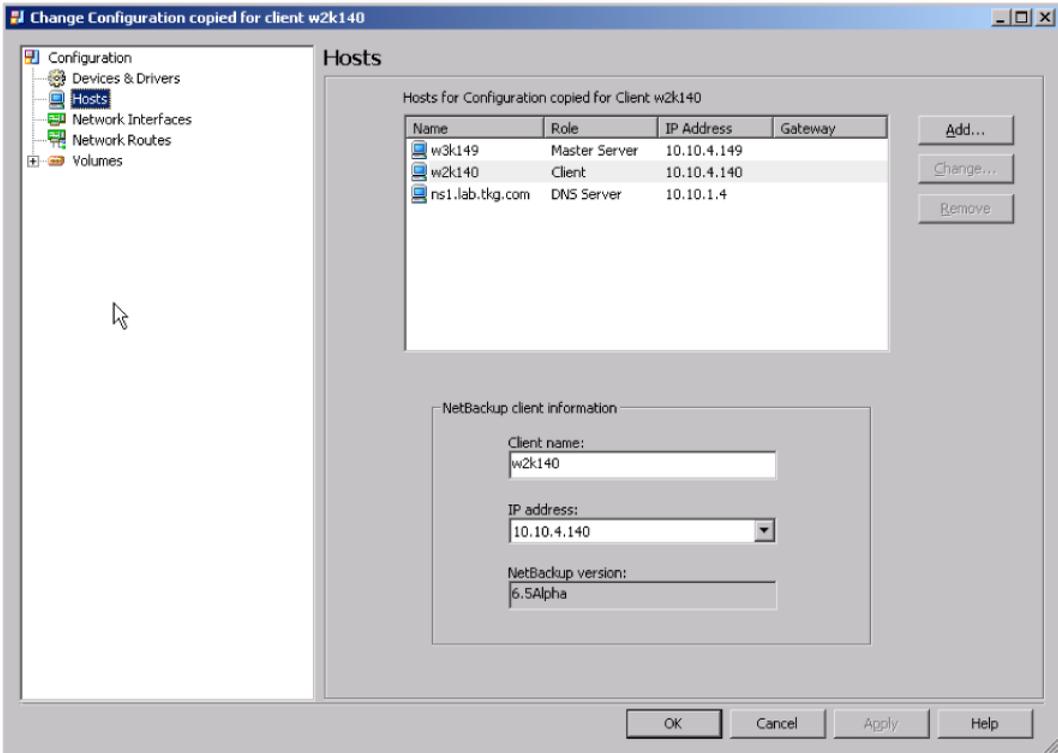


表 8-5に、このプロパティシートから開始できる処理を示します。

表 8-5 ホストのマッピング処理

処理	説明
追加 (Add)	新しいホストを追加し、その役割を指定し、その IP アドレスおよびゲートウェイを入力できるダイアログボックスを開きます。
変更 (Change)	選択したホストのプロパティを変更できるダイアログボックスを開きます。
削除 (Remove)	選択したホストを削除します。ホストを削除しない場合は、[キャンセル (Cancel)]をクリックして、変更を適用せずに、[構成の変更 (Change Configuration)]ダイアログボックスを閉じます。

表 8-6プロパティシートの[クライアント情報 (Client Information)]フィールドを示します。

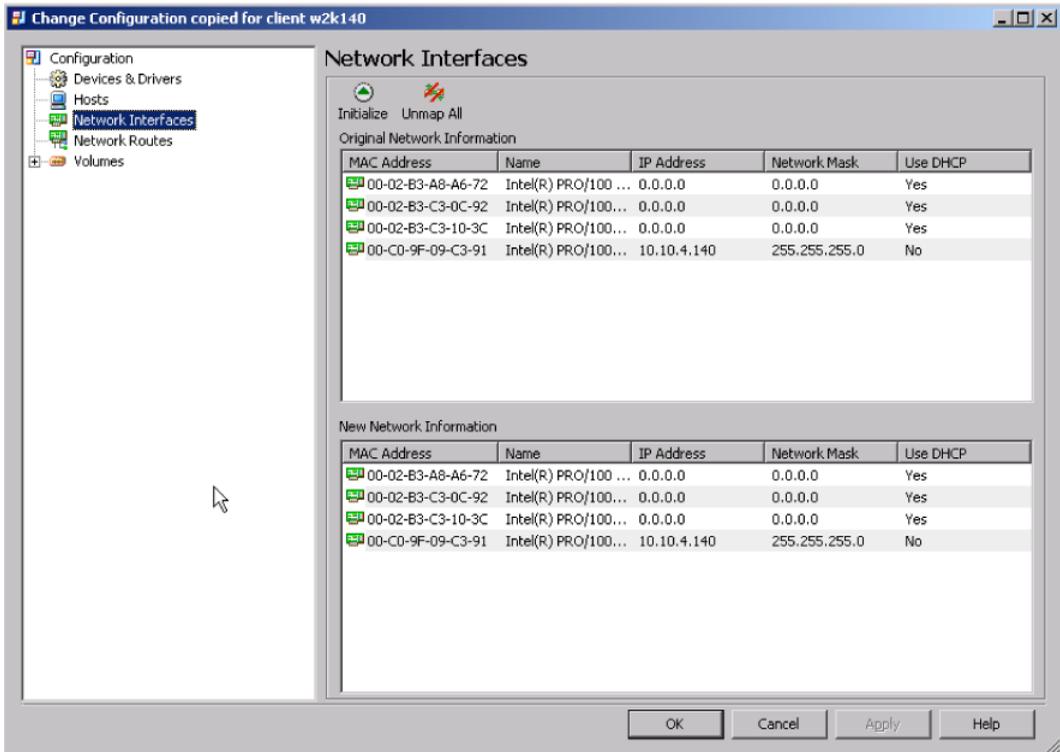
表 8-6 [ホスト (Hosts)]ダイアログボックスの NetBackup クライアント情報のフィールド

フィールド	説明
クライアント名 (Client Name)	NetBackup がクライアントを識別するための名前。指定するクライアント名は、クライアントをバックアップする NetBackup ポリシーのクライアント名と一致している必要があります。
IP アドレス (IP address)	クライアントの IP アドレス。ネットワークインターフェースで定義されたすべての IP アドレスがドロップダウンメニューに表示されます。
NetBackup バージョン (NetBackup version)	クライアントの NetBackup ソフトウェアのバージョン。

## [ネットワークインターフェース (Network Interfaces)]プロパティ

[構成の変更 (Change Configuration)]ダイアログボックスの [ネットワークインターフェース (Network Interfaces)]プロパティシートを使用して、インターフェースを追加または削除したり、インターフェースに関連付けられたネットワーク識別情報を変更します。

図 8-5 [ネットワークインターフェース (Network Interfaces)] プロパティシート



[元のネットワーク情報 (Original Network Information)]は読み取り専用です。[新しいネットワーク情報 (New Network Information)]にはリストアに使用する値が表示されます。構成が編集されていない場合は、上部ペインと下部ペインに同じ情報が表示されます。

表 8-7 のマッピング処理に、このダイアログボックスから開始できる処理を示します。

表 8-7 ネットワークインターフェースのマッピング処理

処理	説明
初期化 (Initialize)	インポートする構成を選択できるダイアログボックスを開きます。構成のハードウェア情報のみがインポートされ、ネットワーク識別情報はインポートされません。インポートされた構成のインターフェースで[新しいネットワーク情報 (New Network Information)]ウィンドウのインターフェースを置き換えます。

処理	説明
すべてをマッピング解除 (Unmap All)	<p>[新しいネットワーク情報 (New Network Information)] ウィンドウにあるすべてのマッピング済みインターフェースのマッピングを解除し、[元のネットワーク情報 (Original Network Information)] ウィンドウにあるすべてのインターフェースを[未マッピング (Unmapped)]に変更します。</p> <p>マッピング解除により、名前、IP アドレス、サブネットマスク、ゲートウェイ、DHCP 属性およびブート可能属性が削除されます。MAC アドレスは削除されません。</p>
マッピング (Map)	<p>[元のネットワーク情報 (Original Network Information)] ウィンドウでインターフェースを右クリックして、ショートカットメニューから[マッピング (Map)]を選択します。[マップインターフェース (Map Interface)] ダイアログボックスで、IP アドレス、ネットマスクおよびドメイン名をソースネットワークカードからマッピングするインターフェースを選択します。元のインターフェースの MAC アドレスは、選択したインターフェースにマッピングされません。</p>
マッピング解除 (Unmap)	<p>[新しいネットワーク情報 (New Network Information)] ウィンドウでインターフェースを右クリックし、ショートカットメニューから[マッピング解除 (Unmap)]を選択します。</p> <p>インターフェースのマッピング解除により、名前、IP アドレス、サブネットマスク、DHCP 属性およびブート可能属性が削除されます。MAC アドレスは削除されません。</p>
変更 (Change)	<p>[新しいネットワーク情報 (New Network Information)] ウィンドウでインターフェースを右クリックし、ショートカットメニューから[変更 (Change)]を選択します。</p>

## ネットワークインターフェースのインポートおよびマッピング

異なるシステムにリストアしているときに、ターゲットシステムをバックアップしてその構成を保存した場合は、次の操作を実行できます。

- ターゲットシステムのネットワークインターフェースカード (NIC) 情報をリストア構成にインポートする。
- 元の構成の NIC のネットワーク識別情報をリストア構成の NIC にマッピングする。

### インターフェースをインポートしてマッピングする方法

- 1 [初期化 (Initialize)] をクリックします。
- 2 [インポートの構成 (Import Configuration)] ダイアログボックスで、インポートするクライアント構成を選択します。

- 3 [OK]をクリックします。

ネットワークハードウェア情報が[新しいネットワーク情報 (New Network Information)] ウィンドウにインポートされ、既存のインターフェースと置き換わります。ネットワーク識別情報 (IP やルートなど) はインポートされません。
- 4 [元のネットワーク情報 (Original Network Information)] ウィンドウでインターフェースを右クリックして、ショートカットメニューから[マッピング (Map)]を選択します。
- 5 [マップインターフェース (Map Interface)]または[変更インターフェース (Change Interface)]ダイアログボックスで、[インターフェースへのマッピング (Map to Interface)] ドロップダウンメニューからインターフェースを選択します。
- 6 [OK]をクリックします。

IP アドレス、ネットマスクおよび完全修飾ドメイン名がリストアされたシステムのインターフェースに適用されます。

## 手動によるネットワークインターフェースの変更

異なるシステムにリストアするときに、ターゲットシステムの構成を検出または保存していない場合は、リストア用に元の構成インターフェースプロパティを手動で変更できます。

まず、ターゲットシステムの NIC の MAC アドレスを確認する必要があります。

### 手動でインターフェースを変更する方法

- 1 [新しいネットワーク情報 (New Network Information)] ウィンドウでインターフェースを右クリックし、ショートカットメニューから[変更 (Change)]を選択します。
- 2 [マップインターフェース (Map Interface)]または[変更インターフェース (Change Interface)]ダイアログボックスで、[DHCP を使用する (Use DHCP)]を選択します (DHCP を使用する場合)。この処理ではインターフェースを変更しているため、ダイアログボックスには[ハードウェア MAC アドレス (Hardware MAC Address)]フィールドが表示されます。

手順 5 に進みます。
- 3 [ネットワークインターフェースの属性 (Attributes for Network Interface)] ウィンドウで属性の行を選択し、[変更 (Change)]をクリックします。
- 4 [ネットワーク識別情報の追加 (Add Network Identity)]ダイアログボックスで、保護対象のシステムのインターフェースの IP アドレス、ネットマスクおよび完全修飾ドメイン名を入力します。

次に[OK]をクリックします。
- 5 ターゲットシステムの NIC のハードウェア MAC アドレスを入力します。
- 6 [OK]をクリックします。

MAC アドレスおよびネットワーク識別情報が変更されます。インターフェースの名前は変わりませんが、リストアには影響しません。

## UNIX および Linux のブートインターフェースの指定

UNIX および Linux クライアントでは、ブートからリストアまで、1 つのネットワークインターフェースを使用する必要があります。[ネットワークインターフェース (Network Interfaces)] ダイアログボックスの[ブート可能 (Bootable)]列には、ブートインターフェースとして構成されているインターフェースが表示されます。リストア構成に複数のネットワークインターフェースが含まれる場合は、リストアに使用するインターフェースを指定できます。

表 8-8は、適切なインターフェースの判断に役立ちます。

表 8-8 [ネットワークインターフェース (Network Interfaces)]の[ブート可能 (Bootable)]列

プラットフォームまたはハードウェアの種類	ブート可能なネットワークインターフェース
AIX	統合イーサネット、イーサネットカードまたはトークンリング。 AIX 上のネットワークインターフェースについては、次の点に注意してください。 <ul style="list-style-type: none"><li>■ CHRP ハードウェアのみサポートされます。</li><li>■ ネットワークアダプタから RS/6000 をブートする場合は、システムのファームウェアでサポートされている必要があります。</li></ul>
HP-UX	統合イーサネットのみ。
Linux	すべてのイーサネットデバイス。
Solaris	すべてのイーサネットデバイス。

### UNIX および Linux のブートインターフェースを指定する方法

- 1 [ネットワークインターフェース (Network Interfaces)]プロパティシートの[新しいネットワーク情報 (New Network Information)]ウィンドウで、ブートインターフェースとして使用するインターフェースを右クリックします。
- 2 ショートカットメニューから[変更 (Change)]を選択します。
- 3 [マップインターフェース (Map Interface)]または[変更インターフェース (Change Interface)]ダイアログボックスで、[ブート可能 (Bootable)]をクリックします。
- 4 [OK]をクリックします。

---

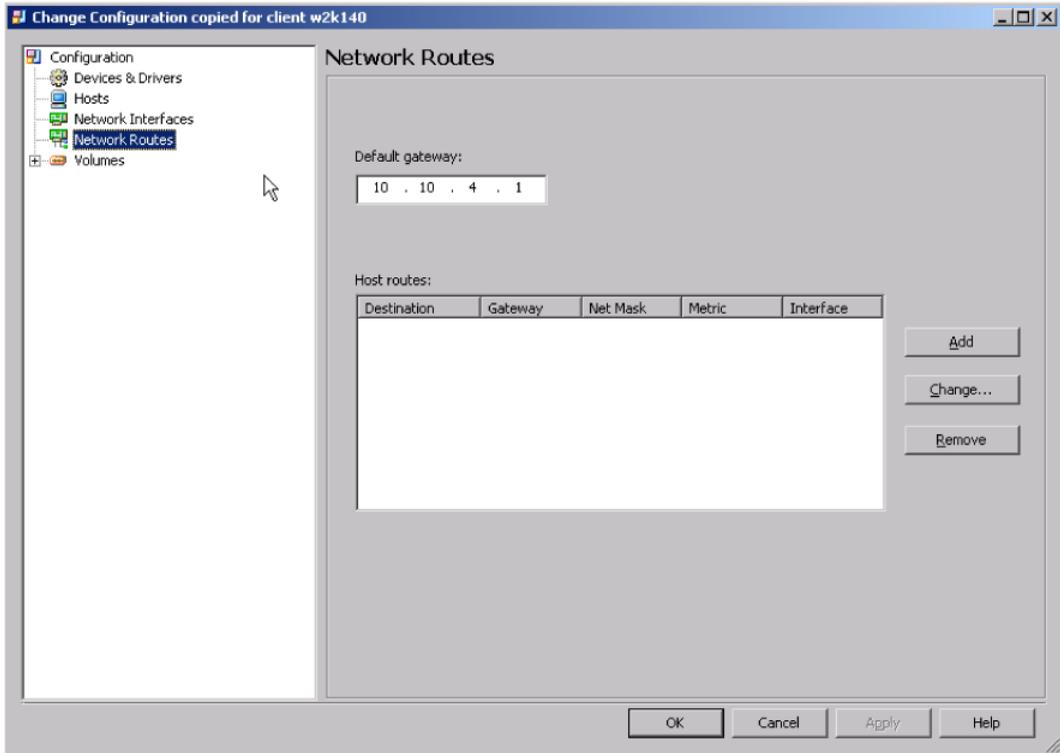
**メモ:** BMR クライアント構成でブート可能として表示されているものとは異なるリカバリ用ネットワークインターフェースを使用して対象のハードウェアがブートされる場合には、リカバリが失敗することがあります。

---

## [ネットワークルート (Network Routes)] プロパティ

[構成の変更 (Change Configuration)] ダイアログボックスの [ネットワークルート (Network Routes)] プロパティシートを使用して、リストア時に使用するネットワークルートを追加します。

図 8-6 [ネットワークルート (Network Routes)] プロパティシート



構成内の既存のルートで **NetBackup** サーバーまたは **BMR** サーバーにアクセスできない場合、ルートを追加する必要があります。これは、異なる場所でディザスタリカバリを実行中に、サブネット間でサーバーを移動する場合に実行する必要があります。また、介在するルーターが変更された場合にも実行する必要があります。

たとえば、クライアント **10.10.5.12** と **NetBackup** マスターサーバー **10.10.6.23** とが異なるサブネットにあり、両者間にルーター (**10.10.5.254**) があるとします。リストア準備時に、リストア処理で **NetBackup** マスターサーバーへのルートが **10.10.5.254** として構成され、リストアは正常に行われるようになります。しかし、両者間のルーターの IP アドレスが変更されると、クライアントはマスターサーバーにアクセスできなくなる場合があります。マスターサーバーへの正しいルートが構成に含まれなくなるため、クライアントはサーバー

にアクセスできません。そのため、リストア準備処理を実行する前に、マスターサーバーにネットワークルートを追加する必要があります。

BMR は、次の順序でホストへのアクセスを試行します。

- ホストルート ([ホスト (Hosts)]プロパティシートで指定したもの)
- このプロパティシートで指定したネットワークルート
- このプロパティシートで指定したデフォルトのルート

表 8-9に、プロパティシートのフィールドとオプションを示します。

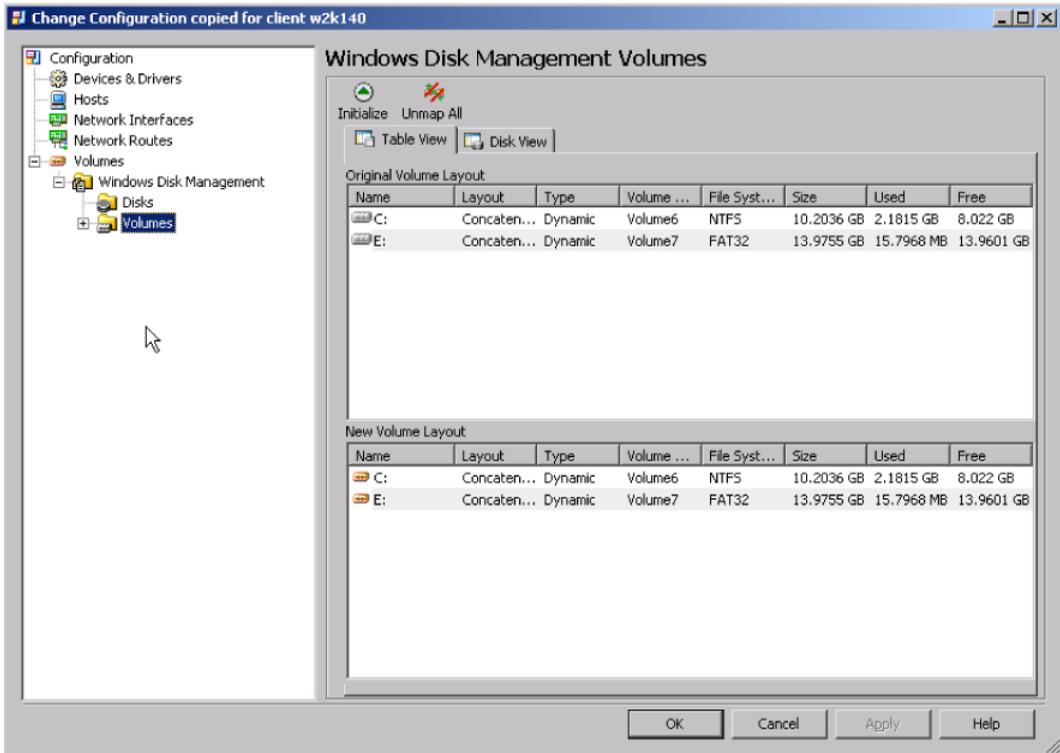
表 8-9 ネットワークルートのマッピングフィールド

処理	説明
デフォルトゲートウェイ (Default gateway)	ホストにアクセスするルートが他にない場合に使用するゲートウェイ。
追加 (Add)	新しいネットワークルートのプロパティを入力できるダイアログボックスが表示されます。
変更 (Change)	選択したルートのプロパティを変更できるダイアログボックスを開きます。
削除 (Remove)	選択したルートを削除します。

## [ボリューム (Volumes)]プロパティについて

[構成の変更 (Change Configuration)]ダイアログボックスの[ボリューム (Volumes)]プロパティシートを使用して、ボリューム構成を保護対象のクライアントからリストア構成の新しいディスクにマッピングします。

図 8-7 [ボリューム (Volumes)] プロパティシート



次のボリュームマッピング操作と構成変更操作を実行できます。

- ディスクグループを作成するディスクを変更する
- リストアするファイルシステムを制御する
- 作成する論理ボリュームを制御する
- ファイルシステム、論理ボリュームまたはディスクの属性を変更する
- マッピングのターゲットとして使用されないようにディスクを制限する
- 検出されたディスクをマッピングできるようにする (制限の削除)

ターゲットディスクに十分な領域があれば、すべての論理ボリュームとそのファイルシステムをマッピングできます。また、特定の論理ボリュームやファイルシステムをマッピングすることもできます。すべての論理ボリュームとファイルシステムをリストアする必要はありません。

プライマリパーティションとシンプルボリュームで必要なディスクは 1 つだけです。ストライプボリューム、ミラーボリュームおよび RAID-5 ボリュームでは複数のディスクが必要です。

## ネイティブディスクオブジェクトについて

この項は、UNIX システムの場合にのみ該当します。

新しい[ネイティブディスク (Native Disk)]ノードは[構成の変更 (Change Configuration)]ダイアログボックスの[ボリューム (Volumes)]ノードの下に表示されます。次の例は、利用可能なネイティブディスクについての情報 (合計サイズ、使用領域と空き領域) を示します。

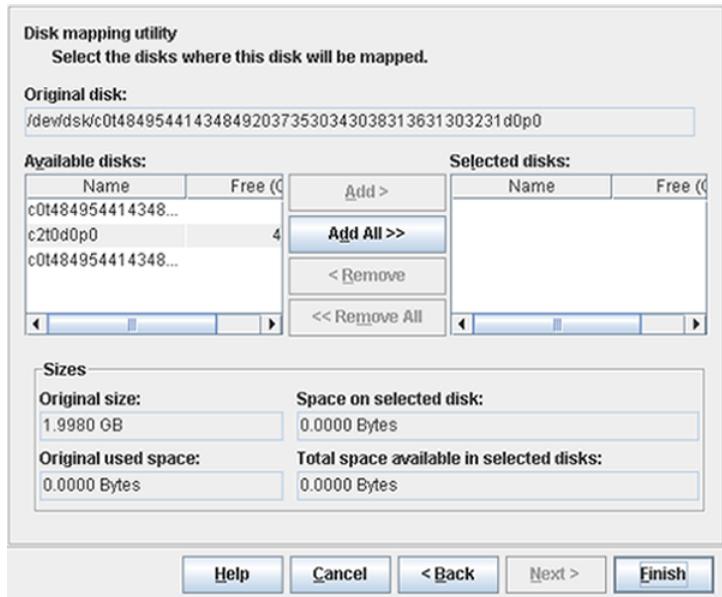
The screenshot shows the 'Native Disks' configuration window. The left sidebar shows a tree view with 'Native Disks' selected. The main area displays two tables: 'Original Volume Layout for Client' and 'New Volume Layout for Client'. Both tables list disk names, sizes (1.9961 GB), used space (0.0000 Bytes), and free space (1.9961 GB). The 'New Volume Layout' table is currently empty.

