Hewlett Packard Enterprise

HPE Data Protector

ソフト ウェアバージョン: 10.00

ディザスタリカバリガイド

ドキュメントリリース日 : 2017年 6月
ソフトウェアリリース日 : 2017年 6月

ご注意

保証

Hewlett Packard Enterprise Development LP製品に関する保証は、製品およびサービスに付属する保証規定に明示されている内容に限定されます。本書のいかなる記述も、追加の保証を構成するものではありません。HPEは、本書の技術的内容や編集に関する誤りや欠落に関して責任を負いません。

ここに記載する情報は、予告なしに変更されることがあります。

権利の制限

機密コンピューターソフトウェア。保持、使用、またはコピーには、HPEからの有効なライセンスが必要です。FAR 12.211および12.212に従って、商用コンピューターソフトウェア、コンピューターソフトウェアドキュメント、および商用品目の技術データは、米国政府に対して、ベンダーの標準商用ライセンスに基づいてライセンスされます。

著作権について

商標について

Adobe™はAdobe Systems Incorporatedの商標です。

Microsoft®およびWindows®は、米国におけるMicrosoft Corporationの登録商標です。

UNIX®は、The Open Groupの登録商標です。

この製品には、'zlib' 汎用圧縮ライブラリのインタフェースが含まれています。Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

ドキュメントの更新情報

このマニュアルの表紙には、以下の識別情報が記載されています。

- ソフトウェアバージョンの番号は、ソフトウェアのバージョンを示します。
- ドキュメントリリース日は、ドキュメントが更新されるたびに変更されます。
- ソフトウェアリリース日は、このバージョンのソフトウェアのリリース期日を表します。

最新のソフトウェア更新をチェックするには、次のサイトを参照してください。
https://softwaresupport.hpe.com/patches

更新状況、およびご使用のドキュメントが最新版かどうかは、次のサイトで確認できます。
https://softwaresupport.hpe.com/manuals

このサイトを利用するには、HPE Passportへの登録とサインインが必要です。HPE Passport IDの登録は、次のWebサイトから行なうことができます。https://hpp12.passport.hpe.com/hppcf/login.do.

適切な製品サポートサービスをお申し込みいただいたお客様は、更新版または最新版をご入手いただけます。詳細は、HPEの営業担当にお問い合わせください。

サポート

HPEソフトウェアサポートオンラインWebサイトを参照してください。https://softwaresupport.hpe.com

このサイトでは、HPEのお客様窓口のほか、HPEソフトウェアが提供する製品、サービス、およびサポートに関する詳細情報をご覧いただけます。

HPEソフトウェアオンラインではセルフソルブ機能を提供しています。お客様のビジネスを管理するのに必要な対話型の技術サポートツールに、素早く効率的にアクセスできます。HPソフトウェアサポートのWebサイトでは、次のようなことができます。

- 関心のあるナレッジドキュメントの検索
- サポートケースの登録とエンハンスメント要求のトラッキング

- ソフトウェアパッチのダウンロード
- 製品ドキュメントへのアクセス
- サポート契約の管理
- HPEサポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェアカスタマーとの意見交換
- ソフトウェアトレーニングの検索と登録

一部のサポートを除き、サポートのご利用には、HPE Passportユーザーとしてご登録の上、サインインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。

HPE Passport IDを登録するには、次のWebサイトにアクセスしてください。
https://hpp12.passport.hpe.com/hppcf/login.do

アクセスレベルの詳細については、次のWebサイトをご覧ください。
https://softwaresupport.hpe.com/web/softwaresupport/access-levels

目次

第1章: 概要

Data Protectorディザスタリカバリの概要

この章では、ディザスタリカバリプロセス全体の概要を示すとともに、『ディザスタリカバリガイド』で使用されている基本用語について説明し、基本的なディザスタリカバリの方法に関する概要を示します。

コンピューター障害とは、人的エラー、ハードウェア障害、自然災害などにより、コンピューターシステムが起動不能になった状態を指します。一般的に、このような場合は、コンピューターのブートパーティションまたはシステムパーティションが使用できないため、標準的な復元作業を行う前に、環境の復旧を行わなければなりません。ディザスタリカバリプロセスでは、ブートパーティションの再作成や再フォーマット、および環境を定義する各種の構成情報を含めたオペレーティングシステムの復旧が必要になります。これらの作業が終了するまでは、その他のユーザーデータを復元することはできません。

ディザスタリカバリの詳細については、『*HPE Data Protectorディザスタリカバリガイド*』を参照してください。

オリジナルシステムとは、システムでコンピューター障害が発生する前にData Protectorによってバックアップされたシステム構成を指します。

ターゲットシステムとは、コンピューター障害発生後のシステムを指します。ターゲットシステムは通常、起動が不可能な状態になっているため、Data Protectorのディザスタリカバリは、このシステムをオリジナルシステムの構成に復元することを目的としています。影響を受けたシステムとは異なり、ターゲットシステムの場合は、障害が発生したハードウェアはすべて交換されています。

ブートディスク/パーティション/ボリュームとは、ブートプロセスの初期段階に必要なファイルを含むディスク/パーティション/ボリュームを指します。一方、**システムディスク/パーティション/ボリューム**とは、オペレーティングシステムファイルを含むディスク/パーティション/ボリュームを指します。

> **注:**
> Microsoft社の定義は上記とは逆で、ブートパーティションはオペレーティングシステムファイルを含むパーティション、システムパーティションはブートプロセスの初期段階で必要なファイルを含むパーティションを示します。

ホストシステムとは、ディスクデリバリーによるディザスタリカバリに使用される、Disk Agentがインストールされた動作中のData Protectorクライアントです。

補助ディスクとは、ネットワーク機能を備えた最低限のOSと、Data Protector Disk Agentがインストールされたブート可能ディスクです。ディスクデリバリーでUNIXクライアントをディザスタリカバリするときの段階1では、補助ディスクをターゲットシステムのブートに使用することができます。

ディザスタリカバリオペレーティングシステム(DR OS)とは、ディザスタリカバリプロセスが実行されているオペレーティングシステム環境です。Data Protectorに基本的ランタイム環境(ディスク、ネットワーク、テープ、ファイルシステムへのアクセス)を提供します。Data Protectorディザスタリカバリを実行する前に、DR OSをインストールして、構成しておく必要があります。

DR OSには、一時DR OSとアクティブDR OSがあります。**一時 DR OS**は、別のオペレーティングシステムをターゲットオペレーティングシステム構成データとともに復元するホスト環境としてだけ使用され、ターゲットシステムをオリジナルシステム構成に復元し終えた後、一時DR OSは削除されます。**アクティブDR OS**は、Data Protectorディザスタリカバリプロセスのホストとして機能するだけでなく、復元後のシステムの一部にもなります。その場合、DR OSの構成データは元の構成データに置き換わります。

重要なボリュームとは、システムの起動に必要なボリュームおよびData Protectorボリュームを指します。使用しているオペレーティングシステムにかかわらず、これには次のようなボリュームが含まれます。

- ブートボリューム
- システムボリューム
- Data Protector実行可能ファイルが格納されているボリューム
- (Cell Manager用に)IDBが格納されているボリューム

> **注:**
> IDBが複数のボリューム上に格納されている場合は、IDBがあるすべてのボリュームがクリティカルボリュームとして扱われます。

WindowsおよびLinuxシステムでは、上記の重要なボリューム以外にも、CONFIGURATIONデータが格納されているボリュームも重要なボリュームとなります。Windowsシステムでは、サービスは、CONFIGURATIONのバックアップの一部としてバックアップされます。

Windowsシステムの場合、CONFIGURATIONオブジェクトに含まれる項目の一部がシステム、ブート、Data Protector、IDB以外のボリュームにある場合があります。これらのボリュームも重要なボリュームとなります。

- ユーザープロファイルボリューム
- Windows Serverシステム上のCertificate Serverデータベースボリューム
- Windows Serverのドメインコントローラー上のActive Directoryサービスボリューム
- Microsoft Cluster Serverの定数ボリューム

Linuxシステムの場合、CONFIGURATIONオブジェクトに含まれるデータは、自動ディザスタリカバリ方法に関連するもの(ボリューム、マウントポイント、ネットワーク設定、およびそれらと同類のデータ)だけです。

オンライン復旧は、Cell Managerがアクセス可能な場合に実行されます。この場合、Data Protectorのほとんどの機能(Cell Managerによるセッションの実行、復元セッションのIDBへの記録、GUIを使った復元作業の進行状況の監視など)が使用可能です。

オフライン復旧は、Cell Managerがアクセスできない場合に行います(ネットワーク問題やCell Managerの障害、オンライン復旧が失敗した場合など)。オフライン復旧では、スタンドアロンデバイス、SCSIライブラリ、ファイルライブラリ、デバイスへのバックアップ(B2D)デバイスだけを使用できます。Cell Managerはオフラインでのみ復旧可能です。

リモート復旧は、SRDファイルで指定されたMedia Agentシステムがすべて使用可能な場合に行います。1台でも使用できない場合は、リカバリプロセスはローカルモードに切り替わります。これは、ターゲットシステムにローカルに接続しているデバイスが検索されることを意味します。デバイスが1台しか見つからない場合は、そのデバイスが自動的に使用されます。デバイスが2台以上見つかった場合、Data Protectorは使用するデバイスを画面に表示してユーザーに選択させます。オフラインOBDRは常にローカルで行うことに注意してください。

障害は重大な問題ですが、以下の要因により状況がさらに悪化するおそれがあります。

- システムをできる限り迅速かつ効率的にオンライン状態に戻す必要がある。
- ディザスタリカバリは日常的な作業ではないため、管理者が要求される作業手順に不慣れである。
- ディザスタリカバリを実行すべき担当者が、基本的なシステム知識しか持っていない。

ディザスタリカバリは、あらかじめ定義された手軽に実行できるソリューションとして提供されるわけではありません。復旧手順は複雑であり、あらかじめ広範囲にわたる計画と準備を行っておく必要があります。障害からスムーズに復旧するには、段階ごとの手順を事前に詳細に定義しておかなければなりません。

ディザスタリカバリフェーズプロセス

どの復旧方法を使用するかにかかわらず、ディザスタリカバリプロセスは、連続する次の4つの段階に大きく分けることができます。

1. 段階0
2. 段階1
3. 段階2
4. 段階3

1. **段階0**は、ディザスタリカバリを成功させるために必要な準備作業です。障害が発生する前に計画と準備を実施しておく必要があります。
2. **段階1**で、DR OSのインストールと構成を行います。通常はブートパーティションの再作成と再フォーマットも行います。これは、システムのブートもしくはシステムパーティションは常に使用可能とは限らず、通常の復元操作を行う前に環境の復旧が必要な場合があるためです。
3. 段階2では、Data Protectorを含むオペレーティングシステム環境を定義するすべての構成情報を以前と同じように復旧します。
4. このステップが完了した場合にのみ、アプリケーションとユーザーデータの復元が可能になります(**段階3**)。

迅速で効率的な復元のためには、明確なプロセスを確実に実行することが必要です。

ディザスタリカバリの方法

この項では、基本的なディザスタリカバリの方法に関する全般的な概要を示します。各オペレーティングシステムでサポートされているディザスタリカバリ方法の一覧については、にある最新のサポート一覧を参照してくださいhttps://softwaresupport.hpe.com/。

> **注:**
> いずれかの方法を選択する前に、それぞれの方法の制限事項についても確認しておいてください。

ディザスタリカバリの方法に関する概要、下は、Data Protectorのディザスタリカバリの方法に関する概要を示しています。

ディザスタリカバリの方法に関する概要

段階0	段階1	段階2	段階3
手動によるディザスタリカバリ			
システム全体のフルファイルシステムバックアップ、内部データベースバックアップ(Cell Managerのみ)。SRD	ネットワークサポート付きのDR OSをインストールします。 ディスクパーティションを再作成し、オリジナル	`drstart`コマンドを実行して、重要なボリュームを自動復旧します。拡張復旧タスクを実行するには、追加の手順が必要になります。	Data Protectorの標準復元手順でユーザーデータとアプリケーションデータを復元します。

ファイルを更新します(Windowsシステムの場合のみ)。DR OSをインストールならびに構成できるようにするため、オリジナルシステムに関する情報を収集します。	の記憶データ構造を再確立します。		
半自動ディザスタリカバリ(AMDR)、ページ 22または手動によるディザスタリカバリ(MDR)、ページ 87を参照してください。			
ディスクデリバリーによるディザスタリカバリ(DDDR)(UNIXシステムのみ)			
システム全体のフルファイルシステムバックアップ、内部データベースバックアップ(Cell Managerのみ)、補助ディスクを作成します。	補助ディスクをターゲットシステムに接続します。 交換ディスク上にパーティションを再作成し、オリジナルの記憶データ構造を再確立します。	オリジナルシステムのブートディスクを交換ディスク上に復元し、補助ブートディスクを取り外します。 システムを再起動します。 拡張復旧タスクを実行するには、追加の手順が必要になります。	Data Protectorの標準復元手順でユーザーデータとアプリケーションデータを復元します。
ディスクデリバリーによるディザスタリカバリ(DDDR)、ページ 96を参照してください。			
拡張自動ディザスタリカバリ(EADR)			
システム全体のフルファイルシステムバックアップ、内部データベースバックアップ(Cell Managerのみ)。SRDファイルを準備して更新します。DR OSイメージを準備します。	ディザスタリカバリCD、USBフラッシュドライブ、またはネットワークからシステムをブートし、復旧範囲を選択します。	クリティカルボリュームの自動復元。拡張復旧タスクを実行するには、追加の手順が必要になります。	Data Protectorの標準復元手順でユーザーデータとアプリケーションデータを復元します。
拡張自動ディザスタリカバリ(EADR)、ページ 36または拡張自動ディザスタリカバリ(EADR)、ページ 101を参照してください。			
ワンボタンディザスタリカバリ(OBDR)			
OBDRウィザードを使用したシステム全体のフルファイルシステムバックアップ。SRDファイルを準備して更新します。	OBDRテープからターゲットシステムをブートし、復旧範囲を選択します。	クリティカルボリュームの自動復元。	Data Protectorの標準復元手順でユーザーデータとアプリケーションデータを復元します。
ワンボタンディザスタリカバリ(OBDR)、ページ 54またはワンボタンディザスタリカバリ(OBDR)、ページ 111を参照してください。			