Name	Size	Used	Free Space
/dev/dsk/kc0t4849544...	1.9961 GB	0.0000 Bytes	1.9961 GB
/dev/dsk/kc0t4849544...	1.9961 GB	0.0000 Bytes	1.9961 GB
/dev/dsk/kc0t4849544...	1.9961 GB	0.0000 Bytes	1.9961 GB
/dev/dsk/kc0t4849544...	1.9961 GB	0.0000 Bytes	1.9961 GB
/dev/dsk/kc0t4849544...	1.9961 GB	0.0000 Bytes	1.9961 GB
/dev/dsk/kc0t4849544...	1.9961 GB	1.9961 GB	0.0000 Bytes
/dev/dsk/kc0t4849544...	1.9961 GB	1.9961 GB	0.0000 Bytes
/dev/dsk/kc0t4849544...	1.9961 GB	1.9961 GB	0.0000 Bytes
/dev/dsk/r0t4849544...	1.9961 GB	1.9961 GB	0.0000 Bytes

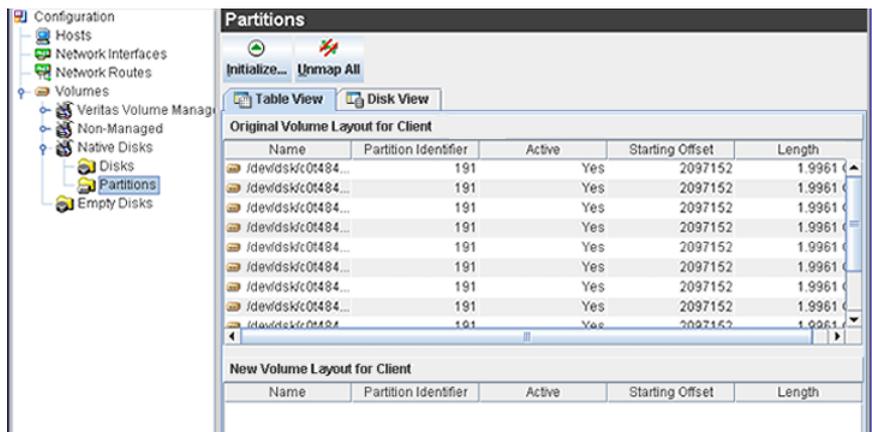
  

Name	Size	Used	Free Space
/dev/dsk/kc0t4849544...	1.9961 GB	0.0000 Bytes	1.9961 GB
/dev/dsk/kc0t4849544...	1.9961 GB	0.0000 Bytes	1.9961 GB
/dev/dsk/kc0t4849544...	1.9961 GB	0.0000 Bytes	1.9961 GB
/dev/dsk/kc0t4849544...	1.9961 GB	0.0000 Bytes	1.9961 GB
/dev/dsk/kc0t4849544...	1.9961 GB	0.0000 Bytes	1.9961 GB
/dev/dsk/kc0t4849544...	1.9961 GB	0.0000 Bytes	1.9961 GB
/dev/dsk/kc0t4849544...	1.9961 GB	0.0000 Bytes	1.9961 GB
/dev/dsk/kc0t4849544...	1.9961 GB	0.0000 Bytes	1.9961 GB
/dev/dsk/r0t4849544...	1.9961 GB	0.0000 Bytes	1.9961 GB

ディスクマッピングウィザードを使うことによって Solaris ネイティブディスクリソースをマッピングできます。マッピングウィザードを使ってディスクをマッピングするには、リストでボリュームを右クリックして[マッピング (Map)]をクリックします。次に示すのはディスクマッピングウィザードの例です。



パーティションノードはネイティブディスクノードの下に表示されます。次の例は、パーティション名、パーティションの状態、パーティションの長さ (サイズ) に関する情報を示します。



マッピングウィザードを使うことによってパーティションをマッピングできます。[ボリューム (Volume)] を右クリックするとマッピングウィザードを起動できます。宛先ディスクにソースパーティションをマッピングし、パーティションの作成に使う宛先ディスク領域の割合を指定できます。

**Partition mapping utility**  
Select the disks where this partition will be mapped and set its size.

**Partition name:**  
/dev/dsk/c0t4849544143484920373530343038313631303332d0p1

**Selected disk:**  
/dev/dsk/c0t4849544143484920373530343038313631303333d0p0

**Select a disk:**

Name	Free (GB)
c0t484954414348...	1.9960
c2t0d0p0	465.7516

**Sizes**

**Original size:**  
1.9961 GB

**Total creation size:**

**Size in GB:** 1.9980

**Size in percent:** 100 %

**Partition identifier:** SOLARIS2 (Partit... ▼)

**Description**

Solaris native disks can have maximum 4 partitions out of which only one is active at any given time. The active partition identifier can either be 130 (SOLARIS) or 191 (SOLARIS2).

Help Cancel < Back Next > Finish

## ボリュームのマッピングおよびマッピング解除について

表示されるボリュームマッピングウィザードは、マッピングする項目によって異なります。このウィザードに従って、マッピング処理を行います。

マッピングはセッション間で保存されています。そのため、マッピングを停止して後で再開することもできます(Dissimilar Disk Restore でマッピングを実行する場合に、[OK]をクリックして[構成の変更 (Change Configuration)]ダイアログボックスを終了すると、DDR リストア処理は続行します)。

要素のマッピングの設定または解除を行うと、その要素内に存在するすべての要素に対しても同じようにマッピングの設定または解除が適用されます。

主なオプションは次のとおりです。

- 初期化 (Initialize) [新しいボリュームレイアウト (New Volume Layout)]ウィンドウにインポートする構成を選択できるダイアログボックスを開きます。構成のディスク情報のみがインポートされます。このオプションは、新しいディスクのレイアウトを含む構成を初期化してマッピングを開始する場合に使用します。
- すべてをマッピング解除 (Unmap All) [新しいボリュームレイアウト (New Volume Layout)]ウィンドウにあるすべてのマッピング済み要素を削除して、[元のボリュームレイアウト (Original Volume Layout)]ウィンドウにあるすべての要素を[未マッピング (Unmapped)]に変更します。

**メモ:** マッピングウィザードでは、ボリュームやパーティションのサイズを、ファイルのリストアに必要な領域を下回る値に設定することはできません。

次に、UNIX および Linux の DDR に関する注意事項を示します。

- クラスタ内の共有ディスクは、制限ありとマークされます。
- Solaris クライアント上の未使用の VxVM ディスクは、制限ありとマークされます。
- 物理ボリュームがマルチデバイス上に作成されている Linux LVM ボリュームグループは、同じ構成にマッピングできません。物理ボリュームは、マルチデバイスではなく、ディスクまたはパーティションにマッピングされます。

次に、Windows の DDR に関する注意事項を示します。

- システムドライブは常にマッピングされているため、移動できません。ただし、リストア前にディスクをマッピングする場合は、システムドライブのサイズを変更できます。
- クラスタ構成の元のディスクおよびそのボリュームをマッピングすることはできません。
- クラスタ構成の元のディスクとディスク署名が同じである検出ディスクをマッピングすることはできません。

表 8-10 に、実行可能なボリュームのマッピング処理を示します。

**表 8-10** ボリュームのマッピング処理

処理	説明
初期化 (Initialize)	[新しいボリュームレイアウト (New Volume Layout)]ウィンドウにインポートする構成を選択できるダイアログボックスを開きます。構成のディスク情報のみがインポートされます。
自動マッピング (Fast Map)	元の構成を評価し、必要な属性を持つターゲット構成にあるディスクにソースディスクをマッピングします。
すべてをマッピング解除 (Unmap All)	ターゲット構成にあるすべてのマッピング済み要素を削除し、元の構成にあるすべての要素を[未マッピング (Unmapped)]に変更します。

処理	説明
マッピング (Map)	[元のボリュームレイアウトのテーブルビュー (Table View of the Original Volume Layout)]ウィンドウの要素を右クリックして、ショートカットメニューから[マッピング (Map)]を選択します。選択した要素に対してマッピングウィザードが表示されます (主要要素のディスクグループ、ディスク、ボリューム、ボリュームセットなどを除く)。
ボリュームのマッピング (Map Volume)	[元のボリュームレイアウトのディスクビュー (Disk View of the Original Volume Layout)]ウィンドウのボリュームを右クリックして、ショートカットメニューから[ボリュームのマッピング (Map Volume)]を選択します。選択した要素のマッピングウィザードが起動します。
ボリュームグループのマッピング (Map Volume Group)	[元のボリュームレイアウトのディスクビュー (Disk View of the Original Volume Layout)]ウィンドウのボリュームグループを右クリックして、ショートカットメニューから[ボリュームグループのマッピング (Map Volume Group)]を選択します。選択した要素のマッピングウィザードが起動します。
ディスクのマッピング (Map Disk)	[元のボリュームレイアウトのディスクビュー (Disk View of the Original Volume Layout)]ウィンドウのディスクを右クリックして、ショートカットメニューから[ディスクのマッピング (Map Disk)]を選択します。選択した要素のマッピングウィザードが起動します。
ディスクグループのマッピング (Map Disk Group)	[元のボリュームレイアウトのディスクビュー (Disk View of the Original Volume Layout)]ウィンドウのディスクグループを右クリックして、ショートカットメニューから[ディスクグループのマッピング (Map Disk Group)]を選択します。選択した要素のマッピングウィザードが起動します。
制限 (Restrict)	(Veritas Cluster Server のみ) [元のボリュームレイアウト (Original Volume Layout)]ウィンドウの要素を右クリックして、ショートカットメニューから[制限 (Restrict)]を選択します。
制限の削除 (Remove Restriction)	(Veritas Cluster Server のみ) [新しいボリュームレイアウト (New Volume Layout)]ウィンドウを右クリックして、ショートカットメニューから[制限 (Restrict)]を選択してディスクをマッピングします。

## ボリュームのマッピング

保護対象のクライアントからリストア構成にボリュームをマッピングするには、次の手順を実行します。

## 各要素のマッピングを実行する方法

- 1 [テーブルビュー (Table View)] タブまたは [ディスクビュー (Disk View)] タブで、[元のボリュームレイアウト (Original Volume Layout)] ウィンドウに表示されている要素を右クリックします。
- 2 ショートカットメニューで適切なマッピングオプションを選択します (マッピングオプションは状況に応じて異なります)。

次に示す状況に応じたマッピングウィザードが表示されます。

**マッピング (Map)** 選択した要素に対してマッピングウィザードが表示されます (主な要素のディスクグループ、ディスク、ボリューム、ボリュームグループなどを除く)。

**ボリュームのマッピング (Map Volume)** ボリュームマッピングウィザードが表示されます。

**ボリュームグループのマッピング (Map Volume Group)** ボリュームグループマッピングウィザードが表示されます。

**ディスクのマッピング (Map Disk)** 要素がディスクグループまたはボリュームグループのディスクである場合は、ディスクグループまたはボリュームグループのウィザードが表示されます。その後、ボリュームごとのボリュームマッピングウィザードが表示されます (必要なプロパティが設定されます)。要素が次に該当する場合は、ディスクマッピングウィザードが表示されます。

- ディスクグループに存在しないディスクである
- ボリュームグループ (AIX) に属していない
- どのボリュームも他のディスクにまたがっていない (ミラー、ストライプなど)

その後、すべてのボリュームとファイルシステムがターゲットのディスクにマッピングされます。ソース要素とターゲット要素 (ディスク、ボリューム、ファイルシステム) の両方の状態が [マッピング済み (Mapped)] に設定されます。

**ディスクグループのマッピング (Map Disk Group)** ディスクグループマッピングウィザードが表示されます。

### 要素のマッピングを解除する方法

- 1 [テーブルビュー (Table View)]タブまたは[ディスクビュー (Disk View)]タブの[新しいボリュームレイアウト (New Volume Layout)]ウィンドウで、マッピングを解除する要素を右クリックします。
- 2 ショートカットメニューでマッピング解除オプションをクリックします。マッピング解除オプションは、状況に応じて[マッピング解除 (Unmap)]、[ディスクのマッピング解除 (Unmap Disk)]、[ボリュームのマッピング解除 (Unmap Volume)]などになります。  
要素のマッピングが解除され、使用領域と空き領域の値がそれに応じて変更されます。

### Windows でシステムのボリュームサイズを変更する方法

- 1 [テーブルビュー (Table View)]タブまたは[ディスクビュー (Disk View)]タブで、[新しいボリュームレイアウト (New Volume Layout)]ウィンドウに表示されているボリュームを右クリックします。
- 2 ショートカットメニューで[サイズの変更 (Change Size)]をクリックします。
- 3 Windows [システムボリュームサイズの変更 (System Volume Size Change)]ダイアログボックスで、ボリュームのサイズを変更します。
- 4 ボリュームのサイズを変更します。

### ディスクの制限を設定または解除する方法

- 1 [テーブルビュー (Table View)]タブまたは[ディスクビュー (Disk View)]タブで、[新しいボリュームレイアウト (New Volume Layout)]ウィンドウに表示されているディスクを右クリックします。
- 2 ショートカットメニューで[制限 (Restrict)]または[制限の削除 (Remove Restriction)]をクリックして、次を指定します。
  - [制限 (Restrict)]を選択すると、ディスクがマッピングの対象外になります。また、ディスクがフォーマットされなくなり、ディスク上のボリュームグループまたはボリュームが作成およびリストアされません。
  - [制限の削除 (Remove Restriction)]を選択すると、制限が削除され、ディスクをマッピングの対象として使用できるようになります。ディスクをマッピングすると、ディスクがフォーマットされ、ディスク上のボリュームグループまたはボリュームが作成されてリストアされます。

### Windows でディスクをダイナミックディスクに昇格する方法

- 1 [テーブルビュー (Table View)]タブまたは[ディスクビュー (Disk View)]タブで、[新しいボリュームレイアウト (New Volume Layout)]ウィンドウに表示されているディスクを右クリックします。
- 2 ショートカットメニューで[ダイナミックディスクへの昇格 (Promote to Dynamic Disk)]をクリックします。

## Windows システムミラーを追加または削除する方法

- 1 ディスクがベーシックディスクの場合は、ダイナミックディスクに昇格します。
- 2 [テーブルビュー (Table View)] タブまたは [ディスクビュー (Disk View)] タブで、[新しいボリュームレイアウト (New Volume Layout)] ウィンドウに表示されている要素を右クリックします。
- 3 ショートカットメニューで [ミラーの追加 (Add Mirror)] または [ミラーの削除 (Remove Mirror)] をクリックします。
- 4 ミラーを追加する場合は、Windows [システムボリュームへのミラーの追加 (Add Mirror to System Volume)] ダイアログボックスで、ミラーに使用するディスクを選択します。
- 5 ミラーを追加する場合は、ミラーに使用するディスクを選択します。

## ボリュームビュー

ツリービュー (左側のペイン) には、ディスクレイアウトの構成要素が表示されます。ツリーに表示される要素は、クライアントのオペレーティングシステムと、有効になっている **Volume Manager** によって異なります。ツリービューは、右側にある詳細ペインの表示内容のフィルタとして使用できます。要素を選択すると、右側のペインにその要素の属性が表示されます。他のすべての要素は除外されるため、詳細ペインには表示されません。

次のインジケータは、マッピング処理中の要素の状態を表します。

未マッピング (Unmapped)	要素は新しい構成にマッピングされていません。
マッピング済み (Mapped)	要素は新しい構成にマッピングされています。
制限あり (Restricted)	ディスクが共有されている (または共有されていた) か、手動で制限されているため、使用できません。

右側の詳細ペインには、次のビューがあります。

- [テーブルビュー (Table View)] タブには、各要素がソートされてリストに表示されます。
- [ディスクビュー (Disk View)] タブには、各ディスクの構成が表示されます。色の付いたバーは、ストレージレイアウトの種類を表します。拡張パーティションについては、プライマリパーティションの色が上部のバーに表示され、拡張部分の色は下部のバーに表示されます。ソフトパーティションについては、上部のバーに、ソフトパーティションが作成された下位ボリュームまたはスライスが表示されます。
- [プールビュー (Pool View)] タブには、ZFS プールのそれぞれのファイルシステムとボリュームの構成が表示されます。

- [元のボリュームレイアウト (Original Volume Layout)]ウィンドウ (上部のウィンドウ) には、元のシステムのボリュームレイアウトとソース要素 (ディスク、ディスクグループまたはボリューム) が表示されます。  
 領域の使用量とディスクのサイズが表示されます。要素のプロパティを表示するには、要素を右クリックして、ショートカットメニューから[プロパティ(Properties)]を選択します。
- [新しいボリュームレイアウト (New Volume Layout)]ウィンドウ (下部のウィンドウ) には、ターゲットシステムのボリュームレイアウトと要素が表示されます。レイアウトのある構成を検出された構成から初期化する場合は、要素を[元のボリュームレイアウト (Original Volume Layout)]から[新しいボリュームレイアウト (New Volume Layout)]にマッピングします。

ボリューム情報は、次のような階層構成になっています。

- ディスクグループ、ボリュームグループまたはディスクセットには、ディスクが含まれています。
- ディスクには、ボリュームとパーティションが含まれています。
- ボリュームまたはパーティションには、ファイルシステムが含まれています。

すべての **Volume Manager** で、このような論理概念がすべて適用されているわけではありません。たとえば、**Solaris** スライスにはディスクグループに属さず、スライス内にあるのはファイルシステムだけです。

次の表に、ツリービューの各種要素および[テーブルビュー (Table View)]タブと[ディスクビュー (Disk View)]タブの表示内容を示します。

表 8-11に、Windows の要素を選択したときの詳細を示します。

表 8-11 Windows の要素

ノード	[テーブルビュー (Table View)]タブの表示内容	[ディスクビュー (Disk View)]タブの表示内容
Windows ディスク管理	ディスクとボリューム	該当なし
ディスク	システム内のすべてのディスク	システム内のすべてのディスク
ボリューム	(管理対象であるかどうかに関係なく)システムで定義されているすべてのボリューム	(作成に使用した <b>Volume Manager</b> に関係なく)ボリュームが存在するすべてのディスク
特定のボリューム	そのボリュームが存在するディスク	そのボリュームが存在するディスク

表 8-12に、Veritas Volume Manager の要素を選択したときの詳細を示します。

表 8-12 Veritas Volume Manager および Veritas Storage Foundation for Windows の要素

選択された要素	[テーブルビュー (Table View)] タブの表示内容	[ディスクビュー (Disk View)] タブの表示内容
Veritas Volume Manager	ディスクグループ、ボリュームセットおよびボリューム	該当なし
ディスクグループ	構成内のディスクグループ	すべてのディスクグループ内のディスク
特定のディスクグループ	そのディスクグループ内のディスク	そのディスクグループ内のディスク
ボリューム	Volume Manager で管理されているすべてのボリューム	Volume Manager ボリュームが存在するディスク (ディスクグループ順)
特定のボリューム	そのボリュームが存在するディスク	そのボリュームが存在するディスク

表 8-13 に、ZFS Manager の要素を選択したときの詳細を示します。

メモ: の BMR では、ZFS ストレージプールが接続された Solaris 10 クライアントもリストアできます。

表 8-13 ZFS Manager の要素

選択された要素	[テーブルビュー (Table View)] タブの表示内容	[プールビュー (Pool View)] タブの表示内容	[ディスクビュー (Disk View)] タブの表示内容
ZFS Manager	該当なし	該当なし	該当なし
ZFS プール	該当なし	各 ZFS プールのファイルシステムとボリュームの詳細	各 ZFS プールと関連付けられたディスクの詳細
ZFS ファイルシステム	該当なし	選択した各 ZFS ファイルシステムのプール領域消費量の詳細	該当なし
ZFS ボリューム	該当なし	選択した各 ZFS ボリュームのプール領域消費量の詳細	該当なし

表 8-14 に、Solaris Volume Manager の要素を選択したときの詳細を示します。

表 8-14 Solaris Volume Manager の要素

選択された要素	[テーブルビュー (Table View)] タブの表示内容	[ディスクビュー (Disk View)] タブの表示内容
Solaris Volume Manager	ディスクセットとボリューム	該当なし
ディスクセット	名前付き (非ローカル) のすべてのセット	名前付き (非ローカル) セット内のディスク (ディスクセット順)
特定のディスクセット	そのディスクセット内のディスク	そのディスクセット内のディスク
ボリューム	すべての SVM ボリューム	SVM ボリュームが存在するディスク
特定のボリューム	そのボリュームが存在するディスク	そのボリュームが存在するディスク

表 8-15 に、管理対象外の Solaris の要素を選択したときの詳細を示します。

表 8-15 Solaris 管理対象外要素

選択された要素	[テーブルビュー (Table View)] タブの表示内容	[ディスクビュー (Disk View)] タブの表示内容
管理対象外	ディスクとパーティション	該当なし
ディスク	VxVM の管理対象外のすべてのディスクと、SVM ディスクセットにないすべてのディスク	VxVM の管理対象外のすべてのディスクと、SVM ディスクセットにないすべてのディスク
スライス	管理対象外で SVM メタデバイスとして使用されていないすべてのスライス	管理対象外スライスが存在するすべてのディスク

表 8-16 に、空のディスクの要素を選択したときの詳細を示します。

表 8-16 空のディスクの要素

選択された要素	[テーブルビュー (Table View)] タブの表示内容	[ディスクビュー (Disk View)] タブの表示内容
空のディスク	使用されていないディスク	使用されていないディスク

表 8-17 に、AIX と HP-UX の Logical Volume Manager の要素を選択したときの詳細を示します。

表 8-17 AIX および HP-UX Logical Volume Manager の要素

選択された要素	[テーブルビュー (Table View)] タブの表示内容	[ディスクビュー (Disk View)] タブの表示内容
Logical Volume Manager	ボリュームグループとボリューム	該当なし
ボリュームグループ	構成内のボリュームグループ	すべてのボリュームグループ内のディスク (ボリュームグループ順)
特定のボリュームグループ	そのボリュームグループ内のディスク	そのボリュームグループ内のディスク
ボリューム	LVM で管理されているすべてのボリューム	LVM ボリュームが存在するディスク
特定のボリューム	そのボリュームが存在するディスク	そのボリュームが存在するディスク

# BMR ブートサーバーの管理

この章では以下の項目について説明しています。

- [ブートサーバーについて](#)
- [ブートサーバー要件](#)

## ブートサーバーについて

ブートサーバーは、システムリカバリや共有リソースツリー (SRT) などシステムリカバリの必要なリソースを含む、保護対象のクライアントの再構築に必要な環境を提供します。ブートサーバーは、リストアに先立ってネットワークブートを実行するときにクライアントシステムのブートに使用するリソースも提供します。

この一時的なオペレーティングシステム環境は、NetBackup-BMR の言語で SRT または共有リソースツリー (Shared Resource Tree) と呼ばれます。この環境を作成およびホストする際は、ホストのオペレーティングシステム固有の必要条件と NetBackup-BMR 固有の必要条件に従う必要があります。SRT は OS ファイル、NetBackup クライアントソフトウェア、Arctera Volume Manager のようなその他の必須ソフトウェアの集合です。SRT はクライアントのイメージではありません。単一の SRT は、複数のクライアントをリカバリするために使うことができます。SRT の作成や変更に必要な操作の多くはターゲットホストのオペレーティングシステムに依存します。そのため、NetBackup-BMR には、リカバリするホストと同じオペレーティングシステムのブートサーバーが必要になります。

ブートサーバーソフトウェアは、NetBackup インストールメディアからインストールします。

BMR ブートサーバーを含む一般的な配置は、次のように表示されます。

BMR ブートサーバーの設定について詳しくは「BMR の設定」の章を参照してください。

# ブートサーバー要件

ブートサーバーに関連する SRT 要件に関する詳細情報が利用可能です。

p.192 の「ブートサーバーについて」を参照してください。

表 9-1 ブートサーバー要件

サーバーの種類	要件
一般的なブートサーバー	<p>ブートサーバーは、保護するクライアントの種類ごとに用意する必要があります。たとえば、Solaris クライアントには Solaris ブートサーバー、Windows クライアントには Windows ブートサーバーが必要です。</p> <p>UNIX と Linux のリストア、および Windows のレガシーのリストアの場合、特定のバージョンのオペレーティングシステムのブートサーバーは、同じバージョンかそれ以前のバージョンのオペレーティングシステムの SRT のみをホスティングできます。たとえば、Solaris 9 のブートサーバーは Solaris 8 および Solaris 9 の SRT をホスティングできますが、Solaris 10 の SRT をホスティングできません。</p> <p>UNIX と Linux のリストア、および Windows のレガシーのリストアの場合、特定のバージョンのオペレーティングシステムのクライアントには、同じバージョンのオペレーティングシステムの SRT が必要となります。</p> <p>異なるプラットフォーム用のネットワークベースリカバリの前提条件の設定について詳しくは、付録の「BMR ブートサーバーに対するネットワークサービスの設定」を参照してください。</p>
AIX ブートサーバー	<p>AIX ブートサーバーには、特別な要件はありません。AIX ブートサーバーは、クライアントと同じサブネット上にあっても、異なるサブネット上にあってもかまいません。ただし、特定のバージョンのオペレーティングシステムの AIX ブートサーバーは、同じバージョンかそれ以前のバージョンのオペレーティングシステムの SRT のみをホスティングできます。たとえば、5.3.0.10 ブートサーバーがホスティングできるのは、5.1.x.x、5.2.x.x、5.3.0.0 および 5.3.0.10 の SRT のみであり、5.3.0.20 の SRT はホスティングできません。同様に、5.2.x.x のブートサーバーは、5.3.x.x の SRT をホスティングできません。</p> <p>また、5.3.0.10 のクライアントをリカバリするには、5.3.0.10 の SRT を作成する必要があります。5.3.0.11 または 6.1.0.1 の SRT は、このクライアントのリカバリに使用できません。</p>

サーバーの種類	要件
HP-UX ブートサーバー	<p>HP-UX クライアントの各ネットワークセグメントで、クライアントをサポートする HP-UX ブートサーバーが必要です。</p> <p>HP-UX ブートサーバーでは、SRT の Ignite バージョンと、ブートサーバーにインストールされている Ignite バージョンが一致している必要があります。</p>
Linux ブートサーバー	<p>Linux クライアントの各ネットワークセグメントで Linux ブートサーバーが必要です。</p> <p>ただし、VLAN (仮想ローカルエリアネットワーク) を設定する場合には、クライアントの存在しない VLAN にあるサーバーにネットワークブート要求パケットを配送するようにスイッチを設定できます。このようにすると、単一の Linux ブートサーバーが異なる VLAN に属している Linux クライアントをリカバリできます。</p>