次の段 階に進む前に、以下の作 業を完 了する必 要があります。

- *段 階 0:*

  フルクライアントバックアップおよびIDBバックアップ(Cell Managerのみ)を実 行するとともに、DR OSのインストールと構 成に必 要な情 報を管 理者がオリジナルシステムから収 集する必 要があります。UNIXシステム上のディスクデリバリーによるディザスタリカバリに使 用する補 助ブートディスクを作 成する必 要があります。
- *段 階 1:*

  DR OSをインストールおよび構 成するとともに、オリジナルの記 憶データ構 造を再 確 立する必 要があります(すべてのボリュームを復 元できるようにします)。UNIX上のディスクデリバリーによるディザスタリカバリに使 用する交 換ディスクをブート可 能にする必 要があります。
- *段 階 2:*

  クリティカルボリュームが復 元されます。拡 張 復 旧タスクを実 行するには、追 加の手 順が必 要になります。「拡 張 復 旧タスク」を参 照してください。
- *段 階 3:*

  アプリケーションデータが正 しく復 元されたかどうかをチェックします (データベースの整 合 性など)。

手 動によるディザスタリカバリ

これは最 も基 本 的なディザスタリカバリ方 法で、ターゲットシステムをオリジナルシステム構 成に復 旧します。

最 初に、DR OSをインストールして構 成します。次に、Data Protectorを使 用して(オペレーティングシステムファイルを含 めた)データを復 元し、先 ほど構 成したー時 的なオペレーティングシステムファイルを、復 元されたオペレーティングシステムファイルで置き換えます。

手 動 復 旧では、フラットファイルに維 持されない記 憶域構 造に関する情 報(パーティション情 報、ディスクミラー化、ストライプ化など)を収 集しておくことが重 要なポイントになります。

ディスクデリバリーによるディザスタリカバリ

ディスクデリバリーによるディザスタリカバリ方 法(DDDR)は、UNIXのクライアントでサポートされています。サポートされているオペレーティングシステムの詳 細は、『*HPE Data Protector製 品 案 内、ソフトウェアノート、およびリファレンス*』を参 照してください。

この方 法では追 加の作 業 用クライアントは必 要ありません。最 小 限のオペレーティングシステム、ネットワーク機 能、およびData Protector Disk Agentがインストールされた、(持ち運びができる)ブート可 能な補 助ディスクを使 用します。また障 害 発 生 前に、ディスクの適 正なフォーマットとパーティション作 成に必 要な情 報を収 集しておかなければなりません。

この方 法を使うと、クライアントを短 時 間で簡 単に復 旧できます。

> **ヒント:**
> この方 法では、電 源を切らずにシステムを稼 動させたまま、システムからハードディスクドライブを取り外して新しいディスクドライブを接 続することができます。ホットスワップ式のハードディスクドライブを使 用している場 合は、この方 法が特に役 立ちます。

ディスクデリバリーによるディザスタリカバリ(DDDR)、ページ 96を参 照してください。

拡張自動ディザスタリカバリ(EADR)

Data Protectorには、WindowsおよびLinuxData Protectorクライアントおよび Cell Manager用の拡張ディザスタリカバリ手順が用意されていますこの手順を使用すると、ユーザーの操作は最小限に抑えられます。

EADRの手順では、環境に関連するすべてのデータがバックアップ時に自動収集されます。構成データのバックアップの際に、一時DR OSのセットアップと構成に必要なデータが、1つの大きなDRイメージ(リカバリセット)ファイルにパックされ、バックアップテープ(および、オプションでCell Manager上)にセル内のバックアップクライアントごとに保存されます。

このイメージファイルに加え、ディスクの適切なフォーマットとパーティション作成に必要な段階1開始情報(P1Sファイルに保存)がCell Managerに保存されます。障害発生時には、EADRウィザードを使用して、バックアップメディアからDR OSイメージを復元し(フルバックアップ中にCell Managerに保存されていない場合)、**ディザスタリカバリCD ISOイメージ**に変換し、起動可能USBドライブに保存するか、起動可能ネットワークイメージを作成します。次に、任意のCD書き込みツールを使用して、ディザスタリカバリCD ISOイメージをCDに書き込むことができます。

その後、CDまたはUSBドライブから、あるいはネットワーク経由でターゲットシステムをブートすると、DR OSが自動的にインストールおよび構成されます。ディスクのフォーマットとパーティション作成も自動的に実行され、最終的に、オリジナルシステムがData Protectorのバックアップ時の状態に復旧されます。

復旧されるボリュームは、以下のとおりです。

- ブートボリューム
- システムボリューム
- Data Protectorのインストールと構成データを含むボリューム

その他のボリュームは、Data Protectorの標準復元手順で復旧できます。

ワンボタンディザスタリカバリ(OBDR)

ワンボタンディザスタリカバリ(OBDR)とは、WindowsとLinux Data Protectorクライアント用に自動化されたData Protectorディザスタリカバリ方法で、ユーザーの操作は最小限に抑えられています。この方法では、OBDRデバイスの使用とテープへのイメージファイルのコピーが必要になります。サポートされているオペレーティングシステムの詳細は、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。

OBDRバックアップ中には、DR OSを一時的にインストールして構成するために必要なデータが単一の大きいOBDRイメージファイルにパックされ、バックアップテープに書き込まれます。障害が発生した場合には、OBDRデバイスを使用して、OBDRイメージファイルとディザスタリカバリ情報を含むテープからターゲットシステムを直接ブートします。Data Protectorは次に、DR OSのインストールと構成、ディスクのフォーマットとパーティション作成を自動的に行い、最後に元のオペレーティングシステムをData Protectorとともにバックアップと同じ状態に復元します。

自動的に復旧されるボリュームは、以下のとおりです。

- ブートボリューム
- システムボリューム
- Data Protectorのインストールと構成データを含むボリューム

その他のボリュームは、Data Protectorの標準復元手順で復旧できます。

重要:
ハードウェア、ソフトウェア、または構成を変更するたびに、新しいOBDRブートテープをクライアント上でローカルに準備する必要があります。これは、IPアドレスやDNSサーバーの変更など、ネットワーク構成が変更された場合も同じです。

HPEバックアップメディア、DRイメージ、SRDファイル、ディザスタリカバリCD、DR OSデータを格納しているUSBドライブへのアクセスを制限しておくことをお勧めします。

HPE Data Protectorの統合とディザスタリカバリ

ディザスタリカバリは、複数のメーカーの製品に関係する非常に複雑なプロセスです。したがって、ディザスタリカバリを成功させるには、すべてのベンダーの製品に対して適切な処置をとる必要があります。ここに記載されている情報は、あくまで目安として使用してください。

ディザスタリカバリにどのように備えるべきかについては、データベースやアプリケーションのベンダーの指示をチェックしてください。

ここでは、アプリケーションを復旧する際の全般的な手順を示します。

1. ディザスタリカバリを実行します。
2. Data Protectorメディア上のデータをシステムに再ロードできるように、データベースやアプリケーションをインストール、構成、および初期設定します。データベースを準備するために必要な手順の詳細は、データベースやアプリケーションのベンダーから提供されているマニュアルを参照してください。
3. 必要なData Protectorクライアントソフトウェアがデータベースやアプリケーションのサーバーにインストールされており、正しく構成されていることを確認します。*HPE Data Protectorインテグレーションガイド*の該当する部分の手順に従ってください。
4. 復元を開始します。復元が完了したら、データベースやアプリケーションのベンダーの指示に従い、データベースをオンラインにするための手順を、必要に応じて実施します。

第2章: ディザスタリカバリの準備方法

迅速かつ効率的な復元処理を可能にするには、以下の手順に慎重に従って、ディザスタリカバリの準備をしておかなければなりません。選択するディザスタリカバリ方法にかかわらず準備手順は同じであり、あらかじめ詳細なディザスタリカバリ計画をたてて、整合性のとれた適切なバックアップを行い、Windows上でSRDファイルを更新します。

この章では、すべてのディザスタリカバリの方法に共通の一般的な準備手順について説明します。ディザスタリカバリ方法ごとに、追加の準備作業が必要になります。追加の準備作業については、対応するトピックを参照してください。

Cell Managerのディザスタリカバリは特に重要であるため、より慎重な準備作業が求められます。

> **重要:**
> 障害が発生する前にディザスタリカバリを準備します。

計画

綿密なディザスタリカバリプランの作成は、ディザスタリカバリの手順が円滑に実行されるかどうかに大きく影響します。さまざまなシステムが混在する大規模な環境でディザスタリカバリを行うには、以下の手順で行います。

1. **計画**

   計画は、IT管理者が作成する必要があります。計画には、以下の手順を含めてください。

   - 特に重要であり最初に復旧する必要があるシステムの一覧を作成します。重要なシステムには、ネットワークを正常に機能させるために必要なシステム(DNSサーバー、ドメインコントローラー、ゲートウェイなど)、Cell Manager、Media Agentクライアントなどがあります。これらのシステムは、ほかのシステムよりも前に復旧する必要があります。
   - 各システムに適したディザスタリカバリ方法を選択します。選択した方法に従って、それぞれのシステムに必要な準備手順を検討してください。
   - 復旧に必要となる情報をどのように取得するかを決定します。たとえば、IDBを格納するメディア、更新されたSRDファイルの保存場所、Cell Managerバックアップメディアの保存場所とラベルなどを決定しておきます。さらに、新しいインストールを実行できるようにソフトウェアライブラリの保存場所も定義しておきます。
   - 処理を進めるときに指針となる詳細なチェックリストを作成します。
   - テスト計画を作成してテストを実施し、復旧が実際に可能であることを確認します。

2. **復旧の準備**

   バックアップを実行する前に、バックアップ中に環境上の整合性が保たれるようにするための準備作業を実行します。以下の手順に従ってください。

   すべてのシステム:

- 整合性のあるバックアップを定期的に実行します。
- ボリュームグループやパーティションの概念について理解しておく必要があります。UNIXシステムの場合は、記憶域環境構造に関する情報がどこに存在するかも把握しておかなければなりません。

UNIXシステムの場合:

- 記憶データ構造を収集する実行前スクリプトを作成し、その他のクライアント固有の準備作業を実施します。
- 補助ディスク(必要最小限のオペレーティングシステム、ネットワークリソース、およびData Protector Disk Agentがインストールされたもの)などのツールを作成します。

Windowsシステムの場合:

- 有効なCONFIGURATIONバックアップが利用可能であることを確認します。
- SRDファイルを更新して、安全な場所に保管します。セキュリティを考慮し、SRDファイルへのアクセスは制限しておいてください。

3. **復旧手順の実行**

   テスト済みの手順とチェックリストに従って、影響があったシステムを復旧します。

> **注意:**
> ディザスタリカバリ用に用意されたシステムで、デフォルトのInetリッスンポートを変更しないでください。変更すると、このようなシステムが障害発生によって影響を受けた場合、ディザスタリカバリプロセスが失敗することがあります。

整合性のある適切なバックアップの実行

障害が発生した場合、ターゲットシステムをオリジナルシステム構成に戻す必要があります。さらに、そのシステムが、有効なバックアップを最後に実行したときと同じ状態で稼働および機能するようにしなければなりません。

> **注:**
> UNIXシステムでは、さまざまな理由から、デーモンやプロセスの一部はシステムのブート直後に開始します(実行レベル2)。このようなプロセスの実行により、メモリ内にデータが読み込まれたり、ファイルにダーティフラグが書き込まれたりする可能性さえあります。そのため、標準的な動作ステージ(標準実行レベル4)で実行されたバックアップでは、こうしたアプリケーションのスムーズな再開は期待できません。たとえば、先ほどのライセンスサーバーをこのような問題のある復旧後に開始すると、ファイルからの読み取りデータに不整合が検出されて、サービスが期待通りには実行されません。
>
> Windowsシステムでは、システムの実行中は多くのシステムファイルがシステムによりロックされているため、これらを置き換えることはできません。たとえば、現在使用中のユーザープロファイルは復元できません。このような場合は、ログインアカウントを変更するか、または関連するサービスを停止する必要があります。

バックアップの実行時にシステム上でアクティブであった処理内容によっては、アプリケーションデータの整合性が損なわれて、復旧後の再開や実行に問題が生じるおそれがあります。

整合性のある適切なバックアップの作成

- 理想的には、対象のパーティションをオフラインにした状態でバックアップを実行するのが一番ですが、これは不可能な場合も少なくありません。
- バックアップ中にシステム上のアクティビティを調べます。バックアップの実行中は、オペレーティングシステム関連のプロセスと、オンラインでバックアップされるデータベースサービス以外はアクティブであってはなりません。
- システムアクティビティが最小の状態になるようにします。たとえば、コアオペレーティングシステム、基本的なネットワーク機能、およびバックアップ処理のみがアクティブになるようにしてください。低レベルのアプリケーションサービスが実行中であってはなりません。適切な実行前スクリプトを使用すると、システムをこのような状態に移行できます。

ディザスタリカバリは、ファイルシステムのルートを経由して(ファイルシステム境界を超えて)バックアップされたbtrfsサブボリュームとボリュームを使用してディザスタリカバリISOイメージを作成し、復旧と復元を実行します。つまり、`/ (root)` ファイルシステムオブジェクトのバックアップには、すべてのシステム、プロファイル、関連ユーザーデータを含める必要があります。個別にバックアップされたすべてのデータ(`OB2_SHOW_BTRFS_MOUNTS`を使用したもの)は、通常のDisk Agentファイルシステムの復元操作にのみ使用することができ、復旧プロセスには使用できません。このことは、Linuxオペレーティングシステムにのみ適用されます。

> **注:**
> Data Protectorには手動で作成したbtrfsスナップショットのデータが含まれます。

整合性のある適切なバックアップに含める必要のあるデータは、使用するディザスタリカバリ方法や、システム固有の特性や機能によって異なります(Microsoft Cluster Serverのディザスタリカバリなど)。詳細については、特定のディザスタリカバリ方法の準備に関するトピックを参照してください。

暗号化されたバックアップ

バックアップが暗号化されている場合、暗号化キーが安全に保存されており、ディザスタリカバリを開始するときに使用可能であることを確認する必要があります。適切な暗号化キーにアクセスできないと、ディザスタリカバリの手順が中断してしまいます。異なるディザスタリカバリの方法には、追加の必要条件が存在します。

暗号化キーは、一元化されてCell Managerに保存されます。したがって、暗号化キーを取得するにはディザスタリカバリクライアントをCell Managerに接続する必要があります。暗号化の詳細については、『HPE Data Protectorヘルプ』のキーワード「暗号化」で表示される内容を参照してください。

2つのディザスタリカバリのシナリオが考えられます。

- Cell Managerへの接続を確立できるクライアントの復旧。Data Protectorでは自動的に暗号化キーが取得されるので、このシナリオに暗号化に関連する追加の準備は必要ありません。
- Cell ManagerまたはCell Managerへの接続を確立できないスタンドアロンクライアントのディザスタリカバリ。

  プロンプトが表示されたら、リムーバブルメディア(フロッピーディスクなど)に暗号化キーを設定する必要があります。

  キーは、ディザスタリカバリOSイメージには含まれず、キーファイル(`DR-ClientName-keys.csv`)にエクスポートされます。キーは、ディスケット、USBフラッシュドライブなどの個別のリムーバブルメディアに手動で格納する必要があります。ディザスタリカバリの準備のための各バックアップについて、暗号化キーが

正しくコピーされていることを常に確認するようにしてください。暗号化キーが使用できないと、ディザスタリカバリは実行できなくなります。

システム復旧データの更新と編集

システム復旧データ(SRD)とは、ターゲットシステムの構成に必要な情報が収められたUNICODE(UTF-16)形式のテキストファイルです。SRDファイルは、CONFIGURATIONバックアップがWindowsクライアント上で実行されCell Manager上の次のディレクトリに保存されるときに生成されます。

Windowsシステムの場合: *Data_Protector_program_data*\Config\Server\DR\SRD

UNIXシステムの場合: /etc/opt/omni/server/dr/srd。

> **重要:**
> IDBが使用できない場合、オブジェクトとメディアの情報はSRDファイルだけに保存されます。

Cell Manager上のSRDファイル名は、生成元コンピューターのホスト名と同一になります(computer.company.comなど)。

CONFIGURATIONバックアップの後、SRDファイルに記録されているのは、DR OSをインストールするために必要なシステム情報だけです。ディザスタリカバリを実行するには、バックアップオブジェクトとそのオブジェクトが格納されたメディアに関する情報をSRDに追加する必要があります。SRDは、WindowsクライアントまたはLinuxクライアントでのみ更新できます。更新されたSRDファイルの名前は、recovery.srdとなります。

SRDファイルの更新には、以下の3種類の方法を使用できます。

- SRDファイルの更新ウィザード(Windowsシステムからのみ)
- omnisrdupdate omnisrdupdateコマンド(スタンドアロンユーティリティとして使用)
- omnisrdupdate omnisrdupdateコマンド(バックアップセッションの実行後スクリプトとして使用)

> **重要:**
> Cell ManagerのSRDファイルを更新する際は、復旧後にファイルシステムバックアップセッションとデータを検索できるように、ファイルシステムバックアップセッションより新しいIDBバックアップセッションを指定します。

SRDファイルを更新する手順の詳細については、SRDファイルを更新する(Windowsクライアント)、ページ27を参照してください。

第3章: Windowsシステム上でのディザスタリカバリ

半自動ディザスタリカバリ(AMDR)

Windowsでは、復旧時にディザスタリカバリオペレーティングシステム(DR OS)のインストールが必要になります。元のオペレーティングシステムを復旧するための手順は、omnidrコマンドにより自動化されています。

Windowsシステム上では、ディザスタリカバリを実施する前に、別の方法でシステムを復旧できる可能性があります。最初にセーフモードでシステムをブートするか、システム修復フロッピーディスクからブートして、問題の解決を試みてください。

概要

準備の章に記載されている一般的な準備手順すべてを実行しておく必要があります。Windowsシステムの半手動ディザスタリカバリの一般的手順は以下のとおりです。

1. **段階1**
   a. 故障したハードウェアを交換します。
   b. オペレーティングシステムを再インストールします(必要なボリュームを作成およびフォーマットします)。
   c. サービスパックを再インストールします。
   d. 手動でディスク上にパーティションを再作成し、オリジナルのドライブ文字を割り当てて、オリジナルの記憶データ構造を再確立します。

   > **ヒント:**
   > 手動ディザスタリカバリの段階1は、自動展開ツールと組み合わせて使用できます。

2. **段階2**
   a. Data Protector drstartコマンドを実行します。このコマンドは、DR OSをインストールし、システムの重要なボリュームの復元を開始します。
   b. drstartコマンドの実行が終了したら、システムを再起動する必要があります。
   c. Cell Managerを復旧する場合、または拡張復旧タスクを行う場合は、特別な手順が必要となります。詳細については、「拡張タスク」(72ページ)を参照してください。
3. **段階3**
   a. ユーザーデータおよびアプリケーションデータを復元する場合は、Data Protectorの標準復元手順を使用します。

要件

- 新しいディスク上の各パーティションは、障害が発生したディスク上のパーティションと同じかそれより大きいサイズでなければなりません。これにより、クラッシュしたディスク上の情報を新しいディスクに復元できます。また、

ファイルシステムの種類(FAT、NTFS)と圧縮属性も、元のディスクと一致していなければなりません。

- ターゲットシステムのハードウェア構成は、オリジナルシステムのハードウェア構成と同じでなければなりません。これには、SCSIのBIOS設定(セクターの再マッピング)も含まれます。
- すべてのハードウェアが同一でなければなりません。
- クライアントのディザスタリカバリを実行する前に、オンライン復旧用のCell Manager上およびオフライン復旧用のメディアホスト上で以下のコマンドを実行します。
  `omnicc -secure_comm -configure_for_dr <hostname_of_client being_recovered>`
- クライアントのオンライン復旧後に、Cell Manager上で次のコマンドを実行します。
  `omnicc -secure_comm -configure_peer <client_host_name> -overwrite`

手順

1. 半自動ディザスタリカバリの準備(Windowsシステム)、下.
2. Windowsシステムを手動でインストールおよび構成する、ページ 30.
3. システムデータを手動で復元する(Windowsシステム)、ページ 33.
4. ベンダー固有のパーティションを復元する(Windowsシステム)、ページ 34.
5. ユーザーデータを復元します。

半自動ディザスタリカバリの準備(Windowsシステム)

ディザスタリカバリを成功させるには、このトピックに記載された手順を実行する前に、ディザスタリカバリ方法の一般的な準備手順に従ってください。ディザスタリカバリを迅速かつ効率的に実行するには、事前の準備作業が欠かせません。Cell Managerのディザスタリカバリの準備は、特に慎重に行う必要があります。

> **重要:**
> 障害が発生する前にディザスタリカバリを準備します。

一般的な準備作業

この項で挙げられている手順を行う前に、すべてのディザスタリカバリの方法に共通する一般的な準備手順として「計画、ページ 18」も参照してください。障害から迅速かつ効率的に復旧するため、以下の項目を考慮した上で適切な環境を準備してください。

1. システムをCD-ROMから起動するには、起動可能なWindowsインストールCD-ROMが必要です。起動可能なCD-ROMドライブがない場合は、Windowsフロッピーディスクを使用することも可能です。
2. 復旧するシステムで必要なドライバーが手元にあることを確認します。Windowsのセットアップ中に、HBAやSCSIなどのドライバーのインストールが必要になることがあります。
3. 影響があったシステムを復旧するには、システムに関する以下の情報を障害発生前に収集しておく必要があります。
   - 障害発生前にDHCPが使用されていなかった場合は、TCP/IPプロパティ情報(IPv4の場合はIPアドレス、デフォルトゲートウェイ、サブネットマスクおよびDNS順序、IPv6の場合はサブネットプレ

フィックスの長さ、優先サーバーおよび代替DNSサーバー)が必要です。

- クライアントプロパティ(ホスト名、ドメイン)

4. 以下の条件が当てはまることを確認します。
   - 復旧するシステムの有効なフルクライアントバックアップイメージ(有効なCONFIGURATIONバックアップデータを含む)が必要です。『HPE Data Protectorヘルプ』のキーワード「バックアップ、Windowsの場合」および「バックアップ、構成」で表示される内容を参照してください。
   - 復旧に使用するSRDファイルを用意しておきます。このSRDファイルは、バックアップセッションのオブジェクトに関する情報を反映するように更新しておく必要があります。
   - Cell Managerの復旧では、クライアントバックアップイメージの後に作成された有効な内部データベースバックアップイメージが必要です。IDBバックアップの構成方法および実行方法の詳細は、『HPE Data Protectorヘルプ』のキーワード「IDB、構成」で表示される内容を参照してください。
   - Microsoft Cluster Serverのための整合性のあるバックアップには、(同じバックアップセッションに)以下のものも含まれている必要があります。
     - すべてのノード
     - (管理者が定義した)管理用の仮想サーバー
     - Data Protectorがクラスター対応アプリケーションとして構成されている場合は、Cell Manager仮想サーバーとIDBも含める必要があります。

     詳細は、Microsoft Cluster Serverのディザスタリカバリについて、ページ 67を参照してください。
   - ブートパーティションを含むディスクには、Data Protectorのディザスタリカバリインストール用(15MB)とDR OSインストール用のスペースに加えて、オリジナルシステムを復元するのに十分な空き領域が必要です。
5. USBフラッシュドライブやフロッピーディスクにdrsetupイメージ("drsetupディスク")をコピーします。ディスクの数は、プラットフォームおよびWindowsオペレーティングシステムのバージョンによって異なります。これらのイメージは以下の場所に置かれています。
   - 32ビットWindowsシステム:

     Windows Vista以降のリリースの場合: *Data_Protector_program_data*\Depot\DRSetupX86

     Windows XP、Windows Server 2003の場合: *Data_Protector_home*\Depot\DRSetupX86

     Data Protectorインストールメディア: \i386\tools\DRSetupX86
   - AMD64/Intel EM64Tプラットフォーム上にある64ビットWindowsシステム:

     Windows Vista以降のリリースの場合: *Data_Protector_program_data*\Depot\DRSetupX64

     Windows XP、Windows Server 2003の場合: *Data_Protector_home*\Depot\DRSetupX64

     Data Protectorインストールメディア: \i386\tools\DRSetupX64
   - Itaniumプラットフォーム上にある64ビットWindowsシステム:

     Windows Vista以降のリリースの場合: *Data_Protector_program_data*\Depot\DRSetupIA64

     Windows XP、Windows Server 2003の場合: *Data_Protector_home*\Depot\DRSetupIA64

     Data Protectorインストールメディア: \i386\tools\DRSetupIA64

障害が発生した場合、影響を受けたクライアントの更新済みSRDファイルを1枚目のフロッピーディスク(ディスク1)に保存します。このフロッピーディスクのセットは、同一サイト内のすべてのWindowsシステムについて1組しか必要ありませんが、影響があったクライアントの最新のSRDファイルを、必ず1枚目のフロッピーディスクにコピーしなければなりません。SRDファイルが複数ある場合は、適切なバージョンの選択を求められます。

6. ディスクパーティションを障害前と同じ状態で再作成できるように、パーティションごとに次の情報を記録しておきます。これらの情報は復旧時に必要になります。
   - パーティションの長さと順序
   - パーティションに割り当てられているドライブ文字
   - パーティションのファイルシステムの種類

   この情報は、SRDファイルに保存されています。SRDファイルのdiskinfoセクションで-typeオプションを使用すると、特定のボリュームのファイルシステムの種類が分かります。

   SRDファイルからファイルシステムの種類を知る方法

種類を示す番号	ファイルシステム
1	Fat12
4および6	Fat32
5および15	拡張パーティション
7	NTFS
11および12	Fat32
18	EISA
66	LDMパーティション

次ページの表に、ディザスタリカバリの準備例を示します。表のデータは特定のシステムのものであり、それ以外のシステムでは使用できないことに注意してください。半自動ディザスタリカバリの準備に使用できる空のテンプレートについては、ディザスタリカバリ準備の一覧表の例(Windows用)、ページ 140を参照してください。

CLIを使用したリカバリ用フロッピーディスクの更新

Data Protectorには、リカバリイメージ(フロッピーディスク)を自動的に作成するコマンドはありません。ただし、`omnisrdupdate`コマンドを使用すると、リカバリセットの1枚目のフロッピーディスクの内容を手動で更新できます。リカバリセットの1枚目のフロッピーディスクをフロッピードライブに挿入し、次の例のように保存場所として`a:\`を指定します。

Data Protectorクライアントシステム:

```
omnisrdupdate -session 10/04/2011-1 -host clientsys.company.com -location a:\ -asr
```

Data Protector Cell Manager:

```
omnisrdupdate -session 10/04/2011-1 10/04/2011-2 -host cmsys.company.com -location
a:\ -asr
```

リカバリ用フロッピーディスクを手動で作成するには、さらに、Data_Protector_program_data\Depot\DRSetup\DiskDiskNumberフォルダーからDRDiskNumber.cabファイルを適切なリカバリ用フロッピーディスクにコピーする必要があります。

Cell Managerのための追加の準備作業

Cell Managerのディザスタリカバリを成功させるには、追加の準備作業が必要になります。

- Cell Managerに対してディザスタリカバリを実行する前に、ディザスタリカバリで使用するメディアホスト上で次のコマンドを実行します。

  ```
  omnicc -secure_comm -configure_for_dr <cell_manager_hostname>
  ```

- リカバリが完了したら、メディアホスト上で次のコマンドを実行します。

  ```
  omnicc -secure_comm -configure_peer <cell_manager_hostname>
  ```

- IDBを定期的にバックアップします。

制限事項

- Internet Information Serverデータベース、ターミナルサービスデータベースおよびCertificate Serverデータベースは、段階2で自動的には復元されません。標準のData Protector復元手順を使用して、ターゲットシステムに復元できます。
- このようなバックアップの整合性を保証できないので、再開されたオブジェクトバックアップを復旧に使用することはサポートされていません。

ディザスタリカバリ準備の一覧表の例(Windows用)

クライアントプロパティ	コンピューター名	ANAPURNA
	ホスト名	anapurna.company.com
ドライバー		tatpi.sys, aic78xx.sys
Windows Service Pack		Windows Vista
IPv4用のTCP/IPプロパティ	IPアドレス	10.17.2.61
	デフォルトゲートウェイ	10.17.250.250
	サブネットマスク	255.255.0.0
	DNS順序	10.17.3.108, 10.17.100.100