サーバーの種類	要件
Solaris ブートサーバー	

サーバーの種類	要件
	<p><b>Solaris</b> クライアントの各ネットワークセグメントで、クライアントをサポートする <b>Solaris BMR</b> ブートサーバーが必要です。</p> <p>ただし、次の方法によって、この要件の影響を最小限に抑えることができます。</p> <ul style="list-style-type: none"> <li>■ 必要に応じて、<b>BMR</b> ブートサーバーソフトウェアをネットワークセグメント内の <b>Solaris</b> コンピュータにインストールできます。その後、クライアントに障害が発生してリストアの必要性が生じた場合に、<b>SRT</b> を作成します。</li> <li>■ <b>Solaris BMR</b> ブートサーバーは、複数のネットワーク上に物理 IP が存在する <b>Solaris</b> コンピュータで定義できます。つまり、複数のネットワークインターフェースを含む 1 つの <b>Solaris BMR</b> ブートサーバーを、各ネットワークセグメント上の <b>Solaris BMR</b> クライアントで使用できます。</li> <li>■ リモートサブネット上の <b>Solaris</b> コンピュータが、ネットワークゲートウェイを使って <b>BMR</b> ブートサーバーからブートできるように、リレーブートサーバーを構成します。</li> <li>■ サポート担当者に連絡して詳細情報を入手できます。</li> <li>■ <b>Solaris10_x64</b> 用の <b>BMR</b> ブートサーバーには、次のソフトウェアがインストールされている必要があります。 <ul style="list-style-type: none"> <li>■ TFTP サーバー</li> <li>■ DHCP サーバー</li> <li>■ NFS サーバー</li> <li>■ <b>Solaris10_x64</b> クライアントの <b>BMR (Bare Metal Restore)</b> を実行するための <b>SRT</b> は、<b>Solaris10_x64</b> ブートサーバーのみで作成し、ホストにすることができます。<b>OS</b> レベルと <b>Kernel</b> レベルは、リストアするクライアントのレベル以上である必要があります。</li> </ul> </li> <li>■ <b>BMR</b> ブートサーバーの最小 <b>Solaris 11 OS</b> は <b>Solaris 11.3 SRU 20</b> です。</li> <li>■ <b>Solaris 11.3 SRU 20</b> 以上のブートサーバーで <b>SRT</b> を作成する場合は、ブートサーバーで次のリポジトリとそのパブリッシュを設定する必要があります。 <ul style="list-style-type: none"> <li>■ <b>solarisstudio</b> (Oracle <b>Solaris/Developer Studio 12.6</b>)。 <b>Solaris Developer Studio</b> について詳しくは、<a href="http://support.oracle.com">http://support.oracle.com</a> を参照してください。</li> <li>■ <b>SRT</b> の作成に使用する <b>solaris</b> (<b>Solaris</b> リポジトリのバージョンは、<b>Solaris 11.3 AI SRU</b> 以上である必要があります) のバージョン。 <b>Solaris 11 SRU</b>、リポジトリ、<b>Automated Installer</b> イメージのダウンロードについて詳しくは、<a href="https://support.oracle.com">https://support.oracle.com</a> を参照してください。</li> </ul> </li> </ul>

サーバーの種類	要件
	bmrstadm を使用して BMR-ISO SRT を生成する場合は、ブートサーバーに SUNWmkcd パッケージをインストールする必要があります。
Windows ブートサーバー	Windows ブートサーバー要件は次のとおりです。 <ul style="list-style-type: none"> <li>■ ブートサーバーでネットワークブートサービスを使用するには、ネットワーク上に DHCP サーバーが必要です。</li> <li>■ ブートサーバーで PXE サービスまたは TFTP サービスを実行することはできません。</li> </ul>

# トラブルシューティング

この章では以下の項目について説明しています。

- **CD/DVD** からのブートの問題
- リストアにかかる時間が長い
- **Solaris** メディアブートネットワークパラメータの問題
- **BMR** 構成が誤って削除された場合にクライアントを回復する方法
- **BMR** リストアの後の最初のブートが **UNIX** プラットフォームで失敗します
- クライアントのネットワークベースのブートの問題
- **Windows** クライアントのリカバリ中のバックアップエラーの検証
- **VM** は **32** ビットアーキテクチャ **Windows OS** で実行されている仮想マシンへの **BMR** 物理的バックアップ変換後にブートするのに長い時間がかかります。
- 仮想マシンの変換ジョブへの **BMR** が有効に設定されている物理的バックアップが、**Windows** プラットフォームで失敗する
- クライアントバックアップからの仮想マシンの作成に関する問題のトラブルシューティング
- システムブート時や **BMR** の初回ブート時に **Solaris 11** 以降の多くのサービスが警告メッセージを表示する
- **BMR** のリストア後の初回ブート時に、**Solaris 11** 以降の **Solaris** ゴーストリカバリを再構成するまでに時間がかかる
- テキストインストーラのパッケージがカスタマイズされた **AI ISO** 内に存在しない場合、**Solaris BMR** のリストア操作に失敗する
- 複数のデバイスに基づく **OS** 構成では **/boot** パーティションが独立したパーティション上になければならない

- **ZFS** ストレージプールを使ったクライアントのリストア後、初回のブート中に、複数のエラーメッセージが表示されることがある
- **BMR** が **ZFS** メタデータをフォーマットまたは消去しないことがある
- 自動イメージレプリケーションおよび **BMR** を使って保護する場合のクライアントの短縮名の指定
- クライアントリストアの成功後もリストアタスクがディザスタリカバリドメインに完了状態で保持されることがある
- リストア後に **HP-UX** の自動ブートに失敗することがある
- **Solaris** クライアントのリストア準備が機能しないことがある
- **NetBackup 8.1** をインストールしている **Windows (x64)** での **NetBackup 8.0** を対象とした仮想インスタンスコンバータ (**VIC**) ホストの使用はサポートされません。
- アップグレード後のブートサーバーのバージョンの不一致による **PTR** または **PTD** エラー
- リストア準備および検出準備のエラーメッセージと、**BMR** 用の安全な通信に関連する **bmrprep** コマンド
- **Solaris x86 11.2** 以降のクライアントのメディアリストアでメンテナンスモードのユーザー名とパスワードを求められることがある
- クライアントの **PTD** タスクが正常に完了した後も検出タスクが完了中の状態のままになることがある
- クライアントが正常にリストアされても **BMR** リストアタスクが完了中の状態のまま変わらないことがある
- 共有リソースツリー (**SRT**) の作成中にブートサーバーとクライアントでバックアップ操作が開始されると、**BMR** のリストア後に **SRT** の作成が失敗してエラーが発生する
- バックアップ時に **BMR** 情報の受信中に発生するエラー
- **BMR** のバックアップジョブとリストアジョブの詳細が **NetBackup Web UI** のアクティビティモニターに表示されない

## CD/DVD からのブートの問題

AIX、Linux および **Solaris** プラットフォームは、共通のブート可能 CD/DVD 形式 (**ISO-9660**) を使います。HP-UX は、**Logical Interchange Format (LIF)** を使います。システムが CD/DVD からブートできない場合、CD/DVD ドライブのあるシステムにそのメディアを挿入し、内容を確認してください (**UNIX** または **Windows** のいずれのプラットフォームでも **ISO** 形式を読み取ることができます)。

次の手順を実行します。

- CD/DVD の内容が 1 つのファイルの場合、その CD/DVD は ISO-9660 CD/DVD イメージではなく、データ CD/DVD として書き込まれています。ISO イメージファイルの書き込みに必要なオプションを使用して、書き込み手順を繰り返します。
- CD/DVD がブランク、または読み取ることができない場合は、そのメディアをドライブから取り出して、内容が書き込まれているかどうかを詳しく調べます。一部の CD/DVD 書き込みソフトウェアは、デフォルトで、CD/DVD への書き込みをシミュレーションして CD/DVD 書き込みハードウェアの機能をテストします。テスト専用オプションをオフにするまで CD/DVD への書き込みを行いません。テスト専用オプションを無効にして、書き込み手順を繰り返します。
- ブートが部分的に成功している場合、あるいは、いくつかのファイルが紛失または破損していると表示される場合は、次のいずれかが発生しています。
  - 書き込み処理に失敗しています。部分的に書き込まれた CD はブート可能ですが、内容の重要な部分が存在しない可能性があります。書き込みを成功させるには、CD 書き込み速度を遅くします。一部の CD 書き込みソフトウェアで提供されている書き込み後テストまたは検証オプションを使用すると、CD 書き込みの失敗を検出できる場合があります。
  - BMR ブートサーバーから CD ライターとして使っているコンピュータへのファイル転送に失敗しています。  
よくある破損の原因として、FTP でのファイル転送をバイナリモードではなく ASCII 転送モードで行ったことが挙げられます。
- CD が別の類似コンピュータで正常にブートする場合、リストアシステムのドライブが損傷しているか、汚れている可能性があります。同様に、CD 自体も損傷を受けやすく、書き込み後に表面が汚れて読み取り不可能になっている場合があります。物理メディアおよび読み取りを行っている環境を確認してください。
- CD からのクライアントコンピュータのブートを正しい手順で行っているかどうかを確認します。
- インストールメディアからクライアントのブートを試行し、コンピュータに CD からのブート時におけるハードウェアの問題がないことを確認します。

## リストアにかかる時間が長い

リストアに異常に時間がかかる場合 (たとえば、通常 2 時間に対して 20 時間かかるなど)、アダプタと接続先のスイッチまたはハブとの間で通信速度が一致していないことがあります。たとえば、通信速度が 100 MB の全二重モードに設定されていても、ハブが半二重モードである場合は、リストア速度が遅くなります。通信速度をハブまたはスイッチの速度に一致するように変更してみるか、ハブまたはスイッチの設定をクライアントの設定と一致するように変更します。

## Solaris メディアブートネットワークパラメータの問題

Solaris クライアントのメディアブートでは、Solaris コードがローカルサブネットのポーリングを行います。ローカルサブネット上のコンピュータにブートクライアントのネットワークパラメータのレコードが存在するかどうかを確認します。JumpStart サーバーの `/etc/ethers` または `/etc/bootparams` ファイルにクライアントのネットワークパラメータが存在する場合は、これらのパラメータがブートプロセスに使用されます。これらのパラメータは BMR で構成されたブートインターフェースのネットワークパラメータと異なっていても使用されます。

クライアントのネットワークパラメータが存在する場合、リストアが失敗する可能性があります。

この問題を解決するには、次のいずれかを実行します。

- クライアントのサブネットにある他のすべてのコンピュータで、次のファイルから、クライアントシステムへのすべての参照を削除します。

```
/etc/ethers file  
/etc/bootparams
```

- メディアブートがリストア用のネットワークパラメータを構成するまで、ブートクライアントをネットワークから切断します。

## BMR 構成が誤って削除された場合にクライアントを回復する方法

クライアントおよびその現在の構成を削除した場合、次にクライアントがバックアップされるときにその構成が保存されます。クライアントは、[Bare Metal Restore クライアント (Bare Metal Restore Clients)]ビューに再び表示されます。

クライアントが失敗した後で (そのリストアを行う前に) クライアントおよび構成を削除した場合は、`bmrs` コマンドを使用して、クライアントの以前の構成を取得できます。(削除されたクライアントは[Bare Metal Restore クライアント (Bare Metal Restore Clients)]ビューに表示されないため、指定した時点へのリストアは実行できません。)

マスターサーバーで使用する `bmrs` コマンドの形式を次に示します。

```
bmrs -resource config -operation retrieve -client clientName  
-destination newConfigName -enddate dateFormat -policy policyName
```

`bmrs` コマンドについて詳しくは、『NetBackup コマンド UNIX、Windows および Linux』を参照してください。

## BMR リストアの後の最初のブートが UNIX プラットフォームで失敗します

BMR リストアの後で、元々 2 つのディスクにわたってミラーリングされているルートディスクが連結レイアウトに変更された場合、最初のブートは GRUB で失敗する場合があります。システムセットアップでは、ルートディスクは c3t0d0 と c4t0d0 の 2 枚のディスクにわたってミラー化されました。BIOS 設定では、c3t0d0 はブートシーケンスの最初のディスクです。DDR 構成中にルートディスクはミラーから変更され、連結し c4t0d0 にマップされます。BIOS では、このディスクはブートシーケンスの 2 番目のディスクです。したがって、BMR リストアの後にシステムが初めてブートされる時、c3t0d0 がブートシーケンスの最初のディスクで、「ディスクが以前ミラー化されたため GRUB シグネチャがこのディスクにまだ存在する」ため、システムは c3t0d0 上の GRUB からブートしようとしていますが、ルートファイルシステムや他のブート可能なファイルが現在は c4t0d0 にあるためそれらを取得できず、ブートに失敗します。

BMR リストアの後で、システムブート中に、BIOS 設定を変更し、ブートするシステムに対して正しいディスクを選択します。

## クライアントのネットワークベースのブートの問題

オペレーティングシステムが異なれば、ネットワークブートに使用されるネットワークプロトコルも異なります。BMR はこのプロトコルを利用して、ネットワークベースのクライアントリカバリを開始します。たとえば、Windows、Linux および Solaris-x86 では、DHCP、TFTP プロトコルで構成された PXE ベースのネットワークブートを使用します。

それぞれについて説明します。

**Windows の場合:** BMR は PXE サービスおよび TFTP サービスを BMR ブートサーバー上で実行します。DHCP は同じサブネットのどのサーバーでも使用できます。

**Linux の場合:** DHCP サービス、TFTP サービスは、クライアントのネットワークブートを提供するブートサーバー上で実行される必要があります (注意: サービスがブートサーバーに配備され、実行されると、BMR はクライアントのネットワークブートを有効にするために、自動的にサービスを登録または登録解除します)。場合によっては、クライアントのリカバリが行われるのと同じサブネットで、複数のネットワークブートプロトコルサーバーが実行されていることがあります。その中の 1 つがネットワークブート時に BMR クライアントに IP アドレスを割り当てることができる正しい PXE/DHCP/bootp サーバーです。そのような環境では、BMR リカバリのためにクライアントがネットワーク越しにブートされると、ネットワークブートの要求がブロードキャストされ、意図しないネットワークブートサーバー (PXE/DHCP/BOOTP) に最初に到達する可能性があります。そのようなケースでは、エラーが返され、BMR リカバリが失敗する場合があります。

そのため、BMR クライアントのネットワークブートに必要な有効なサービス 1 つを除いて、同じサブネット内で他のネットワークブートサービスが実行されていないことを確認します。

これは、PXE、DHCP、BOOTP ブートプロトコルそのものの制限事項であり、最初の DHCP がエラーを応答すると、ネットワークブートプロセスが停止してしまうためです。

## Windows クライアントのリカバリ中のバックアップエラーの検証

Bare Metal Restore (BMR) リストアプロセスを実行中に、リストアを行うクライアントは、リストアを完了するために有効なバックアップイメージを利用できるかどうかを検証しようとしています。この検証プロセスが失敗します。考えられる主な原因は次のとおりです。

- バックアップイメージが期限切れになっている。
- クライアントが間違ったポリシー形式でバックアップされている。たとえば、Windows クライアントが UNIX の標準ポリシーでバックアップされた場合などです。
- 適切なシステムのリストアに不可欠なファイルがバックアップイメージに存在しない。
- マスターサーバーでリストアまたはリストア操作を実行するために必要な権限がクライアントにない。
- リストアに使用されたリストア構成が無効であるか、ネットワーク情報がない。
- NetBackup プライマリサーバーがクライアントに対して適切な逆引き参照を実行できない。

このエラーメッセージをデバッグするための最もよい方式は、次の手順を実行することです。

- 1 NetBackup Web UI またはコマンドラインからリストア準備処理を実行します。エラーが発生した場合には、以下のいずれかが原因になっていないか確認します。通常、NetBackup カタログのクエリー情報を使用して、正しいポリシー形式を使用したバックアップイメージを利用できることを確認します。また、システム状態コンポーネントおよびシャドウコピーコンポーネントが正しくバックアップされていることを確認します。さらに、クライアントの Bare Metal Restore ソフトウェアのディレクトリがバックアップされていることも確認します。リストア準備処理が正常に完了した場合、バックアップイメージ情報は有効です。その場合は、次にクライアントまたはマスターサーバーの BMR リストア環境に問題がないかを検証します。リストア構成で検証する必要がある項目は次のとおりです。

- 「ネットワークインターフェース」のセクションをチェックして、MAC アドレスが正しく、リストアに使用されるアドレスと一致していることを確認します。クライアントネットワークケーブルが、クライアントの NIC とスイッチの両方で、正しいポートに接続されていることを確認します。
- 「ホスト」のセクションをチェックして、必要に応じて、NetBackup プライマリサーバーおよびメディアサーバーに (ホスト名や IP アドレスなどの) エントリが存在していることを確認します。

- マスターサーバーの **bmrnst** ログを参照して、リストアの進行状況を確認します。リストアを行うクライアント上で根本原因を判断するには、次の手順を実行します。
- 2 リストアウィザードをキャンセルし、終了します。これによりメインメニューの画面に戻ります。
- 3 メイン画面の左上部の隅、歯車の形をしたアイコンの近くの位置にマウスを移動します。マウスポインタが矢印から手の形に変化したら、マウスを右クリックします。これはコマンドラインのウィンドウを開きます。
- 4 `X:\¥BMR¥NBU¥bin` ディレクトリに移動します。
- 5 次のコマンドを実行します。

```
bpclimagelist -client $CLINT_NAME -T echo %ERRORLEVEL%
```

「echo」コマンドは、コマンドの戻りコードを表示するオプションです。bpclimagelist コマンドは、次の原因によりカタログバックアップイメージ情報の収集に失敗します。

- マスターサーバーと通信できませんでした (**rc=25**)。これは、クライアントが間違っていたインターフェースポートに接続した場合、またはマスターサーバーのホスト名および IP アドレスの情報が無効または不完全な場合に発生します。クライアントが最初の段階でクライアント構成にアクセスできていたとしても問題は変わりません。エラーが発生した時点では、リストアに指定されたリストア構成と一致するように、クライアントネットワークのインターフェースが修正されています。最初の入力ページで入力した値は、構成値と一致するように修正されています。
- マスターサーバーがクライアントポートに応答できませんでした (**rc=23**)。サーバーの DNS エントリまたはホストファイルのいずれかで、クライアント逆引き情報が失われているか、クライアントに無効なルーティング情報が返された可能性があります。
- マスターサーバーがリストアを行うクライアントを有効なクライアントとして認識しません (**rc=131、133、135**)。クライアントに使用される IP アドレスが構成と異なる名前に解決されたか、リスト要求およびリストア要求を実行する権限がありません。これを解決する 1 つの方法は、マスターサーバーおよびメディアサーバーの「ホスト」ファイルに一時的にエントリを追加することです。このエントリは、リストアに使用されるリストア情報の「ネットワークインターフェース」のセクションのデータ情報と一致している必要があります。また、NetBackup Web UI で [ホストプロパティ (Host Properties)]、[クライアント属性 (Client attributes)]、[クライアントによるリストアを許可する (Allow client restore)] をチェックして、クライアントにリスト操作およびリストア操作を実行する権限があることを確認します。
- NetBackup プライマリサーバーに有効なバックアップイメージがありません (**rc=227**)。

一般に、すべての BMR のリストアでは、リストア中には固定 IP アドレス情報を使用するようにして、DHCP や DNS は使用しません。必要な場合には、BMR のリストアが完了した後設定をリセットできます。

VM は 32 ビットアーキテクチャ Windows OS で実行されている仮想マシンへの BMR 物理的バックアップ変換後にブートするのに長い時間がかかります。

## VM は 32 ビットアーキテクチャ Windows OS で実行されている仮想マシンへの BMR 物理的バックアップ変換後にブートするのに長い時間がかかります。

VM のブート中でログオン後に、Windows は [新しいハードウェアの検出と構成 (New Hardware Found and Configuration)] ウィンドウをポップアップ表示されます。それは、SAS コントローラ - ベースシステムデバイスのデバイスドライバを設定するようにメッセージを表示します。このウィンドウのダイアログボックスでは、新しいデバイス構成の 2 つのオプション、[自動検索および構成 (Auto search and configure)] と [これらのデバイスのメッセージをスキップ (Skip prompting for these devices)] が表示されます。これらのオプションのいずれか 1 つを選択すると、Windows では SAS コントローラ VMware PVSCI デバイスドライバ構成でエラーが発生します。この問題のため、次のブートは BSOD になる場合があります。

[新しいハードウェア構成 (New hardware configuration)] ダイアログに対してアクションをとりました。Windows クロスボタンを使用して、このダイアログウィンドウを閉じます。このダイアログを無視できます。このプロセスは VM ブート中に毎回行う必要があります。

## 仮想マシンの変換ジョブへの BMR が有効に設定されている物理的バックアップが、Windows プラットフォームで失敗する

この問題はエラーコード 12 のジョブ障害を示します。これは仮想インスタンスコンバーターまたは NetBackup リカバリホストが作成された VM でのファイルシステムのマウントに失敗することを意味します。

VMware マウンターサービスが正しく登録され、開始されるように、NetBackup リカバリホストを再開してください。それは、NB クライアントインストール時に、NB リカバリホストを再ブートするように常にお勧めします。

## クライアントバックアップからの仮想マシンの作成に関する問題のトラブルシューティング

以降の節では、クライアントバックアップからの仮想マシンの直接作成機能を使うときに用いることがあるトラブルシューティング手順についての詳細を提供します。

## 仮想マシン変換クライアントのリストにクライアント名が表示されない

原因をデバッグするためには、以下の手順に従います。

- 1 クライアント BMR バックアップが正常であるかどうかを確認します。p.227 の「バックアップから VM を作成する際の前提条件」を参照してください。
- 2 エラーについて詳しくは bmrdr ログと bmrsvcfg ログを参照してください。
- 3 BMR バックアップが正常な場合、クライアントのホスト名が[Bare Metal Restore クライアント (Bare Metal Restore Clients)]タブに一覧表示されているかどうかを確認します。クライアントのホスト名が[Bare Metal Restore クライアント (Bare Metal Restore Clients)]リストにあり、[VM 変換クライアント (VM conversion Clients)]リストにない場合、サポートに関する表を参照し、クライアントが指定された条件を満たしているかどうかを確認します。ログの場所については表 10-1 を参照してください。

## 仮想マシン作成のジョブの送信中のエラー

仮想マシン作成のジョブのエラーの原因を見つけるためには、以下の手順に従います。

- UI ウィザードウィンドウで、目的の NetBackup リカバリホスト (仮想インスタンスコンバーター) が[リカバリホスト (Recovery Host)]ドロップダウンリストに表示されない場合、VIC (Virtual Instance Convertor の略で仮想インスタンスコンバーターの意味) が NetBackup プライマリサーバーに登録されていることを確認します。  
p.227 の「バックアップから VM を作成する際の前提条件」を参照してください。
- UI ウィザードウィンドウで目的の Hypervisor (vCenter または ESX) サーバーを表示できない場合は、以下の手順に従います。
  - 目的のサーバーが vCenter Server またはスタンドアロン ESX Server の場合、マスターサーバーに登録されていることを確認します。  
p.227 の「バックアップから VM を作成する際の前提条件」を参照してください。
  - Hypervisor がすでに登録されている場合、次のように VIC との接続性を検証します。
    - [メディアおよびデバイスの管理 (Media and Device Management)]>[クレデンシャル (Credentials)]>[仮想マシンサーバー (Virtual Machine Servers)]ノードでターゲットの Hypervisor エントリを開きます。
    - [バックアップホスト (For Backup Host)]タブで目的のリカバリホストを選択します。
    - [OK]をクリックします。  
処理を完了すると、選択された NetBackup リカバリホストによって Hypervisor サーバーの接続性が検証されます。
- Hypervisor のデータストア、リソースプール、vApp、フォルダを表示できない場合、この節で前に説明したように Hypervisor の接続性を確認します。接続性はあるがエン

システムブート時や BMR の初回ブート時に Solaris 11 以降の多くのサービスが警告メッセージを表示する

トリを取得できない場合は、詳細レベル 6 の bpVMutil と bpVMreq のログを参照してください。ログの場所については [表 10-1](#) を参照してください。

## 仮想マシン作成のジョブの失敗

エラーコードを参照するには、詳細レベル 6 の p.246 の「[VM 作成ジョブの監視](#)」を参照してください。bmr2v、bmr2vrst、bmr2d のログを確認します。ログの場所については [表 10-1](#) を参照してください。

表 10-1

コンポーネント	ログディレクトリ	場所
bpVMutil	install_path\NetBackup\logs\bpVMutil	仮想インスタンスコンバーターのリカバリ ホスト
bpVMreq	install_path\NetBackup\logs\bpVMreq	変換ジョブが送信されるマスターサー バー
bmr2v	install_path\NetBackup\logs\bmr2v	変換ジョブが送信されるマスターサー バー
bmr2vrst	install_path\NetBackup\logs\bmr2vrst	仮想インスタンスコンバーターのリカバリ ホスト
bmr2d	install_path\NetBackup\logs\bmr2d	変換ジョブが送信されるマスターサー バー
bmr2savcfg	install_path\NetBackup\logs\bmr2savcfg	BMR バックアップを取るクライアント

## システムブート時や BMR の初回ブート時に Solaris 11 以降の多くのサービスが警告メッセージを表示する

Solaris 11 以降で初回ブート時に BMR をリストアすると、複数のサービスに関するエラーメッセージが表示されます。

システムブート時と BMR の初回ブート時に、多くのサービス (sendmail など) が次の警告メッセージを出力します。

```
sendmail/filesys_update failed
```

これらのメッセージは、システムにオペレーティングシステムを標準インストールするときにも表示されますが、無視できます。

BMR の初回ブート時にコンソールに表示される他のメッセージは、zpool と Solaris ブレーンの再設定に関連します。これらはすべて無害なメッセージで、システムのリストアや、zpool と zones を正しい状態にするのには影響しません。

BMR のリストア後の初回ブート時に、Solaris 11 以降の Solaris ゾーンリカバリを再構成するまでに時間がかかる

これらは、SMF サービスのメッセージです。システムリカバリには影響しません。

## BMR のリストア後の初回ブート時に、Solaris 11 以降の Solaris ゾーンリカバリを再構成するまでに時間がかかる

Bare Metal Restore (BMR) リストア操作後の初回ブート時に、BMR は `detach-attach` コマンドを使ってゾーンを再設定します。多数のゾーンを設定する必要がある場合は、これらのコマンドの実行に時間がかかることがあります。BMR `first boot` コマンドの完了後に、`zpool`、`zones`、`ZFS` の設定が新しい設定で安定するまでに時間がかかることがあります。

システムが正しい設定状態になるまで、初回ブート後に約 10 分間 (ゾーン数によってはさらに長く) 待機します。完全にリカバリするまでシステムを再起動したり、ゾーンにログインしないでください。

## テキストインストーラのパッケージがカスタマイズされた AI ISO 内に存在しない場合、Solaris BMR のリストア操作に失敗する

テキストインストーラパッケージが配布コンストラクタを使って作成されたカスタマイズ済み AI (Automated Installer) ISO 内に存在しない場合は、Solaris Bare Metal Restore (BMR) のリストア操作に失敗します。

共有リソースツリー (SRT) の作成に配布コンストラクタを使って作成されたカスタマイズ済み AI ISO を使う場合は、テキストインストーラパッケージを AI のマニフェストファイルから削除しないでください。

Solaris x86 の場合は、BMR リストアがこのパッケージのファイルを使うのでテキストインストーラパッケージが必須です。

## 複数のデバイスに基づく OS 構成では /boot パーティションが独立したパーティション上になければならない

クライアントがマルチデバイスの下でルート (/) として構成されている場合、正常な BMR リストアのためには、`/boot` パーティションが別のパーティション上にある必要があります。つまり、/ と `/boot` が同じパーティションにある場合、複数デバイスベースの OS 構成に対してサポートされません。

ZFS ストレージプールを使ったクライアントのリストア後、初回のブート中に、複数のエラーメッセージが表示されることがある

## ZFS ストレージプールを使ったクライアントのリストア後、初回のブート中に、複数のエラーメッセージが表示されることがある

ZFS ストレージプールを持つクライアントのリストア後の初回のブートの間に、複数のエラーメッセージが表示されることがあります。次に例を示します。

```
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: bmrso1101.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.
```

コンピュータの各ディスクで、エラーメッセージが発生することがあります。ただし、ログオンして `zpool status -x` コマンドを実行する、次のメッセージが表示されます。

```
all pools are healthy
```

これは、初回ブートシーケンスの間に行われる ZFS インポート操作のためです。Bare Metal Restore (BMR) は BMR リストア環境内のストレージプールと内容をリストアし、後で初回ブート中にクライアント環境にインポートします。これにより、初回ブート操作の間にエラーメッセージまたは警告メッセージが表示される場合があります。

これらのメッセージは初回ブート操作の間にもみ発生し、安全に無視できます。

## BMR が ZFS メタデータをフォーマットまたは消去しないことがある

Dissimilar Disk Restore (DDR) 中に少数のディスクに ZFS ストレージプールを作成するよう選択した場合、Bare Metal Restore (BMR) 残りのディスクの ZFS メタデータをフォーマットまたは消去しません。そのため、それらのディスクを使って他のストレージプールを作成しようとする、ディスクが ZFS ストレージプールで使用であることを示すエラーメッセージが表示されることがあります。

この問題を回避するには、`-f` オプションを使ってそれらのディスクに新しいストレージプールを作成します。

## 自動イメージレプリケーションおよび BMR を使って保護する場合のクライアントの短縮名の指定

自動イメージレプリケーションおよび Bare Metal Restore (BMR) を使って保護したいコンピュータに NetBackup クライアントパッケージをインストールする場合には、クライアントの短縮名を指定する必要があります。また、プライマリドメインに作成したバックアップポリシーにも、クライアントの短縮名を指定する必要があります。このポリシーはすべてのクライアントのローカルドライブをバックアップし、BMR が必要とするクライアント構成を収集します。二次または三次ドメインの DNS は、ディザスタリカバリサイトでのクライアントの BMR リカバリ中に完全修飾名を解決することができません。

## クライアントリストアの成功後もリストアタスクがディザスタリカバリドメインに完了状態で保持されることがある

プライマリとディザスタリカバリのドメイン名が異なる Dissimilar Domain Restore を実行すると、リストアタスクはクライアントのリストアの成功後も、ディザスタリカバリドメインに完了状態で保持されます。Bare Metal Restore (BMR) リストアはディザスタリカバリドメインで正常に実行されますが、リストアタスクの更新のみが失敗します。

この更新は、クライアントに無効なネットワーク構成がある場合に失敗します。このリストアはディザスタリカバリドメインの DNS に関連する構成ファイルを変更しないため、これは予期される動作です。

次のネットワーク構成ファイルを手動で変更し、ディザスタリカバリドメイン内のクライアントをバックアップおよびリストアする必要があります。

- Solaris の場合:
  - /etc/hosts
  - /etc/resolv.conf
  - /etc/nodename
  - /etc/bge0.hostname
- AIX の場合:

smitty を実行して、ネットワーク構成を変更します。
- HP-UX の場合:

HP のシステム管理ホームページ (SMH) を使って、ネットワーク構成を修正します。
- Linux の場合:
  - /etc/hosts
  - /etc/resolv.conf
  - /etc/sysconfig/network-scripts/ifcfg-eth\*
- Windows の場合:

次の URL を参照して、Windows のドメイン名を変更します。

- <http://windows.microsoft.com/en-US/windows7/Connect-your-computer-to-a-domain>
- <http://support.microsoft.com/kb/295017>

リストア処理が完了すると、何らかのエラーメッセージが表示されることがあります。詳しくは、次の Web サイトを参照してください：

[https://www.veritas.com/support/ja\\_JP/article.TECH73586](https://www.veritas.com/support/ja_JP/article.TECH73586)

## クライアントに有効なホスト ID ベースの証明書があっても、マスターサーバーとクライアント間の通信が失敗する場合がある

この問題は主に、Windows プラットフォームの DSR (Dissimilar System Restore) で発生します。

この問題は、初回ブート時のクリーンアップ操作での [ネットワーク設定 (Network Settings)] のエラーによって発生します。

この問題は、[ネットワーク設定 (Network Settings)] の通信を手動で修正または更新しても解決しない場合があります。

回避方法: この問題を解決するには、次の手順を実行します。

1. NetBackup がインストールされているターゲットクライアントシステムのパスに移動します。

次に例を示します。

```
c:¥program files¥veritas¥netbackup¥bin
```

2. 次のコマンドを実行します: `nbcertcmd -getctrl`

## リストア後に HP-UX の自動ブートに失敗することがある

Bare Metal Restore (BMR) のリストア後、クライアントコンピュータの初回のブート時にオペレーティングシステムの自動ブートに失敗する場合があります。その後 HP BIOS はブートドライブを識別できなくなります。

この問題を解決するには、[HP BIOS]>[EFI]シェルを使い、デバイスマッピングテーブルを確認してブートに使うことができるハードディスクドライブ (fs0: など) を選択します。

オペレーティングシステムを手動でブートするために、ディレクトリを ¥EFI¥HPUX¥に変更して (cd)、HP-UX を実行します。

---

**メモ:** EFI シェルを処理する方法については、HP EFI のマニュアルを参照してください。

---

クライアントコンピュータが起動したら、コンピュータに root としてログオンし、次のコマンドを実行して自動ブートを有効にします。

```
setboot -p <hardware_path_of_boot_harddrive>
```

## Solaris クライアントのリストア準備が機能しないことがある

Bare Metal Restore (BMR) ブートサーバーがクライアントコンピュータの IPv4 アドレスの解決に失敗したため、Solaris クライアントコンピュータの BMR のリストア準備が正常に実行されない場合があります。

この問題を回避するには、次を実行します。

- IPv4 アドレスとして、client\_host\_name マッピングエントリが /etc/hosts に最初に存在し、その後に IPv6 マッピングエントリがあることを確認してください。  
Solaris BMR ブートサーバーでは、/etc/hosts ディレクトリに最初に IPv6 アドレス client\_host\_name エントリが含まれていると、BMR ブートサーバーはクライアント IPv4 アドレスの識別に失敗します。
- [リストア準備 (Prepare To Restore)] を再度実行します。

## Netbackup 8.1 をインストールしている Windows (x64) での NetBackup 8.0 を対象とした仮想インスタンスコンバータ (VIC) ホストの使用はサポートされません。

NetBackup 8.1 BMR では、NetBackup 8.1 をインストールしている Windows (x64) での仮想インスタンスコンバータ (VIC) ホストを使用した NetBackup 8.0 を対象とする仮想マシン (VM) の直接作成 (物理から仮想) はサポートされません。この問題は、NetBackup 8.1 をインストールしている仮想インスタンスコンバータ (VIC) ホストで、NetBackup Bare Metal Restore 機能がサポートされていないために発生します。

回避方法: 仮想マシン (VM) の直接作成 (物理から仮想) 操作を正常に行うには、NetBackup 8.0 または NetBackup 8.1.1 以降をインストールしている仮想インスタンスコンバータ (VIC) ホストを使用することをお勧めします。

## アップグレード後のブートサーバーのバージョンの不一致による PTR または PTD エラー

ブートサーバーでの NetBackup 8.1.1 のアップグレード中に、正しくないマスターサーバーの指紋を使用してアップグレードプロセスを続行していたか、または認証トークンを

指定していなかった場合、ブートサーバーのバージョンは NetBackup Web UI で更新されません。

セキュリティ証明書情報が正しくないために、ホスト ID ベースの証明書をブートサーバーに配備できません。これは、ブートサーバーのバージョンの不一致や PTR または PTD 操作のエラーにつながる可能性があります。

この問題を解決するには

- 1 次のコマンドを実行して、ブートサーバーのホストにホスト ID ベースの証明書を配備します。

```
nbcertcmd -getCACertificate
```

```
nbcertcmd -getCertificate
```

ホスト ID ベースの証明書の配備について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

<http://www.veritas.com/docs/DOC5332>

- 2 NetBackup サービスを再起動します。

あるいは、ブートサーバーホスト上で次のコマンドを実行します。

```
bmrsetupboot -register
```

コマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

<http://www.veritas.com/docs/DOC5332>

## リストア準備および検出準備のエラーメッセージと、BMR 用の安全な通信に関連する `bmrprep` コマンド

このセクションでは、リストア準備 (PTR) または検出準備 (PTD) 操作、および `bmrprep` コマンドの使用時に生じる可能性があるエラーのトラブルシューティングに役立つ情報を記載しています。

表 10-2 BMR での安全な通信に関連するエラーメッセージ

エラーメッセージ	説明
<p>&lt;Name of the host&gt; の適切なホストエントリまたはホストマッピングを追加して、操作を再試行します。</p>	<p>NetBackup 8.1.1 以降の BMR 構成をリストアするには、選択したホスト名の有効なホスト ID とホスト名のマッピングが存在している必要があります。</p> <p>ホストデータベースでのホストエントリの追加またはホスト ID からホスト名へのマッピングには、<code>nbhostmgmt</code> コマンドを使用します。</p> <p><code>nbhostmgmt</code> コマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。</p> <p><a href="https://www.veritas.com/support/ja_JP/article.DOC5332">https://www.veritas.com/support/ja_JP/article.DOC5332</a></p> <p>シナリオ 1: リストアする予定のホストには、複数のホスト名が関連付けられている場合があります。あるいは別のコンテキストでは短い名前または FQDN で参照されている場合があります。それらのホスト名のいずれかにホスト ID からホスト名へのマッピングデータベースのエントリがある場合には、<code>nbhostmgmt -add</code> コマンドを使用して既存のホストエントリへの新しいマッピングを追加し、リストアする予定のホスト名とともに該当するホストにマッピングを追加する必要があります。</p> <p>短い名前、FQDN など</p> <p>シナリオ 2: リストアする予定のホストに関連付けられているどのホスト名にもホスト ID からホスト名へのマッピングデータベースのエントリがない場合には、ホストデータベースで必要なホストエントリを追加する必要があります。これは、BMR A.I.R. セットアップで生じる可能性があります。</p> <p>p.265 の「DRドメインのホストデータベースへのホストの追加」を参照してください。</p>

エラーメッセージ	説明
共有リソースツリーバージョン <Version> は、クライアント構成バージョン <Version> と互換性がありません。	<p>NetBackup 8.0 の BMR 構成をリストアするには、共有リソースツリー (SRT) と SRT にインストールされた NetBackup クライアントバージョン 8.0 を使用する必要があります。</p> <p>NetBackup 8.1.1 以降がインストールされた共有リソースツリー (SRT) は、NetBackup 8.0 の BMR 構成のリストアではサポートされません。</p> <p>同様に、NetBackup 8.1.1 以降の BMR 構成をリストアするには、共有リソースツリー (SRT) と SRT にインストールされた NetBackup クライアントバージョン 8.1.1 以降を使用する必要があります。</p> <p>SRT バージョンが BMR 構成バージョン以上でなければならないという通常条件が適用されます。</p>
<Name of the host> のホスト属性をリセットして、操作を再試行します。	<p>NetBackup 8.0 の BMR 構成を、安全に通信しているマスターに認識されているホスト向け (NetBackup 8.1 以降のホストなど) にリストアするには、正常な通信のためにホストをリセットする必要があります。</p> <p>ホストの属性のリセットについて詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。  <a href="https://www.veritas.com/support/ja_JP/article.DOC5332">https://www.veritas.com/support/ja_JP/article.DOC5332</a></p>
マッピング名が <Mapping Name> のすべてのホストのホスト属性をリセットして、操作を再試行します。	<p>ホスト名は、複数のホスト ID と関連付けることができません。</p> <p>例: クラスタ環境。</p> <p>これらのホストの一部またはすべては、安全に通信しているホスト (NetBackup 8.1 以降のホストなど) としてマスターに認識されている場合があります。そのようなホストに対して NetBackup 8.0 以前の BMR 構成をリストアする場合、正常な通信のためにそれらすべてのホストをリセットする必要があります。</p> <p>ホストの属性のリセットについて詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。  <a href="https://www.veritas.com/support/ja_JP/article.DOC5332">https://www.veritas.com/support/ja_JP/article.DOC5332</a></p>
指定したホストの構成バージョンは BMR でサポートされていない 8.1 です。	NetBackup 8.1 バージョンの BMR 構成のリストアはサポートされません。

エラーメッセージ	説明
<p>&lt;Name of the host&gt; のいずれかのホスト ID に「autoreissue」パラメータを設定して、操作を再試行します。</p>	<p>ホスト名は、複数のホスト ID と関連付けることができません。</p> <p>例: クラスタ環境。</p> <p>このようなシナリオでは、リストアする予定の単一のホスト ID に対してのみ <b>autoreissue</b> パラメータを設定する必要があります。</p> <p>ホストマッピングについて詳しくは、『NetBackup コマンドリファレンスガイド』にある <b>nbhostmgmt</b> コマンドの説明を参照してください。</p> <p><a href="https://www.veritas.com/support/ja_JP/article.DOC5332">https://www.veritas.com/support/ja_JP/article.DOC5332</a></p> <p><b>autoreissue</b> パラメータについて詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。</p> <p><a href="https://www.veritas.com/support/ja_JP/article.DOC5332">https://www.veritas.com/support/ja_JP/article.DOC5332</a></p>
<p>認証が失敗しました。Web ログインが必要です。&lt;Command Name&gt; コマンドを実行してログインします。</p>	<p><b>bmrprep</b> コマンドを正常に実行するには、Web ログインが必要です。<b>bpnbat</b> コマンドを実行する前に、<b>bmrprep</b> コマンドを使用して Web ログインを実行します。</p> <p><b>bpnbat</b> コマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』にある <b>bpnbat</b> コマンドの説明を参照してください。</p> <p><a href="https://www.veritas.com/support/ja_JP/article.DOC5332">https://www.veritas.com/support/ja_JP/article.DOC5332</a></p>
<p>BMR クライアント &lt;Name of the client&gt; をリストアする準備ができました。この操作は一定時間のみに有効です。デフォルトは 48 時間です。クライアントをブートして続行します。</p>	<p>NetBackup 8.1.1 以降の BMR 構成をリストアするために、一定の時間が確保されています。デフォルトは 48 時間です。</p> <p><b>web.conf</b> ファイルを使用して、デフォルトの 48 時間という有効期間を、目的の値に編集または更新できます。</p> <p><b>autoreissue</b> 有効期間の構成設定について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。</p> <p><a href="https://www.veritas.com/support/ja_JP/article.DOC5332">https://www.veritas.com/support/ja_JP/article.DOC5332</a></p> <p><b>メモ:</b> これは NetBackup 8.0 の BMR 構成をリストアするための要件ではありません。</p>

Solaris x86 11.2 以降のクライアントのメディアリストアでメンテナンスモードのユーザー名とパスワードを求められる場合がある

エラーメッセージ	説明
BMR クライアント <Name of the client> を検出する準備ができました。この操作は一定時間のみの有効です。デフォルトは 48 時間です。クライアントをブートして続行します。	<p>NetBackup 8.1.1 以降の BMR 構成を検出するために、一定の時間が確保されています。デフォルトは 48 時間です。</p> <p>web.conf ファイルを使用して、デフォルトの 48 時間という有効期間を、目的の値に編集または更新できません。</p> <p>autoreissue 有効期間の構成設定について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。</p> <p><a href="https://www.veritas.com/support/ja_JP/article.DOC5332">https://www.veritas.com/support/ja_JP/article.DOC5332</a></p> <p><b>メモ:</b> これは NetBackup 8.0 以前のバージョンの BMR 構成をリストアするための要件ではありません。</p>
指定された IP アドレス <IP address> はホスト名 <Name of the host> に関連付けられていません。正常な検出準備操作のための適切な IP アドレスを指定します。	特定の BMR クライアントの検出準備 (PTD) 操作中に指定した IP アドレスがそのクライアントに関連付けられていない場合、PTD 操作は失敗します。適切な IP アドレスを入力したことを確認する必要があります。
指定された IP アドレスが解決できないため、検出準備操作は成功しません。	検出準備 (PTD) 操作中に指定された IP アドレスが解決できない場合、PTD 操作は失敗します。適切な IP アドレスを入力したことを確認する必要があります。

## Solaris x86 11.2 以降のクライアントのメディアリストアでメンテナンスモードのユーザー名とパスワードを求められる場合がある

Solaris x86 11.2 以降のバージョンがインストールされているクライアントのメディアリストア中、リストアシステムが次のメッセージを表示することがあります。

```
Enter user name for system maintenance (control-d to bypass):
```

同時に、BMR がネットワークアダプタ名の入力を求めます。

```
Enter the network adapter (LINK) name from the above list
corresponding to MAC Address:
```

ネットワークアダプタ名を入力するとその名前はシステムメンテナンスのためのユーザー名として受信され、システムはさらにパスワードの入力を求めます。たとえば、net0 というネットワークアダプタ名を入力すると、次のメッセージが表示されます。

クライアントの PTD タスクが正常に完了した後も検出タスクが完了中の状態のままになることがある

Enter net0 password (control-d to bypass):

この問題は、リストアに重要でない Solaris サービスのいずれかがメンテナンスモードになることで発生します。

回避策: この問題を解決するには、Ctrl+d を押して BMR のリストアを続行します。

## クライアントの PTD タスクが正常に完了した後も検出タスクが完了中の状態のままになることがある

Solaris クライアントでは、クライアントの PTD (Prepare to Discover) タスクが正常に完了した後も、[Bare Metal Restore の管理 (Bare Metal Restore Management)] > [BMR タスク (BMR Tasks)] タブで発見タスクの状態が [完了しています (Finalizing)] と表示される場合があります。

回避方法: タスクの状態を更新するか、タスクを手動で削除します。タスクの状態を手動で更新するには、ターゲットクライアントのマスターサーバーで次のコマンドを実行します。

```
bmr -op complete -resource discovertask -client <clientName> -status 0
```

## クライアントが正常にリストアされても BMR リストアタスクが完了中の状態のまま変わらないことがある

クライアントの BMR (Bare Metal Restore) リストアタスクが正常に完了しても、[Bare Metal Restore の管理 (Bare Metal Restore Management)] > [BMR タスク (BMR Tasks)] タブでタスクの状態が [完了しています (Finalizing)] と表示される場合があります。実行するために構成されている外部プロシージャが、初回ブート時またはクリーンアップ時に実行されていない可能性があります。

回避策: クライアントが正常にリストアされている場合は、次の手順を実行します。

- 1 リストアしたクライアントで、コマンドプロンプトまたはシェルを開きます。
- 2 リストアしたクライアントのオペレーティングシステムに基づいて、コマンドプロンプトまたはシェルで適切なディレクトリに移動します。
  - リストアしたクライアントで Linux を実行している場合は、次の場所に移動します。  
<インストールディレクトリ>/netbackup/bin
  - リストアしたクライアントで Windows を実行している場合は、次の場所に移動します。  
<インストールディレクトリ>%netbackup%bin

共有リソースツリー (SRT) の作成中にブートサーバーとクライアントでバックアップ操作が開始されると、BMR のリストア後に SRT の作成が失敗してエラーが発生する

- 3 次のコマンドの <クライアント名> に正しいクライアントホスト名を入力して実行します。

```
bmrc -op complete -resource restoretask -client <クライアント名>
-status 0
```

- 4 初回ブート時またはクリーンアップ時に外部プロシージャを実行する設定になっている場合は、リストアしたクライアントで外部プロシージャを手動で実行します。

## 共有リソースツリー (SRT) の作成中にブートサーバーとクライアントでバックアップ操作が開始されると、BMR のリストア後に SRT の作成が失敗してエラーが発生する

この問題は、SRT の作成中にバックアップが実行された Windows ブートサーバーとクライアントで発生します。

SRT の作成中、Windows のブート前環境は、<NetBackup Install Path>/BareMetal/Server/Data/BaseSrd パスのステージング領域にマウントされます。この段階でバックアップを作成すると、マウント済みのステージング領域の内容もバックアップされます。リストア後の SRT 作成中にこのようなバックアップのリストアを実行しようとしても、ステージング領域の内容は無効な状態にあるため、マウント解除または削除できません。そのため、SRT の作成は、リストア後に空白のエラーメッセージで失敗する可能性があります。

回避策: SRT の作成中は、ブートサーバーとクライアントのバックアップを作成しないようにします。

意図せずこの問題が発生した場合は、次の手順を実行します。

1. 次のコマンドを実行します。

```
Dism /Get-MountedWimInfo
```

次の例のような出力が表示されます。

```
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
```

共有リソースツリー (SRT) の作成中にブートサーバーとクライアントでバックアップ操作が開始されると、BMR のリストア後に SRT の作成が失敗してエラーが発生する

Mounted Read/Write : No

Status : Invalid

1. 新しい SRT を作成するには、ディレクトリ <NetBackup Install Path>/BareMetal/Server/Data/BaseSrd を削除またはクリーニングする必要があります。

このパスにある dir / files を削除しようとする、エラーメッセージが表示されません。

You require permission from TrustedInstaller to make changes to this file

2. Windows のブート前環境をクリーンアップするには、次のコマンドを実行します。

```
dism /Cleanup-Wim
```

3. クリーニングする <NetBackup Installed

Dir>¥BareMetal¥server¥data¥baseSrd¥EN -x86¥mount¥Windows ディレクトリの所有権を取得します。次の手順を実行します。