IPv6用のTCP/IPプロパティ	IPアドレス	td10:1234:5678:abba::6:1600
	サブネットプレフィックスの長さ	64
	デフォルトゲートウェイ	td10:1234:5678:abba::6:1603
	優先度の高いDNSサーバー	td10:1234:5678:abba::6:1603
	代替DNSサーバー	td10:1234:5678:abba::6:1604
メディアラベル/バーコード番号		"anapurna - disaster recovery" / [000577]
パーティション情報/順序	最初のディスクラベル	
	最初のパーティションの長さ	31MB
	最初のドライブ文字	
	最初のファイルシステム	EISA
	2番目のディスクラベル	BOOT
	2番目のパーティションの長さ	1419MB
	2番目のドライブ文字	C:
	2番目のファイルシステム	NTFS/HPFS
	3番目のディスクラベル	
	3番目のパーティションの長さ	
	3番目のドライブ文字	
	3番目のファイルシステム	

SRDファイルを更新する(Windowsクライアント)

構成後に、SRDファイル(DR OSのインストールに必要なシステム情報を含む)をバックアップします。これは、次のCell Managerにあります。

Windowsシステムの場合: *Data_Protector_program_data*\Config\Server\DR\SRD

UNIXシステムの場合: /etc/opt/omni/server/dr/srd

ディザスタリカバリを実行するには、バックアップオブジェクトとそのオブジェクトが格納されたメディアに関する情報をSRDに追加する必要があります。SRDは、Windowsクライアントでのみ更新できます。Cell Manager上のSRDファイル名は、生成元のコンピューターのホスト名と同じになります(例: computer.company.com)。更新されたSRDファイルの名前は、recovery.srdとなります。

バックアップデバイスまたはSRDファイルに格納されたメディアに関する情報が、ディザスタリカバリを実行するときには最新の状態でない可能性があります。その場合は、ディザスタリカバリを実行する前に、SRDファイルを編集して、正しくない情報を関連情報に置き換えます。

重要:
Cell ManagerのSRDファイルは、安全な場所(Cell Manager以外の場所)に保管しておいてください。SRDファイルへのアクセスは制限しておくことをお勧めします。

Windowsシステム上のData Protectorディザスタリカバリウィザードによる SRDファイルの更新

手順

1. Data Protectorコンテキストリストで**[復元]**をクリックします。
2. Scopingペインで**[タスク]**タブをクリックし、**[ディザスタリカバリ]**をクリックしてディザスタリカバリウィザードを開始します。
3. [ホスト]ドロップダウンリストから、SRDファイルを更新するシステムを選択します。
4. [ディザスタリカバリの方法]リスト内で**[SRDファイルの更新]**を選択します。**[次へ]**をクリックします。
   まず最初に、Cell Manager上のSRDファイルが検索されます。見つからなければ、前回のバックアップから復元されます。
5. 論理ボリュームとシステム構成の復元に必要なオブジェクトとバージョンを選択します。オブジェクトごとに、**[次へ]**をクリックします。
6. SRDファイルの出力先を指定します。**[完了]**をクリックします。

omnisrdupdateコマンドによるSRDファイルの更新

スタンドアロンコマンドとして`omnisrdupdate`を使用することも可能です。

SRDファイルを更新するには、既存のバックアップ仕様を修正するか、実行後スクリプトを指定して新しい仕様を作成します。

手順

1. Data Protectorコンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで**[バックアップ仕様]**→**[ファイルシステム]**の順に展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 変更するバックアップ仕様をクリックします。
4. [オプション]プロパティページで、[バックアップ仕様オプション]の下の**[拡張]**ボタンをクリックします。
5. [バックアップオプション]ウィンドウの[実行後]テキストボックスに`omnisrdupdate`と入力します。
6. [実行対象]ドロップダウンリストで、この実行後スクリプトを実行するクライアントを選択し、**[OK]**をクリックします。
7. **[適用]**をクリックします。変更内容が保存されて、ウィザードが終了します。

実行後スクリプトによるSRDファイルの更新

SRDを更新するもう1つの方法は、バックアップの実行後スクリプトとしてomnisrdupdateコマンドを使用します。この方法を使用するには、既存のバックアップ仕様を変更するか、新しいバックアップ仕様を作成す

ることが必要です。以下の手順に従ってバックアップ仕様を変更することにより、バックアップセッション終了時に、バックアップされたオブジェクトに関する情報を使ってSRDファイルが更新されます。

1. [バックアップ]コンテキストで**[バックアップ仕様]** → **[ファイルシステム]**の順に展開します。
2. 変更したいバックアップ仕様を選択します(選択するバックアップ仕様には、SRDファイルでクリティカルとマークされているバックアップオブジェクトがすべて含まれていることが必要です。そうでない場合は、更新は正常に実行されません。このため、ディスクディスカバリを使ったクライアントバックアップを実行することをお勧めします)。選択後、結果エリアで**[オプション]**をクリックします。
3. [バックアップ仕様オプション]の下の**[拡張]**ボタンをクリックします。
4. [実行後]テキストボックスに「`omnisrdupdate`」と入力します。
5. この実行後スクリプトを実行するクライアントを[実行対象]ドロップダウンリストで選択し、**[OK]**を選択して確認します。選択するクライアントは、[ソース]ページでバックアップ対象としてマークされているクライアントでなければなりません。

omnisrdupdateコマンドを実行後ユーティリティとして実行すると、セッションIDは指定しなくても自動的に取得されます。

その他すべてのオプションは、スタンドアロンユーティリティ(`-location` *`Path`*, `-host` *`ClientName`*)の場合と同様に指定できます。

> **重要:**
> IDBは別のセッションでバックアップされるので、Cell ManagerのSRDを更新するために実行後スクリプト内でomnisrdupdateを使用することはできません。

SRDファイルを編集する場合の例

SRDファイル内の情報が最新でない場合(たとえば、バックアップデバイスを変更した場合)、更新されたSRDファイル(`recovery.srd`)を、段階2(ディザスタリカバリの)を実行する前に変更して、正常な復旧ができるように正しくない情報を更新します。

`devbra -dev`コマンドを使用すると、一部のデバイス構成情報を表示できます。

MAクライアントの変更

クライアント`old_mahost.company.com`に接続されているバックアップデバイスを使って、ディザスタリカバリ用のバックアップを実行したとします。しかし、ディザスタリカバリ時には、同じバックアップデバイスが同じSCSIアドレスのクライアント`new_mahost.company.com`に接続されているとします。ディザスタリカバリを実行するには、ディザスタリカバリの段階2を実行する前に、更新後のSRDファイル内の`-mahost old_mahost.company.com`という文字列を`-mahost new_mahost.company.com`に置き換えます。

新しいMAクライアントバックアップデバイスに異なるSCSIアドレスが使用されている場合は、更新後のSRDファイル内の`-devaddr`オプションの値も変更します。

ファイルを編集し終えたら、元の場所にUnicode(UTF-16)形式で保存します。

バックアップデバイスの変更

バックアップに使用したデバイスとは別のデバイスを使ってディザスタリカバリを実行するには、更新後のSRDファイル内の以下のオプション値を変更します。

`-dev`、`-devaddr`、`-devtype`、`-devpolicy`、`-devioctl`、`-physloc`

ここで:

-dev	バックアップに使用するバックアップデバイスまたはドライブ(ライブラリ)の論理名を指定します。
-devaddr	SCSIアドレスを指定します。
-devtype	Data Protectorのデバイスの種類を指定します。
-devpolicy	デバイスのポリシーを指定します。1(スタンドアロン)、3(スタッカー)、5(ジュークボックス)、6(外部制御)、8 (Grau DASエクスチェンジャーライブラリ)、9 (STK Siloメディアライブラリ)、または10 (SCSI-IIライブラリ)のいずれかを定義できます。
-devioctl	ロボティクスのSCSIアドレスを指定します。
-physloc	ライブラリスロットを指定します。
-storname	論理ライブラリ名を指定します。

たとえば、MAホストdagnja (Windowsシステム)に接続されていてデバイス名がUltrium_dagnjaであるHPE Ultriumスタンドアロンデバイスを使用して、ディザスタリカバリ用のバックアップを実行したとします。ただし、ディザスタリカバリには、MAクライアントkerala(Linuxシステム)に接続されているUltrium_keralaというドライブを使用し、論理ライブラリ名がAutoldr_keralaであるHPE Ultriumロボティクスライブラリを使用するとします。

最初に、kerala上でdevbra -devコマンドを実行し、構成済みデバイスと構成情報のリストを表示します。この情報は、更新後のSRDファイル内の以下のオプション値を置き換える場合に必要です。

```
-dev "Ultrium_dagnja" -devaddr Tape4:1:0:1C -devtype 13 -devpolicy 1 -mahost
dagnja.company.com
```

これを次のように置き換えます。

```
-dev "Ultrium_kerala" -devaddr /dev/nst0 -devtype 13 -devpolicy 10 -devioctl
/dev/sg1 -physloc " 2 -1" -storname "AutoLdr_kerala" -mahost kerala.company.com.
```

ファイルを編集し終えたら、元の場所にUnicode(UTF-16)形式で保存します。

Windowsシステムを手動でインストールおよび構成する

障害が発生したら、最初にオペレーティングシステムをインストールして構成する必要があります。オペレーティングシステムをインストールした後、システムデータの復旧を開始できます。

手順

段階1

1. CD-ROMからWindowsシステムをインストールし、必要に応じてその他のドライバーもインストールします。Windowsオペレーティングシステムは、障害発生前と同じパーティションにインストールする必要があります。システムのインストール中は、Internet Information Server(IIS)をインストールしないでく

ださい。

> **重要:**
> 以前にWindowsオペレーティングシステムをインストールしたときに、無人セットアップを使用した場合は、*%SystemRoot%*フォルダーと*%SystemDrive%*\Documents and Settingsフォルダーの両方が同じ位置にインストールされるように、今回も同じスクリプトを使用してWindowsを再インストールしてください。

2. [Windowsパーティションセットアップ]画面が表示されたら、次の操作を行います。
   - 障害発生前のシステムにEISA Utility Partition (EUP)が存在していた場合、SRDファイルに格納されたEUP情報を使用して「ダミー」FATパーティションを作成し、フォーマットします(障害発生により失われている場合)。EUPは、後でこの「ダミー」パーティションが占有しているスペースに復旧されます。「ダミー」パーティションの作成後、ただちに一時的なブートパーティションを作成してフォーマットします。
   - 障害発生前のシステムにEUPが存在していなかった場合は、障害発生前と同じ状態になるようにブートパーティションを作成してフォーマットしてください(障害発生によりブートパーティションが失われている場合)。

     Windowsのセットアップ中に、Windowsのインストールディレクトリを入力するよう求められたら、ブートパーティション上の、元のWindowsインストールが存在していたディレクトリと同じディレクトリを指定してください。

     > **注:**
     > インストール中は、問題のシステムを本来所属していたWindowsドメインではなく、ワークグループに追加してください。プライマリドメインコントローラー(PDC)を復元している場合は、復元対象のシステムを影響があったPDCによって制御されていたドメインに所属させないように注意してください。

3. TCP/IPプロトコルをインストールします。障害の発生前にDHCPが使用されていなかった場合は、次の情報を設定して、障害発生前と同様にTCP/IPプロトコルを構成します。影響があったクライアントのホスト名、IPアドレス、デフォルトゲートウェイ、サブネットマスク、およびDNSサーバー。この情報は、SRDファイルから取得できます。**[このコンピューターのプライマリDNSサフィックス]**フィールドに、適切なドメイン名が指定されていることを確認してください。

   > **注:**
   > Windowsのデフォルト設定では、Windowsのセットアップ中にDHCP(Dynamic Host Configuration Protocol)がインストールされます。

4. Windows管理者グループ(DRAdminなど)に、ディザスタリカバリ用の一時アカウントを作成し、そのアカウントをCell Manager上のData ProtectorのAdminグループに追加します。『*HPE Data Protectorヘルプ*』のキーワード「Data Protectorユーザーの追加」で表示される内容を参照してください。

   このユーザーアカウントは障害発生前のシステムには存在しないものとします。作成した一時的なWindowsユーザーアカウントは、この手順中の後で削除されます。
5. いったんシステムからログオフし、新たに作成したアカウントを使用してログオンします。
6. 障害発生前のディスクと同じ状態になるようにパーティションを作成し、フォーマットされていないすべてのパーティションをフォーマットします(使用している場合は、「ダミー」のEISAユーティリティパーティションも含む)。ユーティリティパーティションを作成するには、ベンダー固有の手順を使用します。「ダミー」のEISA Utility Partitionは、FATファイルシステムとしてフォーマットする必要があります。次に、障害発生前と同じドライブ文字を割り当ててください。

段階2

1. SRDファイル内の情報が最新でない場合(たとえば、障害後にバックアップデバイスを変更したなどの場合)、オフライン復旧を実行するには、この手順を続行する前にSRDファイルを編集します。
2. *Data_Protector_home*\Depot\drsetup\disk1(Cell Manager)または\i386\tools\drsetup\disk1(Data Protectorインストールメディア)ディレクトリからdrstartを実行します。

   drsetupフロッピーディスクを作成してある場合は、1枚目のフロッピーからdrstartを実行することも可能です。
3. drstart最初に現在の作業ディレクトリ、フロッピーディスクドライブ、およびCD-ROMドライブ内で、ディザスタリカバリセットアップファイル(dr1.cabおよびomnicab.ini)の位置がスキャンされます。必要なファイルが検出された場合は、drstartユーティリティによりディザスタリカバリファイルが*%SystemRoot%*\system32\OB2DRディレクトリにインストールされます。これらのファイルが検出されなかった場合は、ファイルをブラウズ機能で選択するか、ファイルのパスをDR Installation Sourceテキストボックスに入力する必要があります。
4. SRDファイル(recovery.srd)がdr1.cabおよびomnicab.iniと同じディレクトリで検出されなかった場合、drstartはリカバリ.srdを*%SystemRoot%*\system32\OB2DR\binディレクトリにコピーし、omnidrユーティリティが自動的に起動します。SRDファイルが見つからなかった場合は、SRDファイル(recovery.srd)のパスをSRD Pathテキストボックスに入力するか、ブラウズします。**[次へ]**をクリックします。

   ディスク上に複数のSRDファイルが見つかった場合は、適切なバージョンのSRDファイルを選択するように促すData Protectorダイアログが表示されます。

   omnidrが正常に終了したら、システムを適切にブートするのに必要なすべての重要なオブジェクトが復元されています。
5. 段階1で追加したData Protectorの一時ユーザーアカウントをCell Manager上のData Protector Adminグループから削除します(ディザスタリカバリ前にそのアカウントがCell Manager上に存在していた場合を除く)。
6. システムを再起動してログオンし、復元されたアプリケーションが実行中であることを確認します。