- <NetBackup Installed Dir>¥BareMetal¥server¥data¥baseSrd¥EN -x86¥mount¥Windows ディレクトリを右クリックします。
- 右クリックし、[プロパティ]をクリックします。
- [セキュリティ]タブをクリックします。
- [詳細設定]をクリックします。
- [セキュリティの詳細設定]ダイアログボックスで、[所有者]タブをクリックします。現在の所有権の詳細が表示されます。
- [編集]をクリックして、<NetBackup Installed Dir>¥BareMetal¥server¥data¥baseSrd¥EN -x86¥mount¥Windows ディレクトリの所有権を編集および取得します。
- UAC に対する権限を付与します。オブジェクトの所有者として割り当てるユーザーの名前を[所有者の変更]ダイアログボックスから選択します。[OK]をクリックします。  
必要な変更を行うと、同じ内容が[セキュリティの詳細設定]ダイアログボックスに表示されます。
- [OK]をクリックして終了します。
- 1 から 4 の手順を繰り返し、<NetBackup Installed Dir>¥BareMetal¥server¥data¥baseSrd¥EN -x86¥mount¥Windows ディレクトリの [プロパティ] ウィンドウをもう一度開きます。

- <NetBackup Installed Dir>%BareMetal%server%data%baseSrd%EN-x86%mount%Windows ディレクトリの[プロパティ]ウィンドウで[編集]をクリックし、UAC の昇格要求を確認します。
  - [グループまたはユーザー名]ダイアログボックスの[管理者]を選択し、[追加]をクリックして、[選択するオブジェクト名を入力してください]ダイアログボックスで管理者のユーザー名を入力し、[OK]をクリックして完了します。
  - [管理者のアクセス許可]ダイアログボックスで、[許可]列の下にある[フルコントロール]をクリックし、[管理者]グループにフルコントロールのアクセス権限を割り当てます。
4. <NetBackup Installed Dir>%BareMetal%server%data%baseSrd%EN-x86%mount%Windows ディレクトリを削除します。
  5. SRT の作成操作を再試行します。

## バックアップ時に BMR 情報の受信中に発生するエラー

NetBackup バージョン 9.1.0.1 以降で、クライアント RHEL 8.4 のバックアップ時に Bare Metal Restore 情報を受信中に発生するエラーです。

### エラーメッセージ

- 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@gf0vsxas024i logs]# /usr/opensv/netbackup/bin/bmrsavecfg -infoonly
```

```
sh: /bin/netstat: No such file or directory
```

```
sh: /sbin/ifconfig: No such file or directory
```

### 原因

発生したエラーをログで確認すると、問題が `ifconfig` と `netstat` の使用に関連していることがわかります。この 2 つのコマンドは、RedHat 8.3 および RedHat 8.4 では非推奨で

BMR のバックアップジョブとリストアジョブの詳細が NetBackup Web UI のアクティビティモニターに表示されない

す。これは `net-tools` パッケージがインストールされている場合に使用できますが、デフォルトでは存在しません。この 2 つのコマンドは、それぞれ IP および SS に置き換えられています。

共通の実行可能ファイル `netstat` および `ifconfig` は、Red Hat 8.4 クライアントにインストールされません。

ポリシーの BMR オプションによって `bmrsavecfg` を呼び出し、クライアントで実行すると、実行可能ファイルが呼び出されますが、その実行可能ファイルが見つかりません。

## 解決方法

バックアップ操作時にエラーを発生させずに BMR 情報を受信するには、次の手順を行います。

- `net-tools` パッケージをインストールします。
- オペレーティングシステムから実行可能ファイルを手動でインストールします。
- バックアップジョブを再度実行します。

# BMR のバックアップジョブとリストアジョブの詳細が NetBackup Web UI のアクティビティモニターに表示されない

`bmrsetupmaster` コマンドの実行後に、BMR のバックアップジョブとリストアジョブの詳細が NetBackup Web UI のアクティビティモニターに表示されません。

この状況は、`bmrsetupmaster` コマンドの実行後に、NetBackup データベースのパスワードがリセットされるために発生します。

対処方法: `bmrsetupmaster` コマンドの実行後、NetBackup データベースのパスワードがリセットされます。そのため、NetBackup Web API を NetBackup データベースに接続して、パスワードの設定機能を実行します。技術的な制限があるため、NetBackup サービスを再起動する必要があります。この操作は、BMR プライマリサーバーの構成後の NetBackup Web API のパフォーマンスに役立ちます。

# クライアントバックアップからの 仮想マシンの作成

この章では以下の項目について説明しています。

- [バックアップからの仮想マシンの作成について](#)
- [BMR 物理マシンに対する仮想マシンの作成の利点およびユースケース](#)
- [仮想マシン作成のための配置ダイアグラム](#)
- [クライアント-VM 変換プロセスのフロー](#)
- [バックアップから VM を作成する際の前提条件](#)
- [バックアップからの仮想マシンの作成](#)
- [仮想マシン作成の CLI](#)

## バックアップからの仮想マシンの作成について

NetBackup BMR は、完全、合成、増分および PIT (特定時点) バックアップからのダイレクトな仮想マシン (VM) 作成 (物理から仮想) をサポートします。この VM 作成は BMR ブートサーバーおよび共有リソースツリーセットアップを必要としません。プラットフォームサポートマトリックスについて詳しくは、付録セクションの p.259 の「[BMR における直接 VM 変換のサポート表](#)」を参照してください。を参照してください。

この機能は、仮想マシンに対する容易なウィザードベースまたは単一 CLI ベースのディザスタリカバリ (DR) をサポートします。VM の作成は、NetBackup 自動イメージレプリケーション (A.I.R.) サポートを使用して DR ドメインでも可能です。ユーザーが仮想マシンレイアウトを作成する必要がない場合や、BMR 方式を使って異なるシステムリカバリを行うときにはこの機能がサーバーレベル DR を実行するように技術的知識のないユーザーを支援します。作成されたクライアントの仮想マシンを見つけ、自動的にブートする

には、物理マシンから仮想マシンの作成ウィザードまたは単一のコマンドラインを実行してください。

## BMR 物理マシンに対する仮想マシンの作成の利点およびユースケース

VM 作成プロセスへのクライアントは、以下の主な利点およびユースケースを提供します。

- インスタント一時 DR メカニズムとして使用できます。
- リカバリの仮想マシンの利用によって OPEX を下げます。
- NetBackup A.I.R. (自動イメージレプリケーション) を有効化して、DR ドメインでプライマリドメインクライアントの素早いリカバリを実行します。自動イメージレプリケーションの有効化について詳しくは、『[NetBackup Web UI 管理者ガイド](#)』を参照してください。
- 使いやすい VM 変換ウィザードにより、RTO (Recovery Time Objective) を短縮するだけでなく、またシステム回復の前提条件の準備を必要としません。
- コンプライアンスおよびファイアドリルのテストをするのに使うことができます。
- 完全、増分、合成バックアップイメージから VM の作成をサポートします。
- 指定時点バックアップイメージからの VM の作成をサポートします。
- 次のような異なる優先設定を提供することにより、VM 作成の柔軟性を提供します。
  - システムのみのリストア: OS ボリュームだけで VM を作成するオプションを提供します。
  - 既存の VM の上書き: 同じ名前での既存の VM を自動的に上書きできます。
  - 作成の後の自動ブート VM: 選択されたとき、VM 作成プロセスは作成後に自動的に VM ブートします。
  - 必須の仮想化ストレージエンティティに個々の仮想ディスクをマップする柔軟性。
  - ネットワークstripping: VM の元のクライアントネットワークインターフェースおよび IP 構成を削除するオプション。
- 選択したディスクのみで VM を作成するオプションを提供します。
- クライアント VM 作成をトリガする単一のコマンドライン機能を提供します。

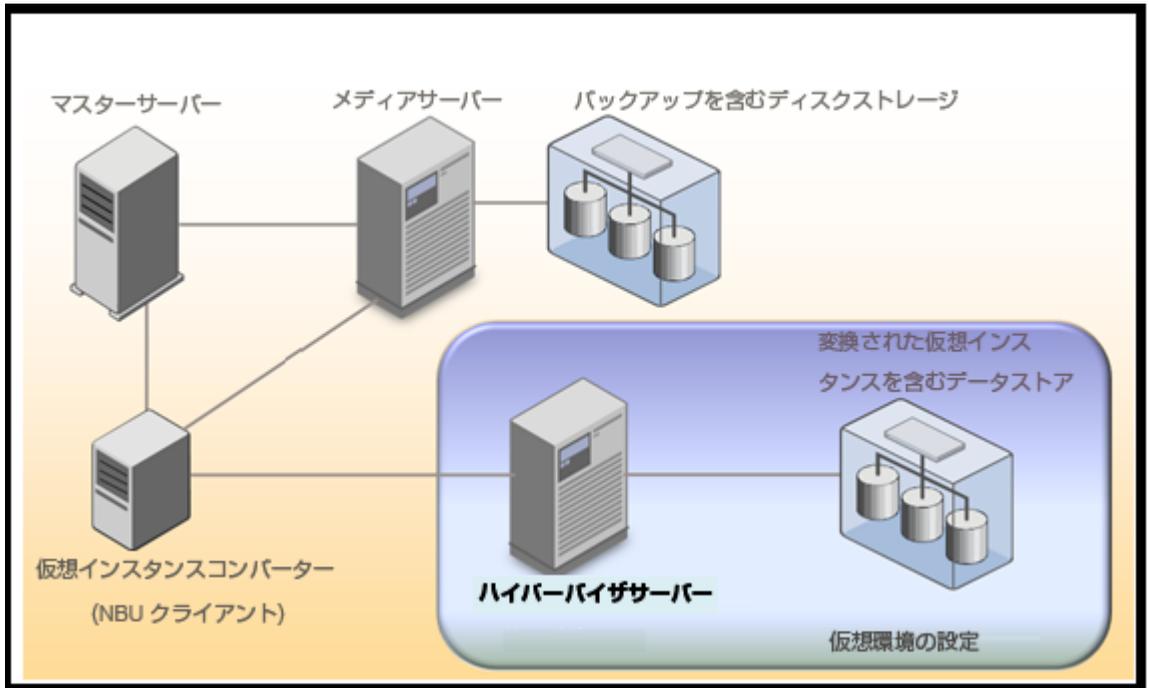
---

**メモ:** 増分データリストアは現在現在サポートされていません、しかし、増分バックアップからの新しい VM の作成が可能です。

---

## 仮想マシン作成のための配置ダイアグラム

以下は、仮想マシン変換までの BMR のクライアントの一般的な配置ダイアグラムです。



マスターサーバー: BMR がクライアントの有効化したバックアップを取る NetBackup プライマリサーバー。

メモ: BMR のマスターサーバーを構成し、BMR クライアント保護を有効にすることについては、以下のセクションを参照してください。

p.17 の「[BMR マスターサーバーの構成](#)」を参照してください。

p.23 の「[BMR クライアントをバックアップするためのポリシーの構成](#)」を参照してください。

メディアサーバー: クライアントの BMR を含む NetBackup メディアサーバーは、ディスクベースのストレージユニットのバックアップイメージを有効化します。

仮想インスタンスのコンバーター (VIC): このホストは NetBackup のクライアントを構成した NetBackup リカバリのホストです。BMR クライアントから VM への変換では、VIC オペレーティングシステムを要求し、クライアントのオペレーティングシステムと同じファミリー

に属し、仮想マシンに変換する必要があります。たとえば、Windows ベースの VIC では、Windows ベースのクライアントの VM を作成できます。

ハイパーバイザサーバー: クライアントの VM が作成される宛先の仮想サーバー。仮想マシン変換ウィザードの実行中に、対象のハイパーバイザサーバーを選択する必要があります。

---

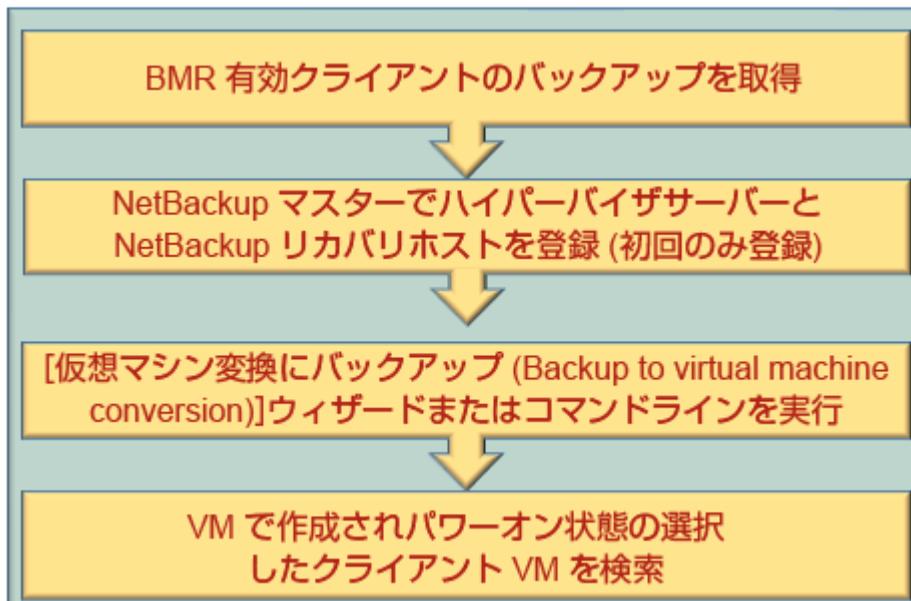
**メモ:** VIC ホストのための余分なハードウェアを必要としません。VIC ホストは仮想マシンに任意に構成できます。

---

サーバー OS が変換されるクライアントの OS ファミリーと同じ OS ファミリーの場合、VIC はまたプライマリまたはメディアサーバーにサーバー上に構成することもできます。しかし、VM 作成プロセスはリソースを消費し、NetBackup サーバーのパフォーマンス速度を低下させることがあるため、NetBackup プライマリまたはメディアサーバーに VIC をセットアップすることはお勧めしません。仮想マシンの変換操作で現在サポートされているハイパーバイザサーバーについては、p.258 の「BMRによる仮想環境のサポート」を参照してください。

## クライアント-VM 変換プロセスのフロー

次の図は、クライアントから VM へ変換するプロセスを簡単に表したプロセスフローです。



## バックアップから VM を作成する際の前提条件

以下はバックアップから仮想マシンを作成する際の前提条件です。

- **BMR** プライマリサーバーの設定  
最初に、NetBackup プライマリサーバーの BMR サーバーを有効にする必要があります。BMR サーバーを有効にする方法については、次のトピックを参照してください。  
p.17 の「[BMR マスターサーバーの構成](#)」を参照してください。
- クライアントの BMR バックアップの有効化  
BMR の NetBackup のポリシーを設定してください。ポリシー属性の[ディザスタリカバリ情報の収集 (Collect disaster recovery information)]オプションで、BMR のチェックボックスにチェックマークを付けます。詳細が利用可能です。  
p.23 の「[BMR クライアントをバックアップするためのポリシーの構成](#)」を参照してください。
- BMR のバックアップポリシーには、バックアップ対象の一部として、OS ボリュームが追加されている必要があります。Windows システムの場合、バックアップ対象リストに、ブート、システムボリューム、システム状態を追加する必要があります。

---

**メモ:** ユーザーの便宜上、バックアップ対象には、デフォルトで ALL\_LOCAL\_DRIVES オプションを選択できます。この指示句はバックアップ時にすべてのクライアントボリュームを考慮します。

---

バックアップポリシーの BMR を有効にした後で、最初の完全バックアップを実行します。

- ハイパーバイザ固有ツールの ISO ファイル  
VM の作成プロセスでは、VM の作成中に VM システムに必須のデバイスドライバを構成するために、ハイパーバイザ固有ツールの ISO ファイルが必要です。通常、ハイパーバイザのベンダーは Web サイトやハイパーバイザサーバーでツールの ISO ファイルを提供します。たとえば、VMware ESX Server 5.0 の場合、関連ツールの ISO ファイルは、ESX Server に用意されているか、VMware Web サイトからダウンロードできます。  
ESX Server でのツールの ISO パス: /vmimages/tools-isoimages/windows.iso  
Web サイトの URL:  
[http://packages.vmware.com/tools/esx/5.0latest/windows/x86\\_64/index.html](http://packages.vmware.com/tools/esx/5.0latest/windows/x86_64/index.html)  
VIC ホストに、ツールのこの ISO ファイルが配置されている必要があります。仮想マシン作成ウィザードでは、VIC で利用可能なこの ISO ファイルの完全ディレクトリパスの入力を求めるメッセージが表示されます。
- NetBackup でのハイパーバイザサーバー名の登録

VM のバックアップを作成する必要がある NetBackup に、ハイパーバイザサーバーを登録する必要があります。登録には、ハイパーバイザサーバーの **admin** クレデンシャルが必要です。

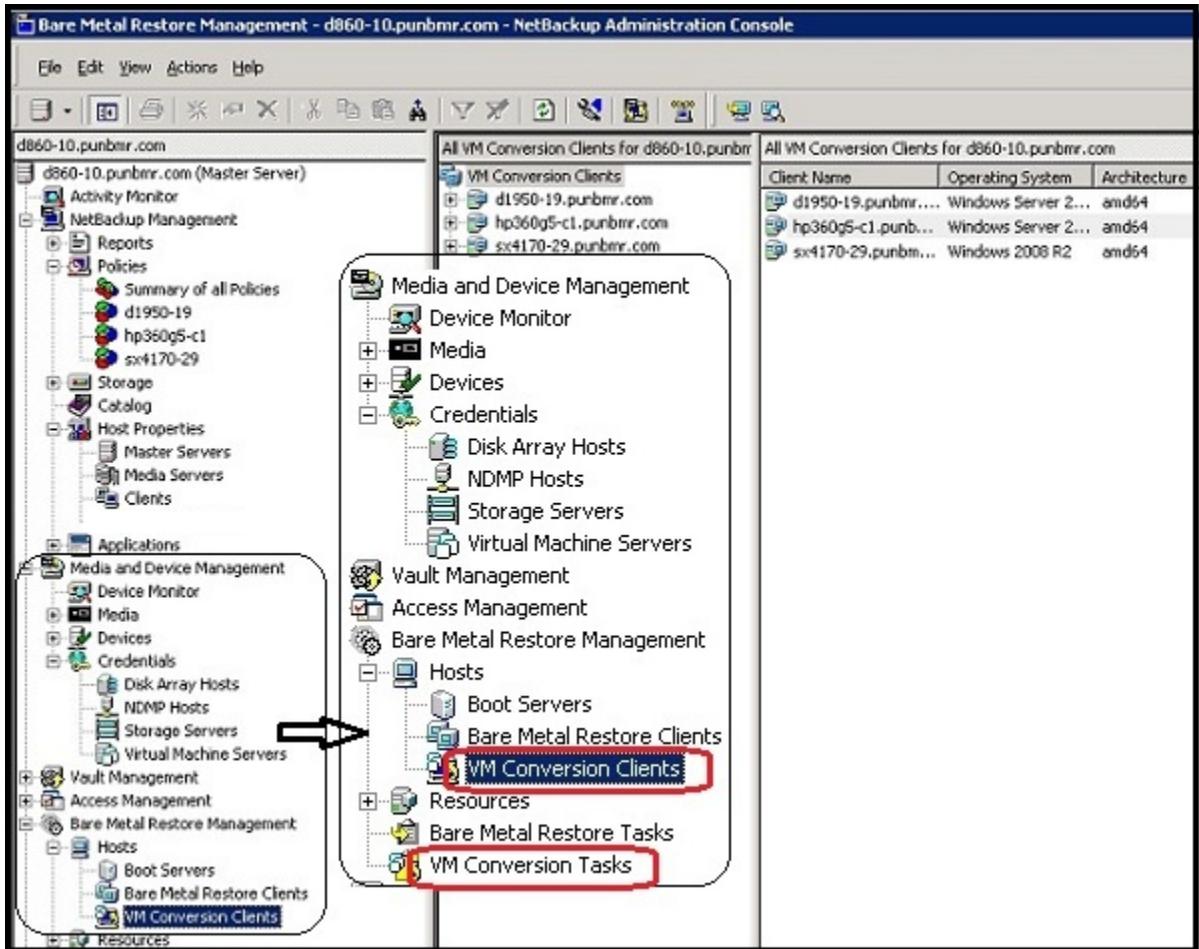
- NetBackup での VIC (NetBackup リカバリホスト) 名の登録  
VMware のハイパーバイザの場合、仮想イメージコンバータのホスト名は、プライマリサーバーの [VMware アクセスホスト (VMware access host)] のホストプロパティで登録する必要があります。

## バックアップからの仮想マシンの作成

以降のセクションで、バックアップからクライアントの VM を作成するプロセスについて詳しく説明します。

### 仮想マシン変換クライアント

NetBackup 管理コンソールでは、タブにおいて [Bare Metal Restore の管理 (Bare Metal Restore Management)] > [VM 変換クライアント (VM Conversion Clients)] パネルが、仮想マシン (VM) への変換が可能なすべてのクライアントを取りまとめます。オペレーティングシステムタイプ、CPU、RAM、ホストおよびネットワーク関連の情報といったクライアントの各種詳細を確認できます。

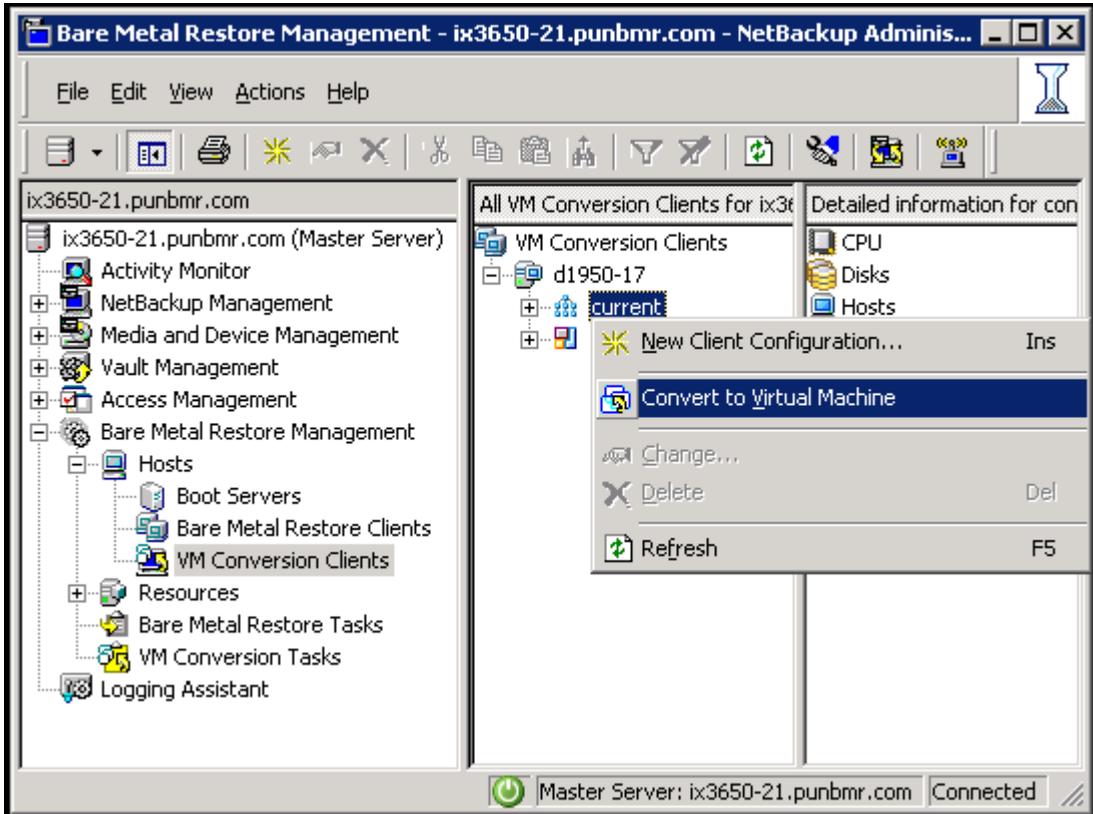


## クライアントバックアップを VM に変換する

仮想マシン変換ウィザードを使用して BMR 有効バックアップを仮想マシンに変換できます。NetBackup Web UI では、同様のウィザードを使用できます。

仮想マシンへのクライアントバックアップの変換に関する操作を開始するには、次の作業を行います。

- 1 NetBackup コンソールの VM 変換クライアントパネルにナビゲートします。
- 2 変換操作オプションのポップアップメニューを取得するには、意図するクライアント構成で右クリックします。



必要に応じて、VM 作成に対してカスタムクライアント設定または PIT (特定時点) 設定を作成できます。そのようなケースでは、[新しいクライアントの構成 (New Client Configuration)] オプションを使用して PIT 設定を作成するか、または既存のクライアント設定をコピーします。クライアント構成を変更する方法については、p.238 の「カスタム構成の作成」を参照してください。を参照してください。

- 3 変換プロセスウィザードを開始するには、変換操作ポップアップメニューで[仮想マシンに変換 (Convert to Virtual Machine)]をクリックします。

このウィザードは宛先 Hypervisor サーバーパラメータおよび変換オプションについての詳細メッセージを表示します。

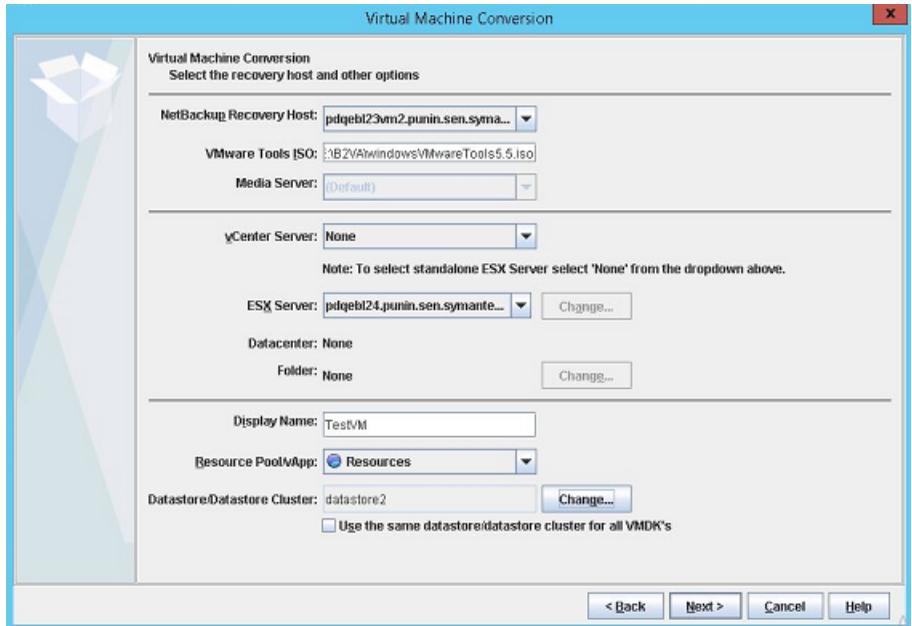
VMware ベースの VM 変換ウィザードのフロー

ウィザードの最初ページは、VMware サーバーパラメータ、VIC ホスト詳細についての情報をユーザーに確認します。

表 11-1 仮想マシンへの変換

パラメータ	パラメータの詳細
NetBackup リカバリホスト:	これは VIC (仮想インスタンスコンバーター)、つまりリカバリホストとして使用される NetBackup クライアントホスト名です。このホストは意図される VMware サーバーで VM を準備します。  <b>メモ:</b> VIC OS には、VM に変換されているクライアントに Windows ベースのファミリーがある場合、Windows ベースの VIC を設定しなければならないというルールがあります。この OS ルールが満たされる場合、VIC が物理または仮想マシンで設定できます。ただし、仮想マシン作成プロセスがリソースを消費し、NetBackup Server パフォーマンスを遅くする可能性がある場合、NetBackup プライマリサーバーまたはメディアサーバーで VIC をセットアップすることは推奨されません。
VMware Tools ISO ファイル:	VMWare .iso ファイルがこのダイアログボックスで先に入力された VIC ホストにある場合、絶対パスを入力してください。  詳しくは、p.227 の「バックアップから VM を作成する際の前提条件」を参照してください。を参照してください
vCenter Server:	該当する場合、vCenter Server 名を選択します。
ESX Server:	ESX Server 名を選択または入力します。
VMware フォルダ:	宛先仮想マシンが作成されるフォルダ。
表示名:	作成されるべき仮想マシンの表示名を入力します。
リソースプール:	ドロップダウンメニューから意図するリソースプール名を選択します。
データストア / データストアクラスタの状態:	ESX Server に接続されたストレージがあります。[すべての VMDK に同じデータストア / データストアクラスタを使用する (Use the same datastore/datastore cluster for all VMDKs)] オプションを選択する場合、VM に属するすべての V ディスクが同じデータストアまたはデータストアクラスタに作成されます。このオプションが選択されない場合、このウィザード後の画面で、個々の V ディスクをデータストアでマップするオプションを提供します。

先に説明されたポピュレート済みパラメータを示す次のサンプルダイアログボックススナップショットを参照してください。詳しくは次のスクリーンショットを参照してください。



## [仮想マシン (Virtual Machine)] のオプション

次のウィザードページは VM 変換オプションを提供するためにメッセージを表示し、仮想ディスクの種類を選択を可能にします。続く表は、VM およびディスクの種類と関連している必要なすべてのオプションを取りまとめます。

表 11-2 [仮想マシン (Virtual Machine)] のオプション

### 仮想マシンオプション (Virtual Machine Options)

既存の VM を上書きする  
(Over-write existing VM):

表示名を複製する場合には既存の仮想マシンの削除を有効にするため、このオプションを選択してください。同じ表示名を持つ仮想マシンが宛先にある場合、リストアが始まる前にその仮想マシンが自動的に削除されます。そうでない場合、リストアに失敗します。このオプションを選択しない場合、重複する VM 名を手動で削除する必要があります。

ネットワークインターフェースの削除  
(Remove network interfaces):

このオプションが選択されると、元のクライアントネットワークインターフェースは宛先で設定されません。このオプションを選択しない場合、コピー元のクライアント構成で存在するネットワークインターフェースおよび詳細と同じ数が VM で設定されます。

リカバリ後に仮想マシンの電源をオン (Power on virtual machine after recovery): リカバリの完了時にリカバリされた仮想マシンに自動的に電源が入るようにする場合は、このオプションを選択します。

システムディスクとボリュームのみをリストアする (Restore system disks and volumes only): VM で OS のみリカバリを必要とする場合、OS ディスクボリュームをリストアするにはこのオプションを選択します。

### 仮想ディスクの種類

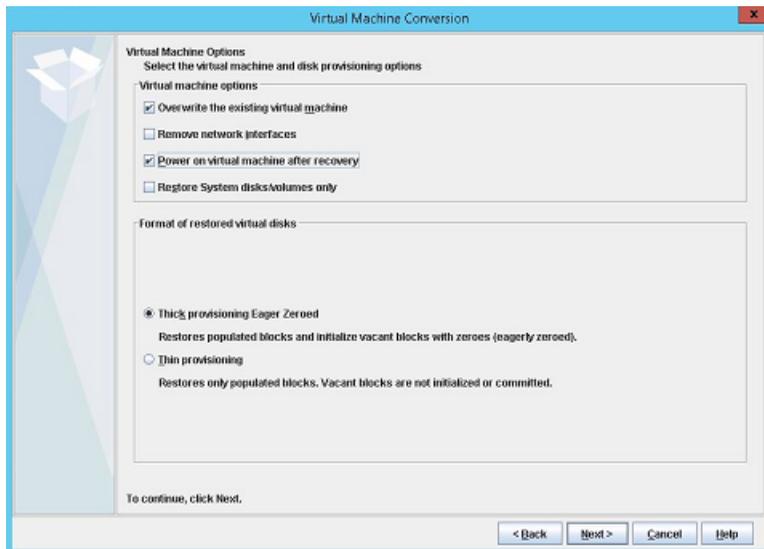
シンプロビジョニング (Thin Provisioning):

リストアされた仮想ディスクをシン形式で設定するには、このオプションを選択します。シンプロビジョニングは vmdk ファイルの動的拡張を介してディスク領域を節約します。vmdk ファイルは仮想マシンのデータが必要とする領域より大きくありません。仮想ディスクのサイズは必要に応じて自動的に増加します。

シックプロビジョニング (Thick Provisioning):

リストアされた仮想ディスクをシック形式で設定するには、このオプションを選択します。VM の物理ディスクの長さと同等の仮想ディスクの長さを作成します。このオプションを使用すると仮想ディスクの作成により時間がかかることがあります。

VM オプションを示す次のサンプルスナップショットを参照してください。

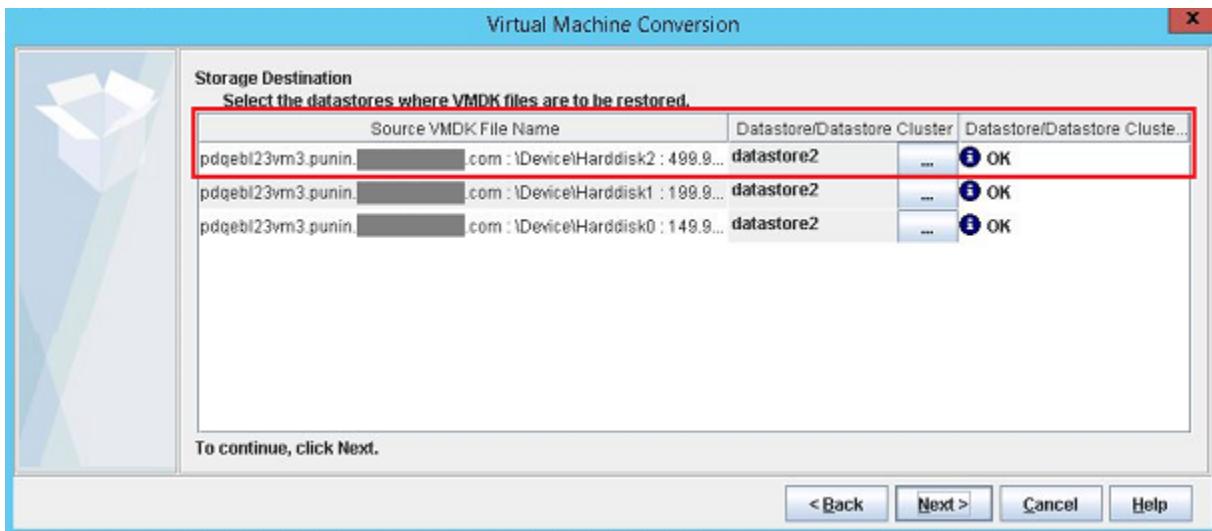


## 仮想マシン変換ストレージ先

VM 変換ストレージウィザードでは、仮想マシンに変換されるクライアントに属するすべてのディスクをリストします。これにより、対応するデータストアにおいてリカバリ処理が同等の VMDK ファイルを作成する個々のディスクを使用してマップされるべきデータストアを選択可能にします。

**メモ:** [VM への変換 (Conversion to VM)]ウィザードのオプション[すべての VMDK に同じデータストア/データストアクラスターを使用する]をチェックしている場合、ストレージ先はすでに選択されています。

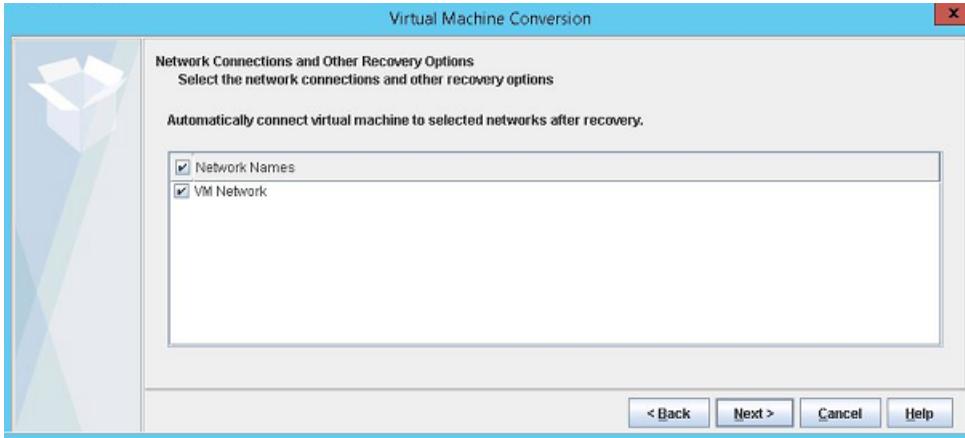
ストレージ先の詳細については、次のサンプルスクリーンショットを参照してください。



## ネットワーク接続の選択

仮想ネットワークに属する VM のネットワークインターフェースを作成するために VMWare ネットワーク接続名を選択できます。ウィザードではすべての利用可能なネットワーク接続をリストします。

選択できるネットワーク名を表示する次のサンプルスクリーンショットを参照してください。



## 仮想マシン変換の概略

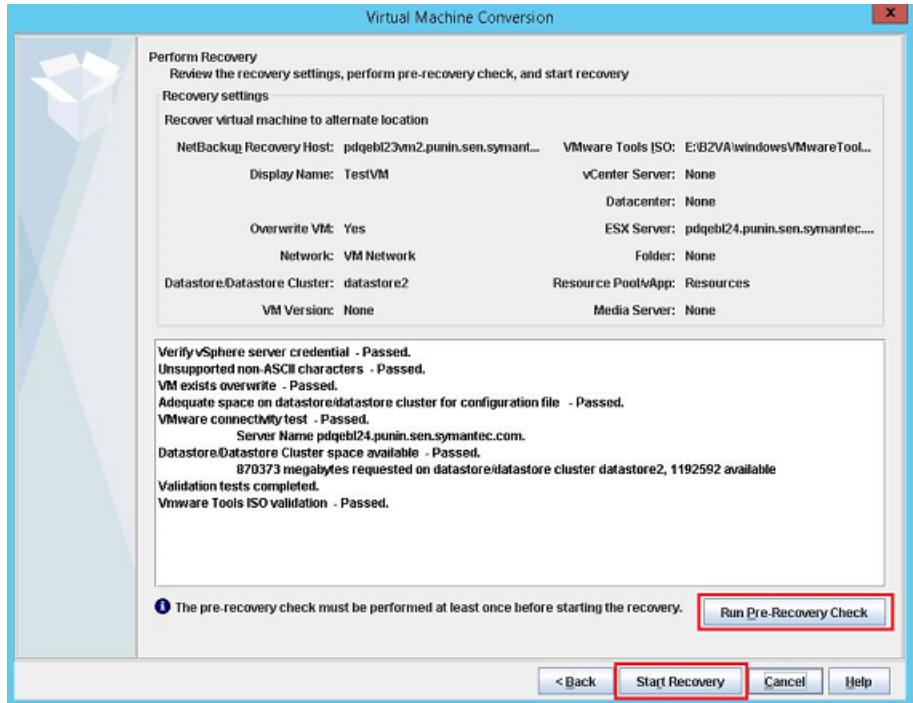
概要ページは VM 変換ウィザードを通して設定されるクライアント変換と関連しているすべての詳細を表示します。

環境の詳細がそのまま完全であることを確認するために事前チェックを実行してください。すべての環境の設定がそのまま完全である場合、検証テストは **Passed** として状態を示します。

**NetBackup** プライマリサーバーを通して VM 作成プロセスのためのタスクを作成するには [リカバリの開始 (Start Recovery)] をクリックします。[Bare Metal Restore の管理 (Bare Metal Restore Management)] タブの下の [VM 変換タスク (VM Conversion Tasks)] にリストされるタスクをチェックし、進行状況を知るにはタスク状態および操作を参照してください。

タスクおよび状態情報の詳細については、**Bare Metal Restore** タスクのモニタリングの章を参照してください。

次のサンプル概略画面を参照してください。



## リストアの完了後に実行される直接仮想マシン (VM) の変換 (物理から仮想) タスク

NetBackup 8.1.1 以降のリリースでは、Windows クライアントの場合、直接仮想マシン (VM) の変換 (物理から仮想) 中にリストアが正常に完了した後、リストアされたクライアントで認証局 (CA) の証明書およびホスト ID ベースの証明書を手動で配備する必要があります。

### ホスト ID ベースの証明書を手動で生成して配備する方法

- 1 操作を続行する前に、ホスト管理者が認証トークン値を CA から取得している必要があります。トークンは各環境のさまざまなセキュリティガイドラインに応じて、電子メール、ファイル、または口頭で管理者に伝えられます。
- 2 マスターサーバーが信頼できる状態を確立するためにマスター以外のホストで次のコマンドを実行します。