段階3

6. Cell Managerを復旧する場合、または拡張復旧タスク(MSCSまたはIISの復旧、kb.cfgおよびSRDファイルの編集など)を行おうとしている場合は、追加の手順が必要となります。詳細については、Data Protector Cell Manager固有の情報の復元、ページ73、および「拡張復旧タスク」を参照してください。
7. Data Protectorの標準復元手順でユーザーデータとアプリケーションデータを復元します。

一時的なDR OSは、最初のログイン後に自動的に削除されます。ただし、以下の場合は例外です。

- ディザスタリカバリウィザードがDRのインストールとバックアップメディア上のSRDファイルを発見した後、10秒以内にウィザードを中断し、**[Debugs]**オプションを選択した場合。
- omnidrコマンドを-no_resetオプションまたは-debugオプションを指定して手動で実行した場合。
- ディザスタリカバリが失敗した場合。

Data Protector Cell Manager固有の情報の復元

Windowsシステムに対する一般的な手動によるディザスタリカバリ手順が終了したら、次にData Protectorを使用して、Cell Managerの復元に必要な追加作業を行います。

IDBの復旧の一貫性を保つには、ディザスタリカバリ処理中に復旧されなかったバックアップオブジェクトに関する情報を復元します。そのためには、ディザスタリカバリで使用したCell Managerのフルクライアントバックアップのメディアをインポートしてを更新します。

システムデータを手動で復元する(Windowsシステム)

オペレーティングシステムをインストールして構成したら(段階1)、Data Protectorを使用して Data Protectorクライアントまたはを復元できます。ディザスタリカバリ(Cell ManagerとInternet Information Server (IIS)のディザスタリカバリ)には、追加の手順が必要です。

Windowsシステムの復元

手順

段階2

1. SRDファイル内の情報が最新でない場合(たとえば、障害後にバックアップデバイスを変更したなどの場合)、オフライン復旧を実行するには、この手順を続行する前にSRDファイルを編集します。
2. *Data_Protector_home*\Depot\drsetup\disk1(Cell Manager)または\i386\tools\drsetup\disk1(Data Protectorインストールメディア)ディレクトリからdrstartを実行します。

   drsetupフロッピーディスクを作成してある場合は、1枚目のフロッピーからdrstartを実行することも可能です。
3. drstart 最初に現在の作業ディレクトリ、フロッピーディスクドライブ、およびCD-ROMドライブ内で、ディザスタリカバリセットアップファイル(dr1.cabおよびomnicab.ini)の位置がスキャンされます。必要なファイルが検出された場合は、drstartユーティリティによりディザスタリカバリファイルが*%SystemRoot%*\system32\OB2DRディレクトリにインストールされます。これらのファイルが検出されなかった場合は、ファイルをブラウズ機能で選択するか、ファイルのパスをDR Installation Sourceテキストボックスに入力する必要があります。
4. SRDファイル(recovery.srd)がdr1.cabおよびomnicab.iniと同じディレクトリで検出されなかった場合、drstartはリカバリ.srdを*%SystemRoot%*\system32\OB2DR\binディレクトリにコピーし、omnidrユーティリティが自動的に起動します。SRDファイルが見つからなかった場合は、SRDファイル(recovery.srd)のパスをSRD Pathテキストボックスに入力するか、ブラウズします。**[次へ]**をクリックします。

   ディスク上に複数のSRDファイルが見つかった場合は、適切なバージョンのSRDファイルを選択するように促すData Protectorダイアログが表示されます。

   omnidrが正常に終了したら、システムを適切にブートするのに必要なすべての重要なオブジェクトが復元されています。
5. 段階1で追加したData Protectorの一時ユーザーアカウントをCell Manager上のData Protector

Adminグループから削除します(ディザスタリカバリ前にそのアカウントがCell Manager上に存在していた場合を除く)。

6. システムを再起動してログオンし、復元されたアプリケーションが実行中であることを確認します。

段階3

6. Cell Managerを復旧する場合、または拡張復旧タスク(MSCSまたはIISの復旧、kb.cfgおよびSRDファイルの編集など)を行おうとしている場合は、追加の手順が必要となります。詳細については、Data Protector Cell Manager固有の情報の復元、ページ 73、および「拡張復旧タスク」を参照してください。
7. Data Protectorの標準復元手順でユーザーデータとアプリケーションデータを復元します。

一時的なDR OSは、最初のログイン後に自動的に削除されます。ただし、以下の場合は例外です。

- ディザスタリカバリウィザードがDRのインストールとバックアップメディア上のSRDファイルを発見した後、10秒以内にウィザードを中断し、**[Debugs]**オプションを選択した場合。
- `omnidr`コマンドを`-no_reset`オプションまたは`-debug`オプションを指定して手動で実行した場合。
- ディザスタリカバリが失敗した場合。

Data Protector Cell Manager固有の情報の復元

Windowsシステムに対する一般的な手動によるディザスタリカバリ手順が終了したら、次にData Protectorを使用して、Cell Managerの復元に必要な追加作業を行います。

IDBの復旧の一貫性を保つには、ディザスタリカバリ処理中に復旧されなかったバックアップオブジェクトに関する情報を復元します。そのためには、ディザスタリカバリで使用したCell Managerのフルクライアントバックアップのメディアをインポートしてを更新します。

ベンダー固有のパーティションを復元する(Windowsシステム)

必要に応じて、一般的な手動によるディザスタリカバリ手順により、ベンダー固有のパーティション(VSP)を復元してください。

免責条項

VSPを復元するには複雑な操作が必要であり、Windowsオペレーティングシステムに対する高度な技術や知識が求められます。ここでは、参照のために情報を提示していますが、*作業者自身の責任*でこの情報を使用してください。なおVSPの復元によりパーティションの順序が変更された場合は、`boot.ini`ファイルを修正しなければなりません。`boot.ini`ファイル内の情報が正しくないと、システムはブートできません。

ディザスタリカバリの準備

VSPの復旧には拡張自動ディザスタリカバリ(EADR)とワンボタンディザスタリカバリ(OBDR)が推奨されており、これらの方法ではVSPが自動的に復旧されます。このため、ここでは、半自動ディザスタリカバリ

(AMDR)にのみ適用する事項を述べます。

AMDRを実行する場合は、VSPを含む以前の記憶領域構造を手動で再作成しなければなりません。

ASRでは、以前の記憶領域構造が自動的に再作成され、ディスク上のVSP用割り当て済みスペースが維持されます。その後で、ベンダー固有のツールと手順を使用して、未割り当てのディスクスペース上にVSPを再作成する必要があります。

Data ProtectorからVSPへのアクセスを可能にするには、Data Protectorの`omnipm`ユーティリティを使用してWindows内でVSPをマッピングしなければなりません。

手順

1. *`Data_Protector_home`*`\bin\utilns\omnipm`を実行して、Data ProtectorのPartition Mapperを開始します。
2. [Partition Mapper]ウィンドウで、[Type]列にベンダー固有のIDが示されているパーティションを選択します。
3. **[Map]**をクリックして、選択したパーティションにドライブ文字を割り当てます。ダイアログウィンドウでドライブ文字を指定し、**[OK]**をクリックします。
4. マッピングしたEISAユーティリティパーティションにData Protectorの標準復元手順でバックアップデータを復元します。
5. 手順3で作成したパーティションのマッピングを削除します。

> **注意:**
> 復旧中にVSPのルートにあるオペレーティングシステムファイル(通常は`*.sys`ファイル)を上書きしないように注意してください。これらを上書きすると、システムが起動不能になる可能性があります。したがって、これらのファイルを除外リストに追加しておくことをお勧めします。

EISAユーティリティパーティションを復元する

手順

1. EISAユーティリティパーティション(EUP)を維持しない場合は、手動で削除する必要があります。EUPが、システムBIOSが見える最初のディスクに存在する必要がある点に注意してください。Disk ManagerはEUPを作成できないため、通常のFAT16パーティションを作成し、ドライブ文字を割り当てます。
2. Data Protectorを使用してその内容を復元します。EISAユーティリティパーティションの構成オブジェクトに、**[別名で復元]**を選択します。割り当てたドライブ文字は、EUP作成時に割り当てた文字にする必要があり、復元先ディレクトリはルートディレクトリ(\)にする必要があります。
3. 必要に応じて、ルートディレクトリのエントリを並べ替えます。
   a. `omnipm`を実行し、EUPを選択して[**ルート...**]をクリックします。EUPのルートディレクトリが表示されます。
   b. ルートディレクトリのエントリの順序を元の位置に変更します。ドラッグアンドドロップを使用するか、エントリを右クリックしてオプションメニューを表示します。
4. FAT16パーティションを実際のEUPに変更します。
   a. EUPを選択して、**[マップ解除]**をクリックします。ドライブ文字が削除されます。

b. **[種類]**をクリックします。ダイアログウィンドウが表示されます。**[EISAユーティリティパーティション]**を選択します。

拡張自動ディザスタリカバリ(EADR)

拡張自動ディザスタリカバリでは、Microsoft Cluster Server (MSCS)の一部であるData Protector Cell Managerおよびクライアントのほか、通常のData Protector Cell Managerおよびクライアントも復旧します。

この項ではディザスタリカバリの状況が発生した後に実行する必要がある手順またはタスクを説明します。

概要

準備の章に記載されている一般的な準備手順すべてを実行しておく必要があります。Windowsクライアントに対して拡張自動ディザスタリカバリを行う手順の概要は、以下のとおりです。

1. **段階1**
   a. 故障したハードウェアを交換します。
   b. ディザスタリカバリCDまたはUSBドライブから、あるいはネットワーク経由でターゲットシステムを起動し、復旧範囲を選択します。完全に無人状態での復旧が可能です。

      重要:
      Windows Server 2003: ドメインコントローラーを復旧する場合、ディザスタリカバリウィザードが起動する前に標準的なWindowsログオンダイアログボックスが表示され、ディレクトリサービス復元モードの管理アカウントのユーザー名 (Administrator)とパスワードの入力が求められます。

2. **段階2**
   a. 選択した復旧範囲に応じて、選択したボリュームが自動的に復元されます。クリティカルボリューム(ブートパーティションとオペレーティングシステム)は常に復元されます。

3. **段階3**
   a. ユーザーデータおよびアプリケーションデータを復元する場合は、Data Protectorの標準復元手順を使用します。

重要:
最初に復元する必要のあるクリティカルなシステム(特にDNSサーバー、Cell Manager、Media Agentクライアント、ファイルサーバーなど)のそれぞれについて、リカバリセットを持つディザスタリカバリCDまたはブート可能USBドライブ、あるいはネットワークブート可能イメージを前もって準備します。

Cell Managerを復旧する場合は、暗号化キーを保存したリムーバブルメディアを事前に準備します。

以降の項では、WindowsクライアントのEADRに関する制限事項、準備、および、復旧方法を説明します。詳細については、「拡張復旧タスク」も参照してください。

前提条件

ディザスタリカバリの方法を選択する前に、以下の必要条件と制限事項をよくお読みください。

- 影響があったディスクと交換するための新しいハードディスクが必要です。新しいディスクのサイズは、リカバリ対象ディスク以上である必要があります。元のディスクのサイズよりも大きい場合、余った分に対しては割り当てが行われません。
- 同じバスの同じホストバスアダプターに交換用ディスクが接続されている必要があります。
- Cell Managerのディザスタリカバリでは、ファイルシステムバックアップイメージより新しい有効な内部データベースバックアップイメージが必要です。
- ターゲットシステムのハードウェア構成がオリジナルシステムのハードウェア構成と同じ必要があります。これには、SCSI BIOSの設定(セクターの再マッピング)も含まれます。
- 必ず自動マウント機能を有効にします。自動マウント機能によって、すべてのボリュームが(マウントポイントなしで)オンラインになります。自動マウントが無効であると、ドライブ文字を指定していないボリュームすべてがブートプロセス中にオフラインになります。これにより、システム予約パーティションがドライブ文字にアクセスできなくなり、ディザスタリカバリ手順が失敗することがあります。

  自動マウント機能を無効にする必要がある場合は、必ずシステム予約パーティションをマウントしておいてください。
- **Windows Server 2003:** 影響を受けたシステムがドメインコントローラーの場合、ディレクトリサービス復元モードの管理者アカウントのパスワードが必要です。
- Windows XPおよびWindows Server 2003システムの場合、DR OSをインストールするブートパーティションは少なくとも200MB以上のサイズにする必要があります。これを下回ると、障害復旧が失敗します。このディスクスペースを使用できないと、ディザスタリカバリが失敗します。元のパーティションに圧縮ドライブを適用した場合は、400MBの空き領域が必要になります。
- Windows Vista以降のリリースでは、少なくとも1つのボリュームをNTFSボリュームにする必要があります。
- Windows Server 2003システムの場合、ブートに必要なドライバーがすべて*%SystemRoot%*フォルダーに置かれていること。
- リモートの復元の場合、DR OSイメージをブートする際はネットワークが利用できる状態である必要があります。

拡張自動ディザスタリカバリの準備(WindowsシステムとLinuxシステムの場合)

ディザスタリカバリを成功させるには、このトピックに記載された手順を完了する前に、すべてのディザスタリカバリ方法の一般的な準備手順に従ってください。ディザスタリカバリを迅速かつ効率的に実行するには、事前の準備作業が欠かせません。Cell Managerのディザスタリカバリの準備は、特に慎重に行う必要があります。

> **重要:**
> 障害が発生する前にディザスタリカバリを準備します。

前提条件

ディザスタリカバリの方法を選択する前に、以下の必要条件と制限事項をよくお読みください。

- この方法による復旧を可能にするシステムおよびDR OSイメージを準備するシステムには、Data Protectorの自動ディザスタリカバリコンポーネントをインストールしておく必要があります。詳細については、『*HPE Data Protectorインストールガイド*』を参照してください。
- Windows Vista以降のリリースでは、少なくとも1つのボリュームをNTFSボリュームにする必要があります。
- ディザスタリカバリに必要なすべてのデータをバックアップすると、大量の空き容量が必要になる場合があります。通常は500MBで十分ですが、オペレーティングシステムによっては1GBが必要になることもあります。
- DR OSイメージの作成中は、Data Protectorがインストールされているパーティションに少なくとも500MBの一時的な空き容量が必要です。このスペースは、一時イメージの作成に使用されます。
- 必ず自動マウント機能を有効にします。自動マウント機能によって、すべてのボリュームが(マウントポイントなしで)オンラインになります。自動マウントが無効であると、ドライブ文字を指定していないボリュームすべてがブートプロセス中にオフラインになります。これにより、システム予約パーティションがドライブ文字にアクセスできなくなり、ディザスタリカバリ手順が失敗することがあります。

  自動マウント機能を無効にする必要がある場合は、必ずシステム予約パーティションをマウントしておいてください。
- Windows Server 2003システムの場合、ブートに必要なドライバーがすべて*%SystemRoot%*フォルダーに置かれていること。
- 必ず自動マウント機能を有効にします。自動マウント機能によって、すべてのボリュームが(マウントポイントなしで)オンラインになります。自動マウントが無効であると、ドライブ文字を指定していないボリュームすべてがブートプロセス中にオフラインになります。これにより、システム予約パーティションがドライブ文字にアクセスできなくなり、ディザスタリカバリ手順が失敗することがあります。

  自動マウント機能を無効にする必要がある場合は、必ずシステム予約パーティションをマウントしておいてください。
- クラスター環境では、各クラスターノードの列挙されたバスアドレスが同じ場合にクラスターノードを正常にバックアップできます。これには、以下のものが必要です。
  - クラスターノードが等しいマザーボード
  - 両方のノードのOSのバージョンが同じ(サービスパックと更新)
  - バスコントローラーの数と種類が同じ
  - バスコントローラーは、マザーボードの同じPCIスロットに挿入する必要がある
- オペレーティングシステムは、バックアップ時にアクティブ化する必要があります。そうでない場合は、アクティベーション期間が期限切れになったときにディザスタリカバリは失敗します。
- Windows Vista以降のリリース用のDR OSイメージを作成するには、イメージを作成するシステムに適切なバージョンのWindows Automated Installation Kit (WAIK)またはアセスメントおよびデプロイメントキット(ADK)をインストールしておく必要があります。

  Windows VistaおよびWindows Server 2008の場合:

  Windows Vista SP1およびWindows Server 2008用のAutomated Installation Kit (AIK)

Windows 7およびWindows Server 2008 R2の場合:

- Windows Automated Installation Kit (AIK) for Windows 7
- Windows Automated Installation Kit (AIK) Supplement for Windows 7 SP1(Microsoft Windows 7 SP1およびWindows Server 2008 R2 SP1用は、オプション)

Windows 8およびWindows Server 2012の場合:

- Windows 8およびWindows Server 2012用のアセスメントデプロイメントキット(ADK 1.0)

Data ProtectorWAIK/ADKバージョンがチェックされ、適切なバージョンが使用できない場合にはイメージ作成が中止されます。

Windows 8.1およびWindows Server 2012 R2の場合:

- Windows 8.1およびWindows Server 2012用のアセスメントデプロイメントキット(ADK 1.1)

- ブート可能USBデバイスからのディザスタリカバリの場合、以下のことを確認する必要があります。
  - USBストレージデバイスのサイズは1GB以上である。
  - ターゲットシステムがUSBデバイスからのブートをサポートしている。古いシステムの場合、BIOSのアップデートが必要であったり、USBストレージデバイスからのブートができない場合があります。
- Windows Vista以降のWindowsシステムバージョン用にブート可能ネットワークイメージを作成するには、次の要件を満たす必要があります。
  - ターゲットシステムで、ネットワークアダプターがPXEプロトコルを介して通信できる。このシステムのBIOSはPXEプロトコルに準拠すること。
  - Windows Deployment Services (WDS)サーバーをWindows Server 2008以降のWindowsシステム上にインストールし、構成している。WDSサーバーが、Active Directoryドメインのメンバーであるか、Active Directoryドメインのドメインコントローラーである必要がある。
  - アクティブ範囲にあるDNSサーバーとDHCPサーバーがネットワーク内で実行されている。
- Windows Vista以降のリリース上にあるIIS構成オブジェクトをバックアップするには、IIS 6 Metabase Compatibilityパッケージをインストールしてください。
- RedHat 7クライアントのリカバリISOイメージの作成時、リカバリISOイメージが正常に作成できるよう、リカバリメディア作成ホストに**squashfsツール**がインストールされていなければなりません。

制限事項

- Microsoftのブートローダーを使用しないマルチブートシステムはサポートされていません。
- Internet Information Serverデータベース、ターミナルサービスデータベースおよびCertificate Serverデータベースは、段階2で自動的には復元されません。標準のData Protector復元手順を使用して、ターゲットシステムに復元できます。
- ブート可能USBドライブは、(サポートされているすべてのプラットフォーム上の)Windows 7、Windows 8、Windows Server 2008 R2システム、(Itaniumプラットフォーム上の)Windows Server 2008システム、およびWindows Server 2012で作成することができます。
- Windows XPおよびWindows Server 2003では、SANブート構成の復旧はサポートされていません。

- 論理ボリュームのVSSディスクイメージバックアップをディザスタリカバリに使用できるのは、Windows Vista以降のリリースのみです。
- Windows XPおよびWindows Server 2003では、ネットワーク経由でターゲットシステムをブートできません。
- Windows XPおよびWindows Server 2003では、HPE Data Protectorディザスタリカバリの GUIの代わりにコンソールインターフェイスが使用できます。
- Windows Vista以降のリリースの場合、元々の暗号化されたフォルダーを非暗号化フォルダーとしてのみ復元できます。
- チェックポイント再起動バックアップセッションに属するバックアップオブジェクトバージョンを選択しないでください。
- 復元のソースとしてオブジェクトコピーを選択する場合は、以下が適用されます。
  - 復元には、フルバックアップオブジェクトのコピーのみを選択できます。
  - ボリュームのリストからボリュームリカバリセットを作成する場合にのみ、オブジェクトコピーを選択できます。セッションはサポートされていません。
  - メディアコピーはサポートされていません。
- このようなバックアップの整合性を保証できないので、再開されたオブジェクトバックアップを復旧に使用することはサポートされていません。
- DRM復元モニターは、VRDAプロセスによってディスクに書き込まれたすべてのバイト数を監視します。ディスクに書き込まれたすべてのバイト数が、Data Protectorセッションマネージャーに表示されるバイト数と一致しないこともあります。

  注:
  新しい復旧セッションモニターは、Windows Vista以降のリリースにのみ実装されています。

- スパースファイルはオフライン復元中にフルサイズに復元されます。これにより、ターゲットボリュームのスペースが不足することがあります。
- SLES 11.3では複数のデバイスがサポートされていないので、AUTODRでは複数のデバイス上のbtrfs (さまざまなbtrfs RAID構成)の復旧はサポートされません。
- SLES 11.3で稼働する現在のbtrfsツールは、新しく作成されたbtrfsファイルシステム上でUUIDを設定しません。したがって、AUTODRはバックアップで設定したように復旧中にbtrfsファイルシステム上で同じUUIDを設定することはできません。

  デバイス名の代わりにUUIDでbtrfsファイルシステムをマウントする場合、復元後に手動で`/etc/fstab`ファイルを編集する必要があります。この手動による編集は、復元されたbtrfsデバイスの新規の正しいUUIDを反映するために実行する必要があります。GRUB構成についても同じことが当てはまります。したがって、ルートデバイスに対してUUIDを指定することを回避し、デバイスを名前で置き換えます。

  システムの復旧後、btrfsにはバックアップ時のUUIDとは別のUUIDが割り当てられます。システムの前回の復旧前に作成されたバックアップから別の復旧を実行すると、AUTODRは正常なbtrfsファイルシステムを識別し、btrfsファイルシステムの再作成をスキップしようとします。
- AUTODRは、UUIDによって復旧されている現在のシステム内のbtrfsデバイスにバックアップ内のbtrfsデバイスの構成しかマップしない場合があります。AUTODRは間違ったデバイスや再作成されたデバイスの復旧をスキップすることがあります。

  これを回避するには、btrfsファイルシステムを前回のシステムの復旧後に作成されたバックアップからのみ復旧するか、システムの復旧前に存在していたbtrfsファイルシステムを手動で破壊してください。前

回のバックアップ後にユーザーが手動で再作成したbtrfsファイルシステムについても同じことが当てはまります。

> **注:**
> 復旧プロセスの開始前に、ユーザーに対してこのことを警告するメッセージが表示されます。

- btrfsスナップショットはバックアップ可能ですが、通常のサブボリュームとしてのみ復元可能です。このようなインスタンス中は、スナップショットと、スナップショットの作成元のサブボリューム間ではデータの共有はありません。親とそのスナップショットの間のすべてのコピーオンライト(COW)の関係が失われます。したがって、スナップショットからのデータが重複し、復元中に元になるデバイス上で領域不足となるため、完全なデータセットの復元ができない場合もあります。
- マウントされたbtrfsサブボリュームからのデータのみが保護されます。OSファイルシステムのインターフェイスからアクセス可能な子サブボリュームと、マウントされている親サブボリュームを考えてみてください。このような場合、Disk Agent (DA)は異なるファイルシステムとしてサブボリュームを検出し、これらのサブボリュームには専用のマウントポイントがないためにこれらをスキップしてしまうため、サブボリュームを保護しません。
- `/etc/fstab`ファイル内のマウントオプション`subvolid`(*btrfsのドキュメント*を参照)を使用してマウントしたサブボリュームは、復旧されたサブボリュームの`subvolid`はバックアップ時のものと同じである必要がないので、復旧されたシステム内のマウントからスキップされたり、間違ったマウントポイントにマウントされたりする場合があります。すべてのサブボリュームが再作成されても、HPE Data Protectorはこのようなサブボリュームでの復元をスキップするか、または間違ったサブボリューム内でデータを復元する可能性があります。

  > **注:**
  > `subvolid`の代わりに`fstab`の`subvol`オプションを使用します。

ディスクとパーティションの構成

- EADRは、Windowsクラスター上にある共有ダイナミックディスクではサポートされていません。
- システム予約済みのボリュームがダイナミックディスク上にある場合、このボリュームはData ProtectorのGUIで黄色のアイコンで示されず、緑色のアイコンで表示されます。
- ダイナミックディスクでディザスタリカバリを実行する場合、EADRを開始する前にすべてのディスクをクリーンアップする必要があります。
- EADRセッション後には、すべてのボリュームが再作成されますが、復元されるのは復旧範囲内にあるボリュームのみです。
- 新しいディスクのサイズは、クラッシュしたディスクのサイズ以上でなければなりません。元のディスクのサイズよりも大きい場合、余った分に対しては割り当てが行われません。
- EADRでサポートされているベンダー固有のパーティションは、タイプ0x12 (EISAを含む)とタイプ0xFEだけです。
- Windows XPおよびWindows Server 2003システムでは、FAT/FAT32パーティションにData Protectorをインストールしているシステム上では、ディザスタリカバリISOイメージを作成できません。Data ProtectorがNTFSボリュームにインストールされているセル内の1つ以上のクライアントが、ディザスタリカバリのイメージを作成できる必要があります。
- HPE Intelligent Provisioningツール(v.1.4、v.1.5)を使用して展開されたオペレーティングシステムの復元は、MBRパーティション情報が正しくないために失敗することがあります。
- スパースファイルはフルサイズに復元されます。これにより、ターゲットボリュームのスペースが不足することがあります。

- 物理ディスクが1つのストレージプール内に完全に属していないストレージスペースの構成はサポートされていません。

一般的な準備作業

1. クライアントシステム全体のフルバックアップを実行します。クライアント全体のバックアップを実行することをお勧めしますが、少なくとも次の重要なボリュームとオブジェクトを選択する必要があります。
   - ブートおよびシステムボリューム
   - Data Protectorインストールボリューム
   - CONFIGURATIONオブジェクトを格納しているボリューム
   - Active Directoryデータベースボリューム(Active Directoryコントローラーの場合)
   - 定数ボリューム(Microsoft Cluster Serverの場合)

   *Data Protector Cell Managerシステム*の場合は、『Cell Managerのための追加の準備作業、ページ44』を参照してください。

   『*HPE Data Protectorヘルプ*』のキーワード「バックアップ、Windowsの場合」および「バックアップ、構成」で表示される内容を参照してください。

   フルクライアントバックアップ中には、リカバリセットおよびP1Sファイルがバックアップメディアに書き込まれます。さらに、リカバリセットをCell Managerに書き込むように指定することもできます。

   留意事項:

   ***Windows Vista以降のリリースの場合*:**

   - システムボリューム(存在する場合)も、必ずバックアップしてください。
   - VSSライターを使用したディスクイメージバックアップを使って論理ボリュームをバックアップすることができます。VSSディスクイメージのバックアップでは、バックアップ中のボリュームがロック解除されたままの状態で、他のアプリケーションからアクセスできます。マウントされていないボリュームまたはNTFSフォルダーとしてマウントされているボリューム同様、IDBとCONFIGURATIONオブジェクトも通常のファイルシステムのバックアップを使用してバックアップする必要があります。

   Windows Server 2012 R2の場合:

   - 次の場合、ディスクイメージバックアップを使用してボリュームをバックアップします。
     - 重複排除ボリューム

       ファイルシステムの復元では、ボリュームはリハイドレートされるため、リカバリ中に復元先ボリュームのスペースが不足することがあります。ディスクイメージの復元では、ボリュームのサイズは維持されます。
     - Resilient File System (ReFS)ボリューム

   ***Microsoft Cluster Server*:**

   - 整合性のあるバックアップには、(同じバックアップセッション)に以下のものが含まれている必要があります。

- すべてのノード
- (管理者が定義した)管理用の仮想サーバー
- Data Protectorがクラスター対応アプリケーションとして構成されている場合は、Cell Manager仮想サーバーとIDB

上記の項目を同じバックアップセッション内に含める必要があります。

詳細は、Microsoft Cluster Serverのディザスタリカバリについて、ページ 67を参照してください。

- *クラスター共有ボリューム:* クライアントシステムのフルバックアップを実行する前に、まずData Protector仮想環境を使用して仮想ハードドライブ(VHD)ファイルおよびCSV構成データをバックアップしてください。『*HPE Data Protectorインテグレーションガイド*』を参照してください。

  一貫性を確保するには、仮想ハードドライブ(VHD)をアンマウントする必要があります。

- バックアップ実行後に、MSCS内の全ノードのP1Sファイルをマージします。これにより、各ノードのP1Sファイルには共有クラスターボリューム構成の情報が格納されます。

  フルクライアントバックアップが暗号化されている場合は、ディザスタリカバリで使用できるように暗号キーをリムーバブルメディアに格納します。Cell Managerを復旧する場合や、Cell Managerを確立できない場合は、このキーが必要です。

Windows Server 2008以降のWindows Serverバージョン上のActive Directory:

- Windows Serverをドメインコントローラーとして使用していて、Active Directoryのサイズが512MBを超える場合、クライアントバックアップのためのバックアップ仕様を変更する必要があります。ソースページで`CONFIGURATION`オブジェクトを展開し、`ActiveDirectoryService`項目および`SYSVOL`項目のチェックボックスをオフにします。

  > **注:**
  > 変更後も、Active DirectoryおよびSYSVOLはシステムボリューム(`C:/`)バックアップの一部としてバックアップされます。デフォルトでは、これらは `C:/Windows/NTDS`と`C:/Windows/SYSVOL`にそれぞれあります。

2. クライアントのディザスタリカバリを実行する前に、オンライン復旧の場合はCell Manager上で、オフライン復旧の場合はメディアホスト上で次のコマンドを実行します。
   ```
   omnicc -secure_comm -configure_for_dr <hostname_of_client being_recovered>
   ```
3. クライアントのオンライン復旧後に、Cell Manager上で次のコマンドを実行します。
   ```
   omnicc -secure_comm -configure_peer <client_host_name> -overwrite
   ```
4. 障害発生後、EADRウィザードを使用してDRイメージをディザスタリカバリCD ISOイメージに変換します。
   Windows Vista以降のリリースの場合: ディザスタリカバリCDの代わりにDR OSイメージを持つ起動可能USBドライブ、または起動可能ネットワークイメージを作成できます。
5. ISO9660形式をサポートしているCD書き込みツールを使用して、ディザスタリカバリCD ISOイメージをCDに記録します。このディザスタリカバリCDは、ターゲットシステムのブートと重要なボリュームの自動復元に使用できます。
6. ディザスタリカバリテスト計画を実施します。
7. Windowsシステムでは、一部のサービスまたはドライバーがブート後に動作しない場合、`kb.cfg`ファイルを手動で編集する必要があります。

Cell Managerのための追加の準備作業

Cell Managerの障害復旧を成功させるには、追加の準備作業が必要になります。

- Cell Managerに対してディザスタリカバリを実行する前に、ディザスタリカバリで使用するメディアホスト上で次のコマンドを実行します。
  `omnicc -secure_comm -configure_for_dr <cell_manager_hostname>`
- リカバリが完了したら、メディアホスト上で次のコマンドを実行します。
  `omnicc -secure_comm -configure_peer <cell_manager_hostname>`
- IDBを定期的にバックアップします。ファイルシステムより古いIDBセッションを指定しないでください。
- Cell ManagerのSRDファイルは、安全な場所(Cell Manager以外の場所)に保管しておいてください。
- Cell Manager用のディザスタリカバリCDイメージを事前に準備しておきます。

リカバリセットをCell Managerに保存する

リカバリセットは、大きな単一ファイルにパックされてバックアップメディアに格納され、オプションでCell Managerにも保存されます(これはフルクライアントバックアップ中に行われます)。ディザスタリカバリCDをCell Manager上で記録する場合は、リカバリセットファイルをCell Manager上のハードディスクに保存しておくと、バックアップメディアからリカバリセットを復元する場合に比べて復元速度が大幅に向上します。

バックアップ中にCell Manager上にリカバリセットファイルを保存した場合は、デフォルトのData Protector `P1S`ファイルの場所に保存されます。

デフォルトの場所を変更するには、新しいグローバルオプション`EADRImagePath = valid_path`(たとえば、`EADRImagePath = /home/images`または`EADRImagePath = C:\temp`)を指定します。

『HPE Data Protectorヘルプ』のキーワード「グローバルオプション、変更」を参照してください。

> **ヒント:**
> あて先ディレクトリに十分な空きディスクスペースがない場合には、マウントポイントを作成する(Windowsシステム)か、他のボリュームへのリンクを作成します(UNIXシステム)。

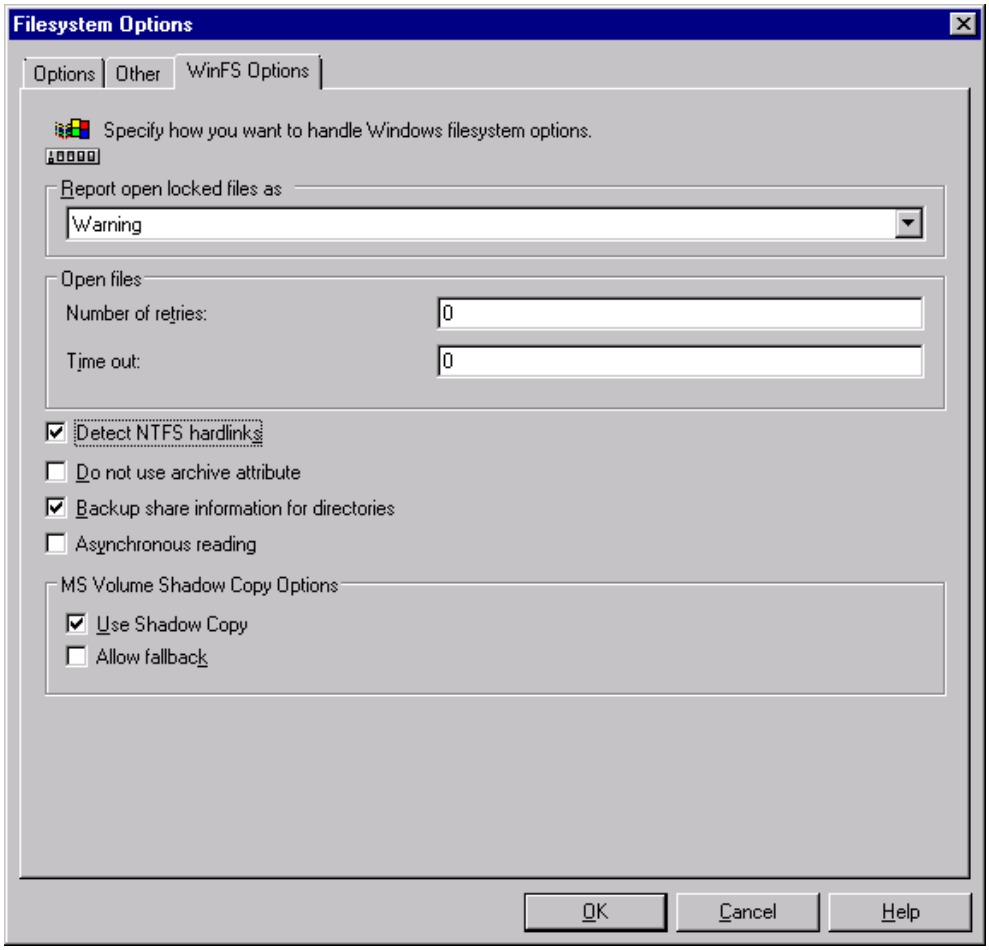
バックアップ仕様に含まれているすべてのクライアントのリカバリセットをCell Managerに保存する

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで**[バックアップ仕様]**→**[ファイルシステム]**の順に展開します。
3. フルクライアントバックアップに使用するバックアップ仕様を選択します(まだ作成していない場合は、作成してから選択します)。詳細については、『HPE Data Protectorヘルプ』のキーワード「作成、バックアップ仕様」で表示される内容を参照してください。
4. 結果エリアで**[オプション]**をクリックします。
5. **[ファイルシステムオプション]**で、**[拡張]**をクリックします。
6. **[その他]**のページで、**[リカバリセットをディスクにコピー]**を選択します。
7. **Windows Vista以降のリリースの場合:** [**WinFSオプション**]ページで[**NTFSハードリンクの検出**]オプ

ションを選択し、[**シャドウコピーを使用**]オプションを選択したまま、また、[**フォールバックを許可する**]を選択しないままにしておきます。オブジェクトを手動で追加した場合や既存のバックアップ仕様を手動で更新した場合は、**[NTFSハードリンクの検出]**オプションは自動的に選択されません。

[WinFSオプション]タブ



バックアップ仕様に含まれている特定のクライアントのリカバリセットファイルをCell Managerに保存する

バックアップ仕様内の特定クライアントのリカバリセットファイルだけをコピーする場合は、以下の手順を実行します。

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで**[バックアップ仕様]**→**[ファイルシステム]**の順に展開します。
3. フルクライアントバックアップに使用するバックアップ仕様を選択します(まだ作成していない場合は、作成してから選択します)。詳細については、『HPE Data Protectorヘルプ』のキーワード「作成、バックアップ仕様」で表示される内容を参照してください。
4. 結果エリアで**[バックアップオブジェクトのサマリー]**をクリックします。
5. リカバリセットファイルをCell Managerに保存するクライアントを選択し、**[プロパティ]**をクリックします。
6. **[その他]**のページで、**[リカバリセットをディスクにコピー]**を選択します。

7. **Windows Vista以降のリリースの場合:** [**WinFSオプション**]ページで[**NTFSハードリンクの検出**]オプションを選択しないままにし、[**シャドウコピーを使用**]オプションを選択したまま、また、[**フォールバックを許可する**]を選択しないままにしておきます。オブジェクトを手動で追加した場合や既存のバックアップ仕様を手動で更新した場合は、**[NTFSハードリンクの検出]**オプションは自動的に選択されません。

暗号化キーの準備

Cell Managerのリカバリまたはオフラインクライアントのリカバリに対しては、暗号化キーをリムーバブルメディアに保存して、ディザスタリカバリの際に使用できるようにする必要があります。Cell Managerのリカバリの場合は、障害が発生する前に、あらかじめリムーバブルメディアを準備してください。

暗号化キーは、DR OSイメージファイルの一部ではありません。ディザスタリカバリイメージの作成において、キーは自動的にCell Managerへ、ファイル*Data_Protector_program_data*\Config\Server\export\keys\DR-*ClientName*-keys.csv(Windowsシステム)または/var/opt/omni/server/export/keys/DR-*ClientName*-keys.csv(UNIXシステム)にエクスポートされます。*ClientName*はイメージが作成されているクライアント名となります。

ディザスタリカバリのために準備したバックアップごとに、正しい暗号化キーがあることを確認します。

DR OSイメージを準備する

障害が発生する前に、ディザスタリカバリCDに記録または起動可能なUSBドライブに保存するためのDR OSイメージを準備する必要があります。このDR OSイメージは、後で拡張自動ディザスタリカバリに使用できます。または、起動可能なネットワークイメージを準備することができます。

DR OSイメージを準備するシステムには、Data Protectorの自動ディザスタリカバリコンポーネントをインストールしておく必要があります。

新しいリカバリセットからハードウェア、ソフトウェア、または構成の変更を行った場合には、その都度新しいディザスタリカバリOSを準備する必要があります。

最初に復元する必要のある重要システムのそれぞれについて、DR OSイメージを事前に準備します。特に、ネットワークが正しく機能するために必要なシステム(DNSサーバー、ドメインコントローラー、ゲートウェイなど)、Cell Manager、Media Agentクライアント、ファイルサーバーなどです。

バックアップメディア、およびOSイメージが格納されているディザスタリカバリCDまたはUSBドライブへのアクセスは、セキュリティ維持のため制限しておくことをお勧めします。

手順

1. Data Protectorコンテキストリストで**[復元]**をクリックします。
2. Scopingペインで**[タスク]**をクリックし、**[ディザスタリカバリ]**をクリックしてディザスタリカバリウィザードを開始します。
3. [結果]エリアで、**[復旧するホスト]**ドロップダウンリストからDR OSイメージを準備するクライアントを選択し、**[検証]**をクリックしてクライアントを検証します。

   > **注:**
   > 検証されたクライアントは**[復旧するホスト]**ドロップダウンリストに追加されます。

4. **[リカバリメディア作成ホスト]**ドロップダウンリストから、DR OSイメージを準備するクライアントを選択します。デフォルトでは、これはDR OSイメージを準備するクライアントと同じクライアントになっています。DR OSイメージを準備するクライアントには、同じOSタイプ(Windows、Linux)をインストールし、またDisk Agentをインストールしておく必要があります。
5. **[拡張自動ディザスタリカバリ]**を選択しておき、ボリュームリカバリセットをバックアップセッションから作成するか、ボリュームのリストから作成するかを選択します。デフォルトでは、**[バックアップセッション]**が選択されています。

   [次へ]をクリックします。
6. リカバリセットの作成方法によって、以下を選択します。
   - バックアップセッションを選択した場合、ホストバックアップセッションを選択します。Cell Managerの場合はIDBセッションを選択します。
   - ボリュームのリストを選択した場合は、重要な各オブジェクトに対して、適切なオブジェクトのバージョンを選択します。

   [次へ]をクリックします。
7. リカバリセットファイルの場所を選択します。デフォルトで、**[バックアップからリカバリセットファイルを復元]**が選択されています。

   バックアップ中にCell Manager上にリカバリセットファイルを保存した場合は、**[リカバリセットファイルへのパス]**を選択してその場所を指定します。**[次へ]**をクリックします。
8. イメージ形式を選択します。以下のオプションを使用できます。
   - **起動可能ISOイメージの作成**: DR ISOイメージ(デフォルトで、`recovery.iso`)
   - **起動可能USBドライブの作成:起動可能なUSBドライブ上のDR OSイメージ**
   - **起動可能ネットワークイメージの作成**: ネットワークブートに使用可能なDR OSイメージ(デフォルトで、`recovery.wim`)
9. 起動可能なISOイメージまたは起動可能なネットワークイメージを作成する場合、作成したイメージの保存先となるディレクトリを選択します。

   起動可能なUSBドライブを作成する場合、作成したイメージの保存先となるUSBドライブまたはディスク番号を選択します。

   > **重要:**
   > 起動可能なUSBドライブの作成時には、ドライブ上に格納されたすべてのデータが消失します。
10. また、パスワードを設定して、DR OSイメージを不正使用から保護することもできます。鍵アイコンが、パスワードが設定されていることを示します。

    [パスワード]をクリックして[イメージのパスワード保護]ダイアログウィンドウを開き、パスワードを入力します。パスワードを削除するには、このフィールドをクリアします。
11. **Windows Vista以降のリリースの場合**:

    DR OSイメージに挿入するドライバーのリストを確認して、必要に応じて変更します。

    このオプションを使用して、見つからないドライバーをDR OSに追加することができます。ドライバーを手動で追加または削除するには、**[追加]**または**[削除]**をクリックします。元のドライバーを再読み込