```
nbcertcmd -getCACertificate
```

- 3 マスター以外のホストで次のコマンドを実行して、メッセージが表示されたらトークンを入力します。

```
nbcertcmd -getCertificate -token
```

---

**メモ:** 複数の NetBackup ドメインと通信するには、そのホストの管理者が `-server` オプションを使って各マスターサーバーから証明書を要求する必要があります。

---

管理者がトークンをファイルで取得した場合、次を入力します。

```
nbcertcmd -getCertificate -file authorization_token_file
```

- 4 証明書がホストに配備されていることを検証するには、次のコマンドを実行します。

```
nbcertcmd -listCertDetails
```

クラスタの証明書を表示するには、`-cluster` オプションを使用します。

ホスト ID ベースの証明書の配備方法について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「ホスト ID ベースの証明書の配備」を参照してください。

[https://www.veritas.com/support/en\\_US/article.DOC5332](https://www.veritas.com/support/en_US/article.DOC5332)

## 仮想マシン変換タスク

仮想マシンの変換ウィザードで、[仮想マシンに変換 (Convert to Virtual Machine)] をクリックすると仮想マシン作成プロセスのためのタスクを作成します。このタスクの状態は [仮想マシン変換タスク (Virtual Machine Conversion Tasks)] タブにおいてチェックでき、タスク操作をチェックすれば進行状況を確認できます。

タスクおよび状態情報について詳しくは、「Bare Metal Restore タスクのモニタリング」の章を参照してください。

## リストアタスクのプロパティ

[リストアタスクのプロパティ (Restore Task Properties)] ダイアログボックスは、いわゆるクライアント VM 変換の全般的設定およびリカバリオプションについてのすべてのパラメータの概略を示します。概略には、VM 名、vCenter Server、VMware Tools ISO ファイルの場所、および VMDK 用データセンターといった仮想マシン変換設定も含んでいます。また、設定されたネットワークパラメータもリストし、ディスクタイプもリストアします。

タスクおよび状態情報について詳しくは、「Bare Metal Restore タスクのモニタリング」の章を参照してください。

## カスタム構成の作成

新しいクライアント構成を作成する場合、PIT VM 作成のため既存のクライアント構成または特定時点 (PIT) の構成ポリシーのいずれかをコピーできます。次のため、カスタマイズされた構成の作成が必要となります：

- コピー構成の作成: 元の構成をカスタマイズするため、既存の変換用のクライアント構成をコピーできます。クライアントプロパティ、すなわちRAM サイズ、割り当て済みの CPU ユニット、VM で作成されるべきディスク、およびネットワークパラメータをカスタマイズできます。

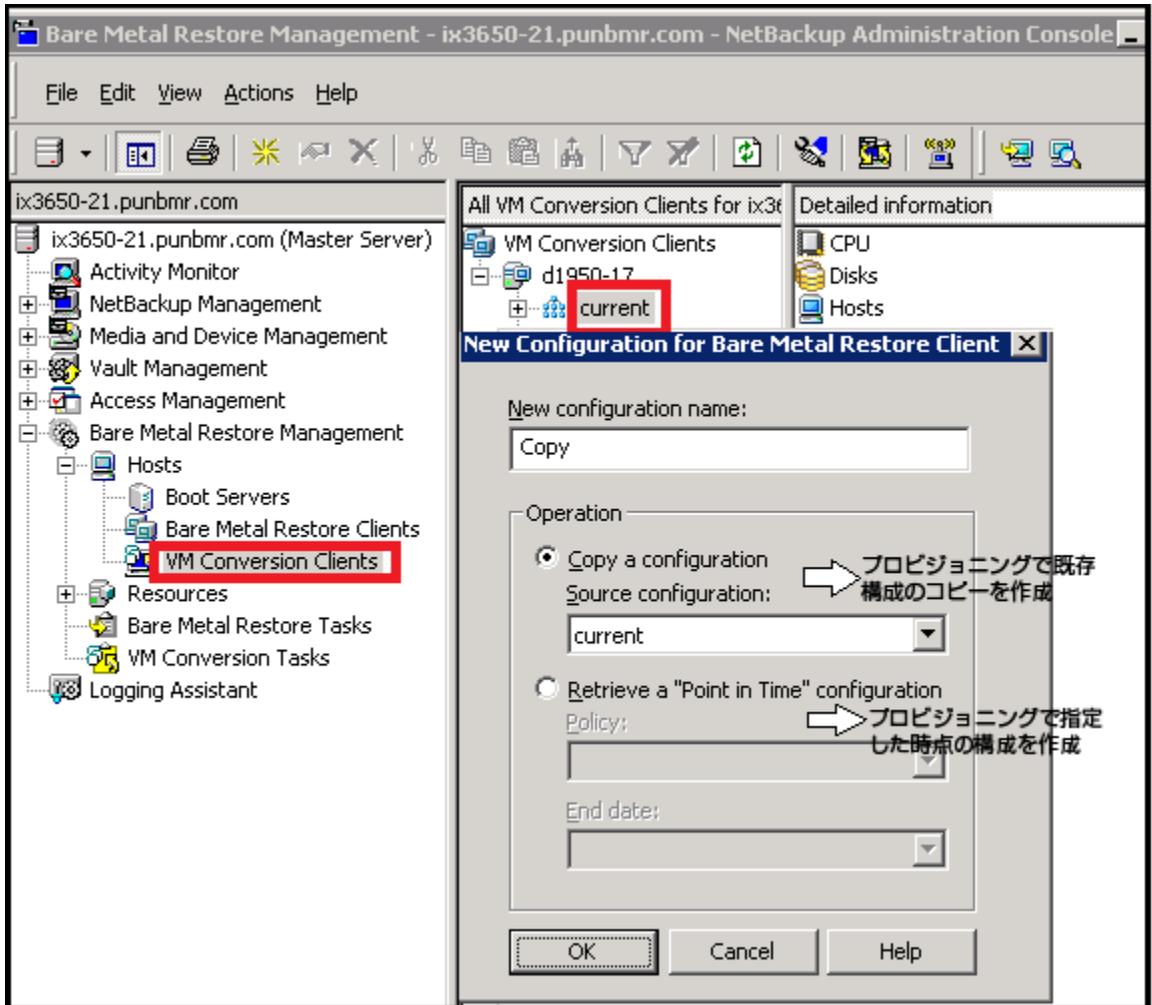
VM のすべての元のディスクまたはボリュームを回復したくない場合、このカスタマイズプロビジョンが役立ちます。この場合、VM 作成中に対応する仮想ディスクの作成を回避するために、望ましくないディスクに制限付きとしてマーク付けすることができます。

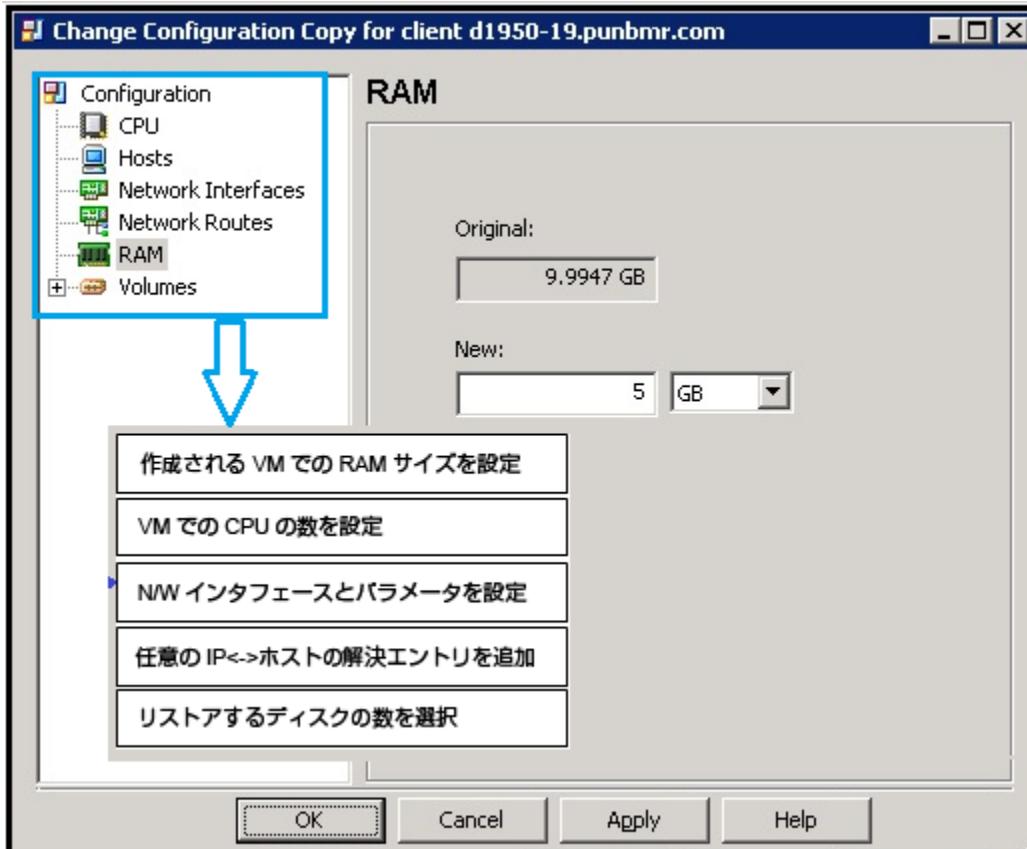
---

**メモ:** OS ディスクを制限していないことを確認してください。そうしないと、作成された VM はブートしません。

---

- PIT バックアップからの特定時点 (PIT) VM 作成: バックアップイメージのための PIT 構成を取り込むことができます。NetBackup Web UI から、PIT 構成を取得してコピーすることもできます。





詳しくは、クライアントおよび構成の管理の章を参照してください。

## 仮想マシン作成の CLI

コマンドラインインターフェースを使用して、クライアントバックアップから VM 作成に関連するさまざまな操作を行うことができます。

- バックアップからの VM 作成ジョブの開始  
マスターサーバーまたは管理者特権を持つ任意のクライアントから `nbrestorevm` コマンドを使用して VM 作成のためのジョブを開始します。パラメータなしで `nbrestorevm` を実行した場合には次のようなヘルプが表示されます。

VM リストアの場合:

```
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] [-vmtid] [-vmfd] [-vmbz] [-vmdrs] [-vmpdrs] [-vmvxd]
[-vmkeephv] [-vmid] [-vmsn] [-vmrb] [-force] [-vcd] [-vcdred]
[-vcdovw] [-vcdрте] [-vcdtemplate] [-vcdlfree] [-vcdremv]
[-ir_activate] [-temp_location temp_location_for_writes]
[[-ir_deactivate | -ir_reactivate | -ir_done]
instant_recovery_identifrier] [-ir_reactivate_all [-vmhost vm_host]
[-media_server media_server_activate_vm]] [-ir_listvm]
```

**BMR の VM を変換する場合:**

```
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]
```

手順の詳細,

**-vmw : VMWare**

**-C: VM に変換されるクライアントの名前**

**-S: マスターサーバーの名前**

**-O: 同じ名前のものがすでに存在する場合は VM を上書きするオプション**

**-vmserver: vCenter または ESX サーバー名**

**-vmproxy: 仮想イメージコンバータまたは NB プロキシの名前**

**-veconfig: 仮想環境の詳細を含んでいるファイル絶対パス**

**-vmpo: [省略可能]指定しておけば VM に自動的に電源が入る**

例:

```
nbrestorevm -bmr -vmw -C dl1950-17.punbmr.com -vmserver
bmrh10.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
```

**-veconfig** ファイルの詳細。

たとえば、**C:\B2V\veconfig.txt** はパラメータ=値の形式で次の情報を含んでいます。

```
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)"
```

- VM 作成ジョブの追跡

次の CLI を使うと送信した VM 作成ジョブを追跡できます。

マスターサーバーで、開始したジョブで実行状態になっているものをリストするには、次のように実行します。

```
<C:¥Program Files¥Veritas¥NetBackup¥bin>bmrs -operation list  
-resource B2VrestoreTask
```

マスターサーバーで、VM 作成ジョブの履歴 (失敗したか正常に完了したか) をリストするには、次のように実行します。

```
<C:¥Program Files¥Veritas¥NetBackup¥bin>bmrs -operation list  
-resource B2VrestoreTaskLog
```

- VM 作成に関連するタスクログの削除

マスターサーバーの場合、データベースからログをクリーンアップするには、次のように実行します。

```
<C:¥Program Files¥Veritas¥NetBackup¥bin>bmrs -o delete -resource  
b2vrestoretasklog -id <p2vRestoreTaskLogId>
```

タスクログのキーワードのリスト操作でコマンドを使用することによって、**p2vRestoreTaskLogId** を取得することができます。

詳しくは、『[NetBackup コマンドリファレンスガイド](#)』を参照してください。

# Bare Metal Restore アクティビティの監視

この章では以下の項目について説明しています。

- [BMR リストアタスクの監視](#)
- [バックアップジョブの監視](#)
- [VM 作成ジョブの監視](#)
- [BMR ログ](#)

## BMR リストアタスクの監視

[タスク (Tasks)] ウィンドウには、タスクの状態、リストア準備のリソース割り当て状況、検出準備の操作状況が表示されます。

## BMR リストアタスクを監視する方法

- 1 NetBackup Web UI で、[Bare Metal Restore]、[BMR タスク (BMR Tasks)]の順に選択します。

[更新 (Refresh)] オプションを使用すると、マスターサーバーから新しい情報を取得して詳細ペインが更新されます。項目を選択すると、その項目のみが更新されます。

次のスクリーンショットは、クライアントポスト PTR (リストア準備操作) のために作成されるリストアタスクを示しています。タスクの状態は、クライアントが BMR リカバリの準備ができていることを示しています。

Client	Configur...	Shared R...	State	Operation	Status	Start Time	End Time	Type
rh20.punb...	current	DynaEFI	Done		0	12/7/2012...	12/7/2012...	Restore
rh20.punb...	PIT_First...	EFI_SRT2	Done		0	12/6/2012...	12/7/2012...	Restore
rh20.punb...	PIT_First...	EFI_SRT2	Done		0	12/5/2012...	12/5/2012...	Restore
rh20.punb...	current	SRT_EFI	Done		0	12/3/2012...	12/3/2012...	Restore
win2k8mbr...	Copy	SPWLog	Done		0	12/11/201...	12/12/201...	Restore
win2k8mbr...	current	SPWLog	Done		0	12/11/201...	12/11/201...	Restore
hp360g5-c...	current	SPW1	Done		0	12/11/201...	12/11/201...	Restore
hp360g5-c...	current	SPW1	Done		0	12/10/201...	12/10/201...	Restore
vm2k8x64...	current	EFIMMSRT	Active	Finalizing		12/12/201...		Restore
rh20.punb...	current	SRT_EFI	Queued	Ready		12/12/201...		Restore

- 2 タスクの詳細を表示するには、[詳細 (Detail)] ペインにあるタスクを右クリックして、[プロパティ (Properties)] を選択します。

また、タスクを管理するために次の他のオプションのいずれかを選択できます。

クリーンアップ (Clean-up)      タスクで使用されていたリソースの割り当てが解除され、[タスクの状態 (State)] が [完了 (Done)] に、[状態 (Status)] が [150] (ユーザーにより終了) に設定されます。

タスクの状態が [有効 (Active)] または [待機しています (Waiting)] になっているタスクはクリーンアップできます。

削除 (Delete)      タスクの状態が [完了 (Done)] になっているタスクは削除できます。

## バックアップジョブの監視

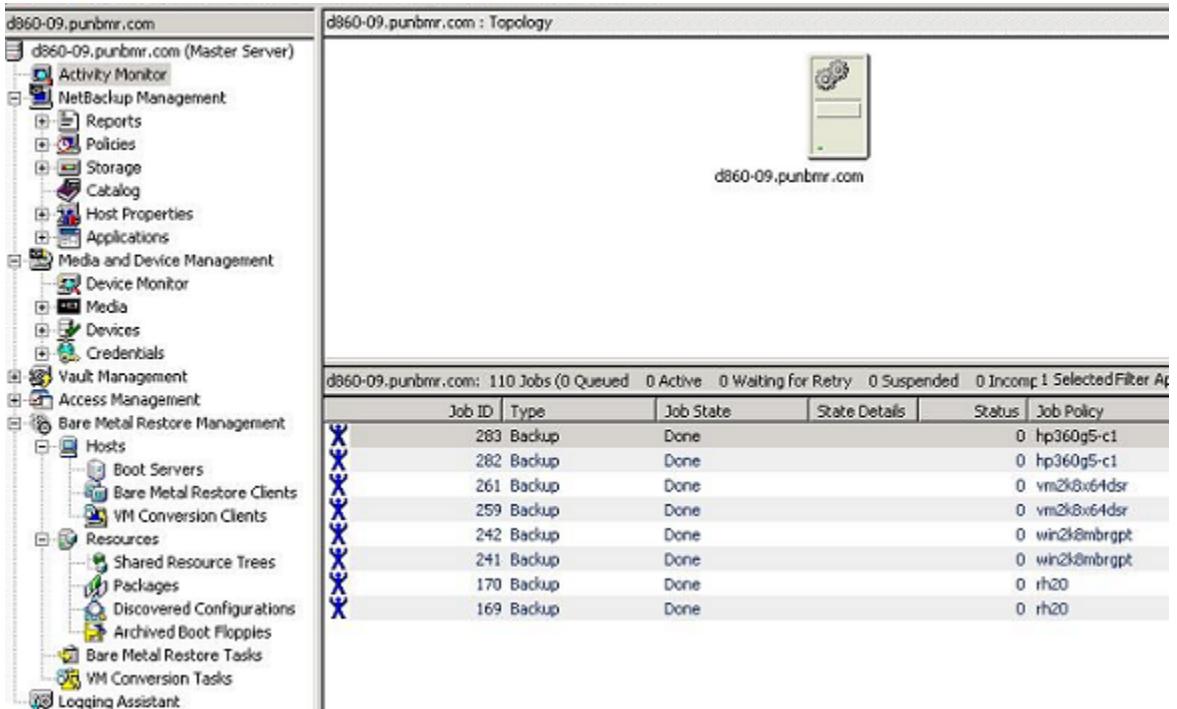
NetBackup Web UI のアクティビティモニターの [ジョブ (Jobs)] を使用して、保護対象のクライアントをバックアップするジョブを監視できます。

ジョブをダブルクリックすると、[ジョブの詳細 (Job Details)] ダイアログボックスが開かれ、ジョブに関する情報を参照できます。

次に示すタブに、ジョブの情報が表示されます。

- [ジョブの概要 (Job Overview)] タブには、ジョブについての一般情報が表示されません。
- [状態の詳細 (Detailed Status)] タブには、クライアント上でのエージェントの稼働状況をはじめ、ジョブについての詳細な情報が表示されます。ここでは、クライアントの構成情報が収集され、BMR マスターサーバーに送信されます。保護対象のシステムが (1 台または数台のディスクの) 単純な構成の場合、エージェントが消費する時間は、ほんの数秒です。さらに複雑な、複数のディスクグループまたはボリュームグループを所有するシステムでは数分かかります。複雑なストレージエリアネットワーク環境では、1 時間程度におよぶ場合があります。

バックアップポリシーで [複数のデータストリームを許可する (Allow Multiple Data Streams)] 属性が有効にされている場合、NetBackup によって各クライアントのバックアップが複数のジョブに分割される場合があります。各ジョブでは、バックアップ対象リストの一部のみがバックアップされます。ジョブは個別のデータストリームに存在するため、同時に実行できます。各クライアントで、1 つのジョブのみによって、クライアント Bare Metal リカバリに必要な構成を収集するエージェントが起動されます (これは、通常、最もジョブ ID が小さいジョブです)。



バックアップが実行され、エージェントが構成情報を収集してマスターサーバーに送信できるように、バックアップジョブの状態が 0 (ゼロ) 以外であることを調査して、問題を解決しておきます。

**メモ:** BMR 構成バックアップジョブ (通常は、ジョブ ID が最も小さいジョブ) が失敗する場合でも、ファイルシステムデータバックアップは正常に完了します。この場合、正常なファイルシステムデータバックアップの後で、BMR 構成バックアップジョブは一部完了として、黄色でハイライト表示されます。

## VM 作成ジョブの監視

仮想マシン変換ウィザードの実行時に、[仮想マシンに変換 (Convert to Virtual Machine)] ボタンをクリックすると、NetBackup が VM 作成プロセスを行うためのタスクを作成します。このタスクのタブで、タスクの状態、選択された Hypervisor 環境の詳細、および VM 変換オプションを調べることができます。

VM 変換タスクを監視するには、次のタスクを実行します。

- 1 NetBackup Web UI から、[Bare Metal Restore]、[ホスト (Hosts)]、[VM 変換タスク (VM Conversion Tasks)]の順に移動します。
- 2 [更新 (Refresh)]オプションを使用すると、マスターサーバーから新しい情報を取得して詳細ペインが更新されます。更新された項目だけがハイライト表示されます。  
次の画面ショットに、VM 変換ウィザードの実行時に作成される VM 変換タスクを示します。
- 3 タスクの詳細を表示するには、[詳細 (Detail)]ペインにあるタスクを右クリックして、[プロパティ (Properties)]を選択します。

---

**メモ:** BMR のリストアタスクや探索タスクと同様、開始した VM 変換タスクをクリーンアップやキャンセルすることはできません。特定クライアントのファイルシステムのデータリカバリジョブを NetBackup アクティビティモニターで確認することができます。

---

次の表に、VM 変換に関連するさまざまなタスク状態コードと、その説明を示します。

状態コード	説明
0	VM 変換タスクが正常に完了しました。
3	リソース配分が失敗しました。
4	VM 作成に対応していないクライアント構成。認識できない例外が VM 作成プロセスの実行中に発生しました。
6	クライアントの構成をロード中にエラーが発生しました。
7	選択されたクライアント構成に対し VM ノードを作成中に、エラーが発生しました。
8	クライアントの物理マシンオブジェクトの準備中にエラーが発生しました。
9	VM 変換のメタデータを構築中にエラーが発生しました。
12	作成された VM にファイルシステムをマウント中にエラーが発生しました。
13	作成された VM に Windows レジストリをロード中にエラーが発生しました。
15	ネットワークオプションを設定中にエラーが発生しました。
16	自動再起動で VM を作成中にエラーが発生しました。場合によっては、Hypervisor サーバーが全面的にロードされると、このタスクが失敗することがあります。そのようなケースでは、VM の手動起動を試みるとよい場合があります。
17	デバイスドライバの設定を処理中にエラーが発生しました。

状態コード	説明
18	MSD のデバイスドライバの設定を処理中にエラーが発生しました。
19	認識できない例外が VM 変換プロセスの実行中に発生しました。

## BMR ログ

BMR によって生成されたメッセージを表示して、BMR のアクティビティを監視することができます。

BMR アクティビティログファイルは、マスターサーバーの次のディレクトリに格納されます。

- `/usr/opensv/logs` ディレクトリ (UNIX および Linux の場合)
- `install_path\NetBackup\logs` フォルダ (Windows の場合)

BMR では、ログファイルの名前に標準化された形式を使用します。

次にログファイル名の例を示します。

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

次に、この例のログファイル名の構成要素を示します。

- 51216 は NetBackup のプロダクト ID です。
- 119 は、このログを書き込んだプロセス (Bare Metal Restore マスターまたはブートサーバーサービスである bmrtd または bmrbd) のオリジネータ ID です。
- 3892578826 は、このログを作成したホストの 10 進数の ID です。
- 050225 は、YYMMDD 形式の日付です。
- 0000000000 は、ログファイルのインスタンスを示すローテーション番号です。このオリジネータで、ログファイルが最大サイズに達し、新しいログファイルが作成されると、ファイルローテーション番号が 1 つ増加します。

統合ログファイルには、次の種類のメッセージが表示されます。

- アプリケーションログメッセージ。通知メッセージ、警告メッセージおよびエラーメッセージが含まれます。
- 診断ログメッセージ。記録されるログの情報量は、ログレベルによって変わります。
- デバッグログメッセージ。主に Cohesity のサポート担当者および技術者が使用します。記録されるデバッグログの情報量は、NetBackup マスターサーバーに対して指定されたログレベルによって変わります。

## BMR ログのオリジネータ ID

次に、ログを実行する BMR プロセスのオリジネータ ID を示します。

- 119        `bmrtd`。Bare Metal Restore のマスター。
- 121        `bmrsavecfg`。クライアントシステムで実行され、クライアント構成を収集してマスターサーバーに保存する Bare Metal Restore エージェント。
- 122        `bmrnc`。リストア中に BMR マスターサーバーと通信するためにクライアントが使用する Bare Metal Restore のユーティリティ。リストア中のクライアントで実行されます。
- 123        `bmrns`。GUI によって実行される様々なアクティビティのための Bare Metal Restore のコマンドラインインターフェース。
- 125        `bmrstrtadm`。共有リソースツリーを作成および管理し、リストア用ブート可能 CD/DVD メディアを作成する Bare Metal Restore のユーティリティ。BMR ブートサーバーで実行されます。
- 126        `bmrprep`。BMR をクライアントリストアまたは検出用に準備する Bare Metal Restore のユーティリティ。マスターサーバー上で実行されます。
- 127        `bmrsetupmaster` と `bmrsetupboot`。Bare Metal Restore マスターサーバーおよびブートサーバーの構成ユーティリティ。
- 128        様々なプログラムと Bare Metal Restore ライブラリ。
- 129        `bmrconfig`。クライアントの構成を変更する Bare Metal Restore のユーティリティ。
- 130        `bmrcreatepkg.exe`。リストアに使用できるように、Windows のドライバ、Service Pack および Hotfix を BMR マスターサーバーに追加するための Bare Metal Restore のユーティリティ。Windows ブートサーバーで実行されます。
- 131        `bmrrst.exe` と `bmrmap.exe` (Windows システムのみ) Windows の Bare Metal Restore クライアントをリストアするユーティリティ。リストア中のクライアントで実行されます。
- 142        `bmrepadm`。リストア中に使用される Bare Metal Restore の外部プロシージャを管理するユーティリティ。マスターサーバー上で実行されます。
- 152        `bmrovradm`。Bare Metal Restore のカスタム上書き機能を管理するユーティリティ。
- 248        `bmrlauncher`。新しい Windows Fast Restore 環境で IP 情報の入力を求めるプロンプトを表示するユーティリティ。
- 433        `bmr2v`。これは VM 作成コマンドラインインターフェースへの BMR バックアップです。
- 434        `bmr2vrst`。VIC (NetBackup Recovery) ホストで VM 作成を実行するユーティリティ。

- 529            bmrbd。root または管理者権限で実行されている BMR ブートサーバーサービス。
- 530            bmrbd。サービスアカウントで実行されている BMR ブートサーバーサービス。

## 統合ログとログファイルを管理するためのコマンド

収集する情報量とその情報の保持時間は、NetBackup マスターサーバーの[ホストプロパティ (Host Properties)]の[ログ (Logging)]プロパティと[クリーンアップ (Clean-up)]プロパティで構成します。

『NetBackup 管理者ガイド Vol. 1』を参照してください。

ログの使用および管理については、『NetBackup トラブルシューティングガイド』を参照してください。

BMR アクティビティログファイルは、表示や管理にコマンドを使う必要がある特殊な形式のファイルです。

次のコマンドを使用して、統合ログおよびログファイルを管理します。

- |           |  |
|-----------|--|
| vxlogview | このコマンドを使用して、統合ログ機能で作成されたログを表示できます。                 |
| vxlogmgr  | このコマンドを使用して、統合ログファイルを管理できます (たとえば、ログファイルの移動や削除など)。 |
| vxlogcfg  | このコマンドを使用して、ログ機能を構成できます。                           |

これらのコマンドは次のディレクトリに存在します。

- /usr/opensv/NetBackup/bin ディレクトリ (UNIX の場合)
- `install_path¥NetBackup¥bin` フォルダ (Windows の場合)

## BMR リストアログ

[ロギング (logging)]オプションがリストア準備ステップ中に選択された場合、BMR リストア処理はマスターサーバー上のリストアログにメッセージを書き込みます。ログファイルの場所および命名規則は、次のとおりです。

```
/usr/opensv/netbackup/logs/bmrrst/client_name/log.mmddyy (UNIX)  
install_path¥NetBackup¥logs¥bmrrst¥client_name¥log.mmddyy (Windows)
```

UNIX および Linux システムでは、メッセージに、外部プロシージャの開始および終了メッセージが含まれます (Windows システムで実行している BMR リストア処理では、開始および終了の記録は行われません)。

BMR アクティビティログと異なり、リストアログファイルはテキストファイルです。

# NetBackup BMR 関連の付録

この付録では以下の項目について説明しています。

- [BMR ブートサーバーに対するネットワークサービスの設定](#)
- [BMR における Linux のネイティブマルチパスのサポート](#)
- [BMR によるマルチパス環境のサポート](#)
- [BMR のマルチパスの表](#)
- [BMR による仮想環境のサポート](#)
- [BMR における直接 VM 変換のサポート表](#)
- [ZFS ストレージプールのサポートについて](#)
- [Solaris のゾーンリカバリのサポート](#)
- [自動イメージレプリケーションを使用した他の NetBackup ドメインへの BMR クライアントのリカバリ](#)
- [NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換性の表](#)
- [Windows 環境での iSCSI ディスクの管理](#)

## BMR ブートサーバーに対するネットワークサービスの設定

ネットワークブートベースのリカバリでは、BMR が OS 固有の NW ブートプロトコルを利用してリカバリを開始します。PXE、bootp、DHCP、TFTP など、OS の種類によって異なる

るNWの設定を行ってネットワークブートのリカバリを行う必要があります。以降のセクションで、特定のプラットフォームに関する詳細を示します。

## 共通の UNIX ネットワーク構成

TFTP サービスが利用可能である必要があります。オペレーティングシステムによっては、このサービスが `/etc/inetd.conf` ファイルからコメントアウトされています。これらのサービスをコメント解除して、BMR ブートサーバーが機能するように `inetd` を更新する必要があります。

NFS サービスが利用可能で、`nfsd` デーモンが実行している必要があります。`/etc/exports` には、NFS プロトコルで他のクライアントに公開されるファイルシステムエントリが含まれています。`/etc/exports` の設定で、手動で行わなければならないものはありません。BMR はこの設定を自動的に処理します。

## Red Hat Enterprise Linux のネットワーク構成

次のシステム前提条件は Red Hat Linux システムにのみ適用されます。

- (まだインストールされていない場合) 次の RPM パッケージをインストールします。
  - `compat-libstdc++`
  - `tftp-server`
  - `dhcp`
- 次の手順に従って、`tftp` サービスを有効にします。
  - `/etc/xinetd.d/tftp` ファイルを編集し、`disable = yes` を `disable = no` に変更します。
  - 次のコマンドを実行してサービスを起動します。

```
/etc/init.d/xinetd restart
```
- `/etc/dhcpd.conf` ファイルを作成して、サービスを提供するネットワークを定義するように構成します。ホスト情報を定義する必要はありません。ホストは、BMR ソフトウェアによって必要に応じて追加および削除されます。次に、構成の例を示します。

```
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;
}
```

/etc/dhcpd.conf ファイルの構文を検証するには、次のコマンドを実行して、デーモンを再起動し、正常に起動することを確認します。

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

## SuSE Linux ネットワークの構成

次のシステム前提条件は **SUSE Linux** システムにのみ適用されます。

- (まだインストールされていない場合) 次の RPM パッケージをインストールします。
  - nfs-utils
  - dhcp-base
  - dhcp-server
  - inetd
  - tftp
- 次の手順を実行して、tftp サービスを有効にします。
  - /etc/inetd.conf ファイルを編集し、tftp 行をコメント解除します。
  - 次のコマンドを実行してサービスを起動します。

```
/etc/init.d/inetd restart
```
- /etc/dhcpd.conf ファイルを変更して、サービスを提供するネットワークを定義します。ホスト情報を定義する必要はありません。ホストは、**Bare Metal Restore** ソフトウェアによって必要に応じて追加および削除されます。次に、構成の例を示します。

```
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;
}
```

/etc/dhcpd.conf ファイルの構文を検証するには、次のコマンドを実行して、デーモンを再起動し、正常に起動することを確認します。

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

---

**メモ:** DHCP サーバーは Linux BMR のブートサーバーで構成される必要があります。ネットワークの既存の DHCP サーバーはどれも、Linux BMR のネットワークベースのブートリカバリに使用することはできません。Linux のクライアントが BMR のブートサーバーを通じてネットワークブートする間は、他のすべての DHCP サーバーを停止することを推奨します。クライアントの DHCP ブート要求が他の DHCP サーバーに行った場合、ネットワークブートリカバリは失敗します。これは BMR の制限事項ではなく、このブートプロトコルが代わりに動作する方法です。

---

## Solaris でのネットワークの構成

Oracle Solaris で使用されるネットワーク構成のブート戦略は、TFTP、NFS および BOOTP、または DHCP (Dynamic Host Configuration Protocol) の NW サービスで構成されます。TFTP および NFS のサービスの設定は、前出のセクションで説明したものと同じです。

p.252 の「[共通の UNIX ネットワーク構成](#)」を参照してください。

### Solaris バージョン 10 のネットワークブートサービス構成

BMR がブートサーバーの必須ネットワーク構成を内部的に処理しながらリストアのためにクライアントを準備するので、Solaris 10 SPARC アーキテクチャでは具体的な DHCP 構成は必要ありません。

Solaris 10 x64 アーキテクチャはブートサーバーで手動で行うべき DHCP および TFTP サービスの構成を必要とします。

DHCP サービスを構成するには、次の手順を実行します。

- dhcp を初期化する dhcpconfig コマンドを実行します。

```
dhcpconfig -D -r SUNWfiles -p /var/dhcp
```
- ネットワーク表のエントリを追加します。

```
pntadm -C <Network-IP> E.g. : pntadm -C 10.209.4.0
```
- サブネットまたはルートの詳細を構成します。

```
dhtadm -A -m <Network-IP> -d <
':option=value:option=value:option=value:'>
例:
dhtadm -A -m 10.209.4.0 -d
':Subnet=255.255.252.0':Router=10.209.4.1':DNSdrain='<yourdomain>.com':DNSserv=10.216.16.101
10.217.160.131:'
```
- 次のコマンドを使用して DHCP サーバーを有効にします。

```
svcadm -v enable dhcp-server.
```

TFTP サービスを構成するには、次の手順を実行します。

- TFTP ベースディレクトリを作成します。  

```
mkdir /tftpboot
```
- TFTP エントリが `/etc/inetd.conf` ファイルになかった場合、次の行を追加してください。  

```
tftp dgram udp6 wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```
- 構成の変更をインポートします。  

```
/usr/sbin/inetconv
```
- TFTP を再起動します。  

```
svcs network/tftp/udp6 svcadm restart network/tftp/udp6
```

---

**メモ:** Solaris では、BMR は Solaris WAN ベースブートプロトコルをサポートしません。ただし、クロスサブネットの場合は、ネットワークベースのブートリカバリが想定されており、リレーブートサーバーを使用できます。

---

## Solaris バージョン 11.0 以降のネットワークブートサービス構成

x64 および SPARC アーキテクチャプラットフォームは、どちらも DHCP サービス設定が BMR ブートサーバーで行われることを要求します。GUI ベースユーティリティの DHCP マネージャでブートサーバー上に DHCP サーバーを設定する必要があります。このユーティリティはウィザードベースに必要な設定手順をガイドします。

---

**メモ:** Solaris 11.0 以降のバージョンの場合は、DHCP サーバーの設定に `dhcpcfg` コマンドラインユーティリティを使わないでください。IP のリースタイムラインに関する問題はコマンドラインの使用で見られるものです。

---

## HP-UX および AIX NW の設定

共通ネットワークサービスを設定するだけでなく、HP-UX および AIX の両プラットフォームに対し BOOTP サービスを有効にします。TFTP、NFS、および BOOTP の各サービスが BMR ブートサーバーで実行されていることを確認してください。

## Windows ネットワークの構成

Windows での BMR ブートサーバーの登録により、次のサービスが有効になります。

- BMRBD (BMR のブートサーバー) サービス
- BMR TFTP サービス
- BMR PXE サービス

BMR の TFTP および PXE サービスは、ネットワークベースのブートリカバリの場合で使用されます。これらのサービスとは別に、DHCP サービスも必要となります。

DHCP サービスの要件: DHCP サーバーは、同じブートサーバーのホストまたはネットワーク上の場所にしか存在することができません。

BMR PXE および TFTP サービスの要件および設定:

- BMR NW のブートが行われている間に同じサブネットで他の PXE サーバーが実行されていないことを確認してください。  
この制限の理由は、むしろこのネットワークプロトコルの動作にあります。クライアント NW のブート要求が想定外の PXE サーバーに行った場合は、クライアント NW のブートが失敗します。要求がネットワーク上の他の有効な PXE サーバーにリダイレクトされることはありません。このため、NW が BMR のリカバリのためにクライアントをブートしている間は、有効な BMR PXE サービスのみを実行することをお勧めします。
- BMR のブートサーバーの登録をポストして、Windows のブートサーバーで利用可能な BMR PXE の設定ウィザードに移動します。  
このウィザードは、[スタート]、[プログラム]、[NetBackup]から実行することができます。このウィザードでユーザーが DHCP サーバーの場所を指定します。DHCP サーバーの場所 (同じブートサーバーコンピュータ上かネットワーク上の他のコンピュータ上か) によって、DHCP サーバーに対してコマンドラインから netsh を実行するようにウィザードから指示されます。
- ウィザードを終了すると、PXE、TFTP、および DHCP サーバーが正常に構成されます。

Windows のブートサーバーを Active Directory サーバーにインストールする場合は、従来のリストア方法により SRT をリストア対象のクライアントと共有します。次のセキュリティ設定を使用してください。

Microsoft ネットワークサーバー

```
Digitally signed communications (always) - Disabled
```

Microsoft ネットワークサーバー

```
Digitally signed communications (if client agrees) -- Enabled
```

## BMR における Linux のネイティブマルチパスのサポート

データストレージドメインにおけるマルチパスは、サーバーが複数の物理パスを使って (接続用のバス、コントローラ、スイッチ、ブリッジデバイスを介して) その大容量記憶装置デバイスと通信する機能です。マルチパスはバスのエラーを防止しますが、特定のストレージデバイスのエラーは防止しません。マルチパス接続を使うもう 1 つの利点は、負荷分散によってスループットが向上している点です。

システム管理者がクライアントシステムで Linux のネイティブマルチパスを構成すると、BMR 側ではネイティブマルチパスを有効にするために追加のインストール、アンインストール、構成手順を実行する必要はありません。

マルチパス環境での一般的な BMR のサポートについて詳しくは、「p.257 の「BMR によるマルチパス環境のサポート」を参照してください。」を参照してください。

## BMR によるマルチパス環境のサポート

BMR はマルチパス環境における整合性をサポートします。つまり、BMR によるバックアップ中にクライアントのマルチパス環境の設定が BMR に通知されるため、BMR はマルチパスのディスクを、そのクライアントから取得した BMR 構成における制限対象としてマークします。その結果、リカバリにおいてユーザーはこれらのディスクの使用を制限されます。マルチパスのディスク上でどのようなファイルシステムが実行されていたとしても、代替の非マルチパスディスクにリカバリすることができます。たとえば、SAN の LUN 上で EMC PowerPath を使用するよう設定されたクライアントの場合には、BMR はそれらの SAN LUN を制限対象としてマークします。ユーザーは、マルチパスが有効にされていなければ、ローカルディスクであるかそれ以外の SAN LUN であるかにかかわらず、それらの上部にファイルシステムをリカバリできます。

### この制限はなぜ存在するのでしょうか。

その理由は、BMR のリカバリの環境には (EMC PP のような) マルチパスソフトウェアの設定や構成が存在しないためです。そのため、BMR のリカバリ環境では、指定されたターゲットハードウェアでマルチパスが有効にされていることを識別できません。現在サポートされているマルチパス環境は次のとおりです：

- UNIX/Linux/Windows をサポートするプラットフォームの EMC PowerPath
- Linux ネイティブマルチパス

環境について詳しくは、次の項で説明されています。

### BMR によるマルチパス環境のサポートとは具体的にどのようなものですか。

BMR では前述した条件のもとにあるマルチパス環境だけがサポートされます。BMR によりバックアップされたクライアントでいずれかのマルチパスが有効されていた場合には、クライアントの BMR 構成を取得する間に、BMR はマルチパスを厳密に一意的な物理ディスクに解決し、それを BMR config に表記します。また前述のように、BMR はそれらを制限対象としてマークすることにより、リカバリタイムエラーを回避します。

### クライアントが上記と異なるマルチパス環境だった場合にはどうなりますか。

BMR バックアップは一意的なディスク名の識別に失敗し、BMR により取得された構成には、マルチパスソフトウェアによって示されたマルチパスディスクの名前が表記されます。

また、ディスクを自動的に制限対象としてマークすることもできません。ここで、管理者 GUI を使用して BMR 構成をコピーし (『NetBackup BMR 管理者ガイド』のクライアント構成の管理に関する章を参照)、MP ディスクを特定し、手動でそれらを制限ありとしてマークする必要があります。これらの MP ディスク上のファイルシステムをリカバリする必要がある場合には、それらを別の非 MP ディスクにマッピングします。MP ベースのファイルシステムのリカバリを無視してオペレーティングシステムのみをリストアし、その後で BMR リカバリを実行する場合に、ターゲットホストにマルチパスディスクが接続されている場合には、マルチパスディスク上のファイルシステムが自動的にオンラインになることがあります。詳しくは、表「システムディスク以外のディスクの処理」と「インポート処理」を参照してください。

マルチパス環境ベースのオペレーティングシステムボリュームがセットアップされたクライアントの場合には、BMR はこのシステムをリカバリできません。

## BMR のマルチパスの表

次の表に、BMR のマルチパスに対するプラットフォームの対応関係を示します。

プラット フォーム (Platform)	EMC Power パスのバージョン	[ネイティブマルチパス (Native Multipath)]	SF のバージョン
Windows の場合	EMCPower.5.5.SP1	該当なし	SFW 5.1 SP1 および SP2
HPUX	EMCPower.HPUX.5.1.SP2.GA	該当なし	SF 5.0 MP3
AIX	EMCPower.AIX.5.5.GA	該当なし	SF 6.0, SF 6.0RP1
Solaris	EMCPower.SOLARIS.5.5	サポート対象外	SF 5.1
RHEL	EMCPower.LINUX.5.6.GA	サポート対象	サポート対象外
SUSE	EMCPower.SUSE_LINUX.5.5.GA	サポート対象	サポート対象外
OEL	EMCPower.LINUX.5.7.GA	サポート対象	サポート対象外

## BMR による仮想環境のサポート

次の表に、仮想化技術でサポートされている BMR のブートサーバーとクライアントのバージョンをリストアップします。

Hypervisor の種類およびバージョン	ゲスト VM の OS のバージョン
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 の AIX 7.1	AIX のバージョン 6.1 および 7.1
Hyper-V	Windows、RHEL-Linux、SuSE-Linux

---

**メモ:** Solaris ズーンリカバリはホストオペレーティングシステムの保護によってサポートされます。p.261 の「[Solaris のズーンリカバリのサポート](#)」を参照してください。を参照してください。

---

参考情報: サポート対象の仮想プラットフォームでの次に示す OS リカバリは公式にテストやサポートはされていませんが、正常に動作したお客様もいらっしゃいます。

- LPAR での AIX リカバリ
- vPar、nPar の HP-UX リカバリ
- LDOM インスタンスの Solaris リカバリ

## BMR における直接 VM 変換のサポート表

最新のサポートに関する表については、<http://www.veritas.com/docs/000006177> を参照してください。

## ZFS ストレージプールのサポートについて

Zettabyte File System (ZFS) は、ファイルシステムと Logical Volume Manager の両方の機能を持つ、Solaris オペレーティングシステムに組み込まれたシステムです。ZFS は SPARC と x86 ベースの両方のシステムで利用可能です。

ZFS のサポートは Solaris 10 6/06 (「U2」) で追加されました。Solaris 11.0 をインストールすると、ZFS もインストールされてデフォルトのファイルシステムとして設定されます。

Bare Metal Restore では、ZFS ストレージプールに接続された Solaris 10 Update 11 以降のクライアントを保護できるようになりました。

BMR 7.6 では、Solaris 10 Update 11 以降の次の構成のクライアントのバックアップとリストアがサポートされます。

- ZFS のルートプールとデータプール

- スライスの ZFS ストレージプール
- ゾーンを含む ZFS ファイルシステム
- SAN ブートが設定された ZFS
- ZFS ストレージプールと VxVM や SVM のディスクグループ

**メモ:** 前述のすべての機能は [Solaris SPARC] と [Solaris] x86\_64 アーキテクチャの両方でサポートされます。

BMR では、次の構成の Solaris クライアントはサポートされません。

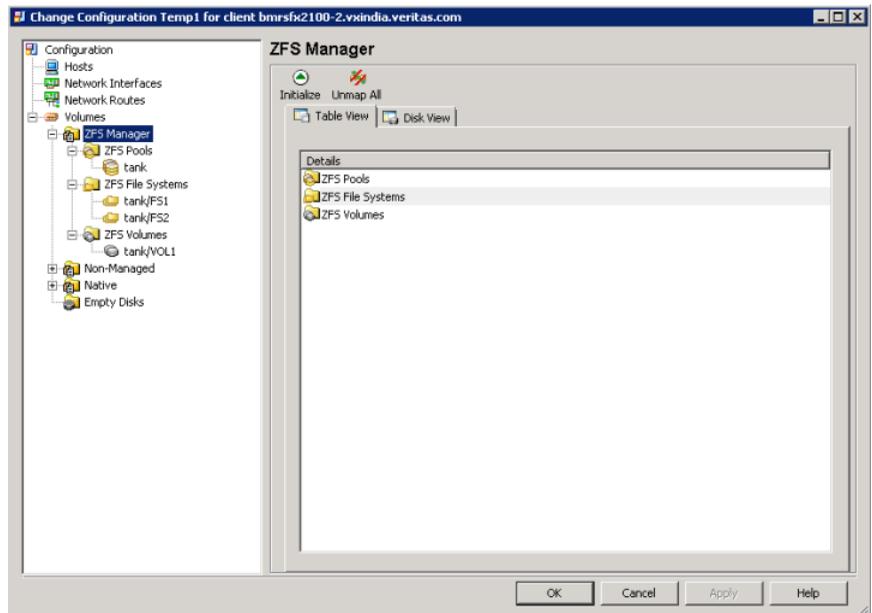
- UFS から ZFS への移行
- ZFS ボリューム上の別のファイルシステム

ZFS Manager の要素とそのパラメータを表示するには、次の手順を実行します。

- NetBackup Web UI で、[Bare Metal Restore]、[ホスト (Hosts)]、[Bare Metal Restore クライアント (Bare Metal Restore clients)] の順に選択します。関連付けられているすべてのボリュームを表示するクライアントの [変更構成 (Change Configuration)] ダイアログボックスを開きます。

☒ **A-1** に ZFS Manager の GUI 画面を示します。

**☒ A-1** ZFS Manager の UI



# Solaris のゾーンリカバリのサポート

BMRを使用して Solaris ゾーンをバックアップおよびリストアする場合は、Solaris ゾーン固有の注意事項に対応する必要があります。

Bare Metal Restore では Solaris システムを実行しているゾーンをリストアできます。BMRを使用して非グローバルゾーンを個々にリストアすることはできません。システム内のすべての非グローバルゾーンが、グローバルゾーンのリストアの一環として再作成されます。グローバルおよび非グローバルなゾーンが ZFS ファイルシステムに基づいていれば、「`vfstab`」構成は必要となりません。

## Dissimilar Disk Restore によるリストアシナリオですべての非グローバルゾーンをリストアする方法

- 1 ゾーンファイルをリストアするために、ゾーン (ゾーンパスとも呼ばれる) をホスティングするファイルシステムを再マッピングします。

再マッピングされていないスライスがグローバルゾーンから非グローバルゾーンにインポートされると、BMR によって、ゾーン構成からそのスライスが削除されます。

異なるディスクに再マッピングされているスライスがグローバルゾーンから非グローバルゾーンにインポートされると、BMR によって、ゾーン構成やゾーンの `vfstab` (`ZONEPATH/root/etc/vfstab`) エントリが再調整され、新しいデバイス名が使われます。

再マッピングされていないシステムがグローバルゾーンファイルから非グローバルゾーンにインポートされると、BMR によって、システムへの参照がゾーン構成から削除されます。

## 2 テスト

非グローバルゾーンによってインポートまたは使用されたすべてのファイルシステムは、BMRによるリストア後に再作成およびリストアする必要がある場合があります。通常、これらのファイルシステムは、グローバルゾーンの `vfstab` (`/etc/vfstab`) には表示されません。

BMR では、`/etc/vfstab` 内のエントリを基に、リストアの対象となるファイルシステムが記述されます。動的に作成およびマウントされ、`/etc/vfstab` に表示されないファイルシステムは (NetBackup によってバックアップされている場合でも)、自動的にリストアされることはありません。このようなファイルシステムを BMR で強制的にリストアする最も簡単な方法は、使われているデバイスとマウントポイントが記述されている `/etc/vfstab` に、**Mount at boot** フィールドを **No** に設定したエントリを追加します。その後、動的ファイルシステムは、以前のとおり継続して使用できます。BMR では、これらのファイルシステムが認識され、DDR にマッピング解除されていない限り、再作成されます。NetBackup によってバックアップされている場合は、その内容がリストアされます。

ゾーン機能により、動的にマウントされたファイルシステムが次のように表示されます。

- グローバルゾーンのデバイスを含む FS エントリ

- グローバルゾーンからインポートされているが、マウントは非グローバルゾーンの `/etc/vfstab` によって、またはゾーン自身によって動的に行われたデバイスエントリ BMR のゾーンリストアを自動化するには、次に示すように、BMR がこれらをリストアする原因となっているエントリをグローバルゾーン (`/etc/vfstab`) に追加します (DDR によってマッピング解除されている場合を除く)。

- FS エントリの場合、グローバルゾーンのデバイスは、非グローバルゾーンのルートの下に表示されるマウントポイントを持つ特別な **raw** 値として使用されます。グローバルゾーンの `/etc/vfstab` に追加するエントリでは、グローバルゾーンのデバイスパスを、ゾーンパスを含めた非グローバルゾーンのマウントポイントへのフルパスとともに使用する必要があります。たとえば、次のようなゾーンがあるとします。

```
zonepath=/export/zone1
fs:
  dir=/export
  special=/dev/dsk/c0t9d0s6
  raw=/dev/rdisk/c0t9d0s6
  type=ufs
```

`/etc/vfstab` のグローバルゾーンのエントリでは、次のようになります。

```
/dev/dsk/c0t9d0s6 /dev/rdisk/c0t9d0s6 /export/zone1/root/export ufs
```

- no -

- 非グローバルゾーンによってマウントされたデバイスエントリの場合は、BMR によるリストアを構成する際に、次に示す処理を行う必要があります。
  - 使用される動的マウントには、ゾーンパスの下に、インポートされるデバイスパスが含まれます。非グローバルゾーン内の `/etc/vfstab` によってマウントされるデバイスの場合、ゾーンには、次のような 1 つ以上のデバイスエントリがあります。

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

表示されるデバイスは、非グローバルゾーンの `/etc/vfstab` では次のようになります。

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

このコマンドによって、グローバルゾーンは、  
`/export/zone2/dev/dsk/c0t0d0s4` (マウントポイント

/export/zone2/root/local 上)を動的にマウントするようになります。ただし、BMR でファイルシステムを自動的に再作成するには、代わりに次のような記述エントリをグローバルゾーンの /etc/vfstab に追加する必要があります。

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

(ゾーンパスに対する相対デバイスパスを使用すると、BMR はファイルシステム全体をリストアするのではなく、マウントポイントを再作成だけです。)

- DDR を使用する場合、BMR による編集を許可するには、デバイスの一致にワイルドカードを使用しないでください。デバイスの指定にワイルドカードが含まれていると、ゾーンに影響する DDR マッピング (マッピング解除やディスク間でのファイルシステムの移動など) が行われた場合に、BMR ではエントリを編集できなくなります。影響を受けるゾーンの /etc/vfstab は編集されますが、デバイスの一致が記述されているエントリが編集されるのは、そこにワイルドカードが含まれていない場合のみです。

たとえば、次のエントリを変更します。

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

このエントリでは、次のように 2 つのデバイスエントリを使う必要があります。

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

例に示すようにエントリを変更した場合、BMR DDR はゾーンの定義と vfstab ファイルを正しく更新します。

## 自動イメージレプリケーションを使用した他の NetBackup ドメインへの BMR クライアントのリカバリ

この付録では、BMR と自動イメージレプリケーション (A.I.R.) をどのように組み合わせて活用すれば他のクライアントまたはディザスタリカバリドメインに対しプライマリドメインのクライアントの Bare Metal リカバリを実行できるかについて説明します。

NetBackup A.I.R. はクライアントバックアップイメージを定義済みの保存先または DR ドメインの NetBackup セットアップに複製するときに役立つ機能です。この機能では、DR サイトでの自動的なプライマリデータのリカバリに対応した高速なバックアップインポートが実行されます。

A.I.R. およびそれを有効にする方法について詳しくは、『NetBackup 管理者ガイド』を参照してください。

この二重ドメイン二重サイトの保護要件のために、自動イメージレプリケーション対応のバックアップポリシーで Bare Metal Restore オプションを有効にする必要があります。自動イメージレプリケーションと BMR が有効になっているバックアップイメージが DR ドメ

ンでインポートされる状態になると、インポートされているイメージで BMR が有効になっているのかを NetBackup サーバーがチェックします。そのイメージで BMR が有効になっていることを NetBackup サーバーが検出すると、自動的にクライアントの BMR 構成も一緒にインポートします。クライアントの Bare Metal Restore 設定ノードは、UI メニューの NetBackup Web UI、[Bare Metal Restore]、[ホスト (Hosts)]、[Bare Metal Restore クライアント (Bare Metal Restore Clients)] で確認できます。

DR サイトで BMR 設定をインポートする間に、BMR マスターサーバーは自動的に DR サイトのエンティティ (NetBackup のプライマリ、メディアサーバーのホスト名、それらの IP アドレスなど) に関してクライアントの設定を微調整します。これにより、古いドメインエントリが新しいサーバーの詳細に更新され、クライアントデータの回復中に BMR のリカバリ環境が DR ドメインの NetBackup サーバーにアプローチできるようになります。任意で、インポートされたクライアントの BMR 設定をコピーまたは編集して、必須のホストエントリを手動で追加または更新できます。手動でクライアント設定を編集するには、「クライアントおよび構成の管理」という章を参照してください。

---

**メモ:** BMR A.I.R. セットアップで BMR 構成をリストアするときに、次のエラーが表示される場合があります。Add an appropriate host entry or host mapping for Name of the host and retry the operation.

この問題を解決するには、DR ドメインのホストデータベースのホストを追加する必要があります。

p.265 の「DR ドメインのホストデータベースへのホストの追加」を参照してください。

---

手動によるバックアップのインポートも構成の変更もない場合は、BMR ネットワークまたはメディアベースのリカバリプロシージャを使用して DR ドメインでクライアントを完全に回復することができます。また、「バックアップから直接 VM を作成する」機能を使用して DR ドメインの仮想環境サーバーにクライアント VM を作成することもできます。

「クライアントバックアップからの仮想マシンの作成」の章を参照してください。

---

**メモ:** プライマリドメインで NetBackup のバックアップポリシーにクライアントの短い名前をリストすることを推奨します。DR ドメインの FQDN がプライマリドメインと異なる場合、DR ドメインでのクライアントデータのリカバリが、クライアントのドメイン名の不一致が原因で失敗する可能性があります。プライマリドメインの [プライマリ] ドメイン > 「バックアップ対象」に、NetBackup クライアントがインストールされる OS のファイルシステムの必要条件が表示されます。Windows の場合には、システム状態も表示されます。これらが表示されない場合には、DR サイトでの BMR 構成のインポートが失敗する可能性があります。BMR のバックアップポリシーの定義について詳しくは、「クライアントの保護」の章を参照してください。

---

---

**メモ:** DR ドメインで BMR マスターサーバーが有効であることを確認します。有効でない場合は、DR サイトでの BMR 構成のインポートが失敗します。

---

## DR ドメインのホストデータベースへのホストの追加

NetBackup Web UI、[Bare Metal Restore の管理 (Bare Metal Restore Management)]、[ホスト (Hosts)]、[Bare Metal Restore クライアント (Bare Metal Restore Clients)] 画面に表示されるクライアントは、DR ドメインのホストデータベースの一部ではない場合があります。[リストア準備 (Prepare To Restore)]、[検出準備 (Prepare to Discover)]、[Bare Metal Restore]などの BMR 操作を正常に実行するには、ホストデータベースでそれぞれのクライアントを手動で追加する必要があります。これにより、リカバリ処理中にホスト ID ベースの証明書がクライアントに対して発行され、BMR を介してクライアントを正常にリカバリできます。

---

**メモ:** Cohesityは、BMR A.I.R. セットアップのような特定のシナリオ以外で、ホストを手動で追加することは推奨しません。ホストを追加する前に、追加するホストエントリがホストデータベースにまだ存在していないことを確認する必要があります。

---

### ホストデータベースに手動でクライアントを追加する方法

- 1 次のコマンドを実行して、マスターサーバーで、Web サービスのログインを認証します。

```
bpnbat -login -loginType WEB
```

- 2 次のコマンドを実行して、ホストをリセットします。

```
nbhostmgmt -addhost -host host name -server master server
```

## NetBackup 8.1.1 以降のリリースでの BMR 用の、安全な通信の互換性の表

このセクションでは安全な通信に関連する NetBackup ブートサーバー、クライアント、SRT のバージョンの互換性についての情報を記載します。

表 A-1は、さまざまな NetBackup ブートサーバー、クライアント、および SRT バージョンの組み合わせにおける、BMR 用の安全な通信の互換性についての詳細を記載しています。

表 A-1 BMR 用の安全な通信の互換性マトリックス

ブートサーバー	リストアされるクライアント	リストアを開始するクライアントバージョン (SRT クライアントバージョン)	説明
NetBackup 8.1.1 以降*	NetBackup 8.1.1 以降*	NetBackup 8.1.1 以降*	サポート対象
NetBackup 8.1.1 以降*	NetBackup 8.1.1 以降*	NetBackup 8.0	サポート対象外
NetBackup 8.1.1 以降*	NetBackup 8.0	NetBackup 8.1.1 以降*	サポート対象外
NetBackup 8.1.1 以降*	NetBackup 8.0	NetBackup 8.0	サポート対象
NetBackup 8.0	NetBackup 8.1.1 以降*	NetBackup 8.1.1 以降*	サポート対象外
NetBackup 8.0	NetBackup 8.1.1 以降*	NetBackup 8.0	サポート対象外
NetBackup 8.0	NetBackup 8.0	NetBackup 8.1.1 以降*	サポート対象外
NetBackup 8.0	NetBackup 8.0	NetBackup 8.0	サポート対象

\*NetBackup 8.1.2 リリース以降では、BMR 操作は AIX と HP-UX プラットフォームでサポートされます。

## Windows 環境での iSCSI ディスクの管理

BMR では、Windows で次のように iSCSI ディスクが管理されます。

- バックアップ時に、BMR によって iSCSI ディスクが識別され、[制限あり (Restricted)] として自動的にマーク付けされます。iSCSI ディスクは制限なしにできません。
- ディスクは制限されているため、ユーザーはディスクを使用して DDR 用のボリュームをマッピングできません。
- BMR では、リストア処理時に iSCSI ディスクが設定されません。そのため、ディスクは制限されたままになり、これらのディスク上に完全または部分的に存在するすべてのボリュームは BMR 時にリストアされません。
- iSCSI ディスクに存在するボリュームに NetBackup がインストールされている場合、BMR では iSCSI ディスクがサポートされません。