みするには、**[再読み込み]**をクリックします。リカバリセットの%Drivers%の部分からドライバーが自動的にDR OSイメージに挿入されます。

> **重要:**
> バックアップ手順で収集されてリカバリセットの%Drivers%ディレクトリに保存されたドライバーが、DR OSでの使用に適しているとは限りません。場合によっては、Windowsプレインストール環境(WinPE)固有のドライバーを挿入して、復旧中のハードウェアの適切な動作を確保する必要があります。

12. **[完了]**をクリックしてウィザードを終了します。これにより、DR OSイメージが作成されます。
13. 起動可能なCDまたはDVDを作成する場合は、ISO9660形式をサポートしている記録ツールを使用して、ISOイメージをCDまたはDVDに記録します。

拡張自動ディザスタリカバリを使用してWindowsシステムを復旧する

Windowsシステムの拡張自動ディザスタリカバリを成功させるには、事前にすべての準備手順を完了しておかなければなりません。Cell Managerを準備する場合、まず内部データベースがそのバックアップイメージから復元され、その次にボリュームとCONFIGURATIONオブジェクトがそのバックアップイメージから復元されます。サポートされているオペレーティングシステムの詳細は、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。

手順

段階1

1. オフラインディザスタリカバリを行う場合を除き、ターゲットシステムのオペレーティングシステムに応じて、Cell Manager上のData Protectorのadminユーザーグループに、以下のプロパティを持つData Protectorアカウントを追加します。

   Windows Vista以降のリリースの場合:

   - 種類:Windows
   - 名前:SYSTEM
   - グループ/ドメイン:NT AUTHORITY
   - クライアント: 復旧するシステムの一時的なホスト名

     一時ホスト名は、Windows Preinstallation Environment (WinPE)によってシステムに割り当てられます。WinPEのコマンドプロンプトウィンドウでhostnameコマンドを実行することによって、ホスト名を取得できます。

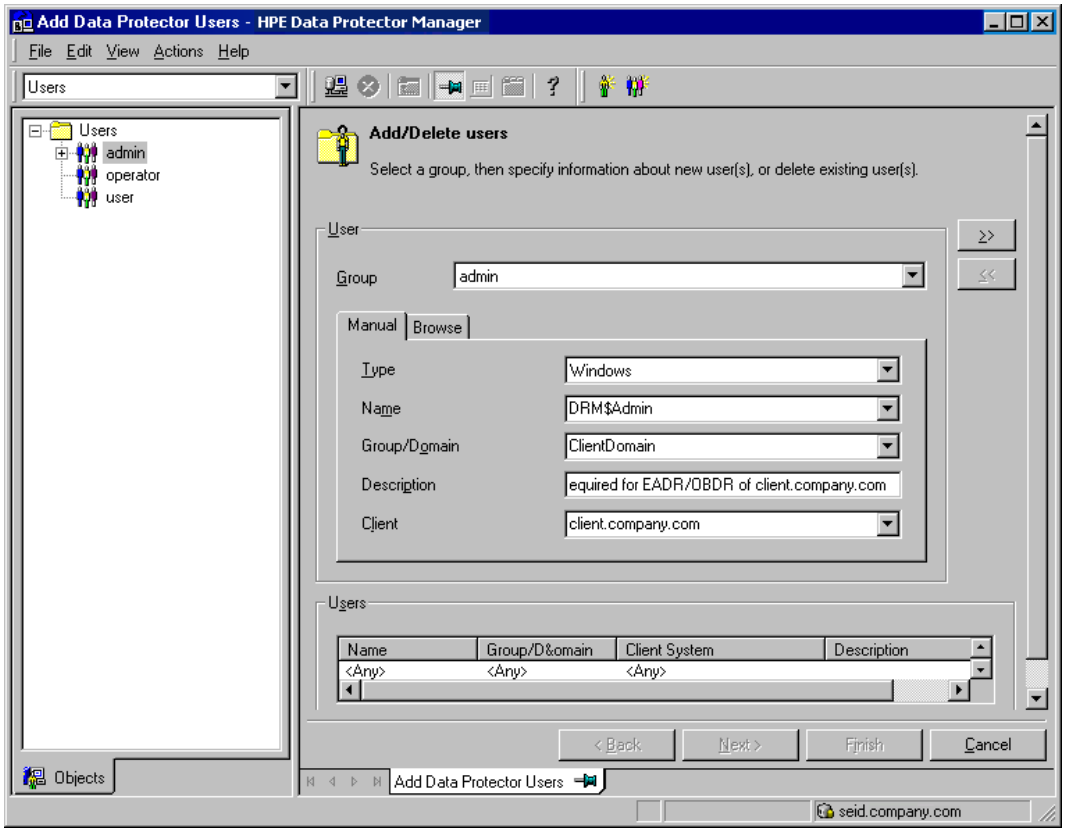
   Windows XP、Windows Server 2003の場合:

   - 種類:Windows
   - 名前:DRM$Admin

- グループ/ドメイン: ターゲットシステムのホスト名
- クライアント: ターゲットシステムの完全修飾ドメイン名 (FQDN)

ユーザーの追加方法の詳細については、『HPE Data Protectorヘルプ』のキーワード「追加、Data Protectorユーザー」で表示される内容を参照してください。

ユーザーアカウントの追加



2. オリジナルシステムのディザスタリカバリCD、起動可能USBドライブ、起動可能ネットワークイメージのいずれかからクライアントシステムをブートします。ディザスタリカバリCDからターゲットシステムを起動する場合は、復旧手順の開始前に、システムに外付けのUSBディスク(USBキーを含む)が接続されていないことを確認してください。

> **注:**
> 復旧中に画面がロックされている場合、次の資格情報を使用してログオンできます。
>
> ユーザー:DRM$ADMIN
>
> パスワード:Dr8$ad81n$pa55wD

3. **Windows Server 2003の場合:**ドメインコントローラーを復旧している場合、[Windows へようこそ]ダイアログボックスが表示されたら、Ctrl+Alt+Deleteを押して、ディレクトリサービス復元モードの管理者アカウントのパスワードを入力して[OK]をクリックします。
4. 復旧の対象範囲と復旧オプションを選択します。次の手順は、オペレーションシステムによって異なります。

   Windows Vista以降のリリースの場合:

a. ディザスタリカバリGUI(インストーラーウィザード)が起動し、オリジナルシステムの情報が表示されます。**[次へ]**をクリックします。

> **ヒント:**
> プログレスバーが表示されたときに利用可能になるキーボードオプションがあります。プログレスバーにカーソルを移動すると、利用可能になるオプションとそれらのオプションについての説明を確認できます。

b. [復旧の対象範囲]ページで、復旧の対象範囲を選択します。

- `Default Recovery`:重要なボリューム(システムディスク、ブートディスク、およびData Protectorインストールボリューム)が復旧されます。それ以外のすべてのディスクは、パーティション化されてフォーマットされ、段階3のために空のままになります。
- `Minimal Recovery`:システムディスクおよびブートディスクのみが復旧されます。
- `Full Recovery`:重要なボリュームだけでなく、復元セット内のすべてのボリュームが復元されます。
- `Full with Shared Volumes`:Microsoft Cluster Server (MSCS)の場合に選択できるオプションです。MSCS内のすべてのノードが障害の影響を受けた場合、最初のノードのEADRを実行するときにこのオプションを選択する必要があります。復元セットに含まれているボリュームがすべて復旧されます。バックアップ時にバックアップ対象のノードでロックされていたクラスター共有ボリュームもこれに含まれます。1つ以上のノードが機能しており、MSCSサービスが稼動している場合、共有ボリュームはアクティブノードによってロックされているため、復元されません。この場合は`Default Recovery`を選択してください。

c. 必要に応じて、復旧設定を変更するには、**[設定]**をクリックして[復旧設定]ページを開きます。

次の追加の復旧オプションが使用できます。オプションによっては、ディザスタリカバリが完全に終了しない場合や、追加手順が必要な場合に使用するものもあります。

- `Use original network settings`:元のネットワーク構成の復元が必要な場合(DHCPサーバーが見つからない場合など)、このオプションを選択してください。デフォルトで、このオプションは選択されていません。DR OSリカバリ環境はDHCPネットワーク構成を使用します。
- `Restore BCD`:このオプションを選択すると、Boot Configuration Data (BCD)ストアも、Data Protector復元セッションで復元される前のディザスタリカバリセッションの際にData Protectorによって復元されます。このオプションは、デフォルトで選択されています。
- `Restore DAT`:このオプションを選択すると、Data Protectorディザスタリカバリモジュールは Microsoft VSSライターのデータも復元します。デフォルトでは、DRモジュールはVSSライターのデータの復元をスキップします。VSS以外のバックアップ中にData Protectorがクリティカルライターのバックアップに失敗する場合、このオプションを使用してください。DRモジュールの復元前にデータを復元するには、`Pre`を選択します。Data Protectorの後にデータを復元するには、`Post`を選択します。
- `Initialize Disks Manually`:このオプションでは、元のシステムディスクと現在のシステムディスクを手動でマップして、それらを初期化して元の構成に一致させることができます。デフォルトではこのオプションは選択されていません。

  このオプションを選択すると、復旧プロセスを開始したときに新しいディスクのマッピングと初期化ページが表示されます。ディザスタリカバリモジュールにより、最初のディスクマッピングが実行され、マッピングの試行結果が表示されます。ディスクマッピングを変更するには提供されているオプションを使用します。マッピングが完了すると、ボリュームが初期化され、システムが再起動されます。
- `Restore Storage Spaces`:デフォルトでは、ストレージスペースが復元されます。ストレージ

構成によって可能であれば、復旧時にこのオプションの選択を解除して、仮想ディスクを直接物理ディスクに復元できます。ストレージスペースを異なるハードウェアまたはUSBディスクに復元する場合ディスクを手動で初期化する必要があるので、注意してください。

- Enable Dissimilar Hardware Restore:このオプションを有効にすると、Data Protectorは復旧中にシステムをスキャンして、見つからないドライバーを検索します。このオプションを有効にするには、ドロップダウンリストから次のいずれかの方法を選択します。
  - Unattend(デフォルト):このモードは、定義済みの構成ファイルを使用して各種のハードウェアプラットフォームに対してオペレーティングシステムを自動的に構成します。これは、異なるハードウェアでの復旧のプライマリモードです。最初のインスタンスではこのモードを使用してください。
  - Generic:無人モードが失敗した場合(復元したオペレーティングシステムの誤った構成が原因である可能性が高い)、このオプションを選択します。これは、異なるハードウェアに対する、復元されたOSレジストリ、およびOSのドライバーとサービスの適用に基づきます。
- Remove Devices:このオプションを使用できるのは、Dissimilar Hardwareオプションが有効な場合です。このオプションを選択すると、Data Protectorは、復元したオペレーティングシステムのレジストリからオリジナルのデバイスを削除します。
- Connect iSCSI Devices:このオプションは、元のマシンがiSCSIを使用していた場合に有効になり、選択されます。このオプションを選択すると、Data Protectorはバックアップ時点のiSCSIの基本構成を自動的に復元します。このオプションを選択しないと、iSCSI構成はスキップされます。

  ネイティブのMicrosoft iSCSI構成ウィザードを使用して、より複雑なiSCSI構成を管理することもできます。DR GUIによって手動構成を必要とするiSCSI機能(セキュリティオプションなど)が検出されると、Microsoft iSCSI構成ウィザードを実行するためのオプションが表示されます。
- Map Cluster Disks Manually:Windows Server 2008以降のリリースで使用可能です。選択すると、クラスターボリュームを手動でマップできます。選択しないと、ボリュームは自動的にマップされます。自動マッピング後にすべてのボリュームが適切にマップされているかどうかを確認することをお勧めします。
- Remove Boot Descriptor:Intel Itaniumシステムで使用可能です。ディザスタリカバリプロセス後に残ったすべての起動記述子を削除します。
- Manual disk selection:Intel Itaniumシステムで使用可能です。ディスク設定が大幅に変更された場合、ディザスタリカバリモジュールはブートディスクを見つけることができなくなる可能性があります。このオプションは、正しいブートディスクを選択するために使用します。

これらのオプションをデフォルト設定に戻るには、**[デフォルト設定を元に戻す]**をクリックします。

[保存]をクリックして、変更内容を保存します。

d. **[完了]**をクリックして復旧を開始します。復旧プロセスが開始され、このプロセスの進行状況を監視できます。

BitLockerドライブ暗号化を使用してボリュームが暗号化されている場合、暗号化されたドライブのロックを解除することを促すメッセージが表示されます。

> **ヒント:**
> ディザスタリカバリGUIで**[タスク]**をクリックすると、以下を実行できます。
> - コマンドプロンプト、タスクマネージャー、またはディスクアドミニストレーターの実行
> - Map Network DrivesおよびLoad Driversツールへのアクセス
> - ディザスタリカバリプロセス固有のログファイルの表示

- DRM構成ファイルの有効化または無効化、このファイルのテキストエディターでの表示、このファイルの編集
- WinPE復旧環境のホストファイルの編集
- ヘルプへのアクセスと、GUIアイコンの凡例の表示

Windows XPおよびWindows Server 2003システムの場合:

a. 以下のメッセージが表示されたら、**F12**を押します。`To start recovery of the machine Hostname press F12`

b. ブートプロセスの開始時に範囲選択メニューが表示されます。復元の対象範囲を選択し、**Enter**を押します。5つの異なる復元対象範囲があります。

- `Reboot`:ディザスタリカバリは実行されず、システムが再起動されます。
- `Default Recovery`:重要なボリューム(システムディスク、ブートディスク、およびData Protectorボリューム)が復旧されます。それ以外のすべてのディスクは、パーティション化されてフォーマットされ、段階3のために空のままになります。
- `Minimal Recovery`:システムディスクおよびブートディスクのみが復旧されます。
- `Full Recovery`:重要なボリュームだけでなく、復元セット内のすべてのボリュームが復元されます。
- `Full with Shared Volumes`:Microsoft Cluster Server (MSCS)の場合に選択できるオプションです。MSCS内のすべてのノードが障害の影響を受けた場合、最初のノードのEADRを実行するときにこのオプションを選択する必要があります。復元セットに含まれているボリュームがすべて復旧されます。バックアップ時にバックアップ対象のノードでロックされていたクラスター共有ボリュームもこれに含まれます。1つ以上のノードが機能しており、MSCSサービスが稼動している場合、共有ボリュームはアクティブノードによってロックされているため、復元されません。この場合は`Default Recovery`を選択してください。

次の追加の復旧オプションが使用できます。オプションによっては、ディザスタリカバリが完全に終了しない場合や、追加手順が必要な場合に使用するものもあります。

- `Remove Boot Descriptor`:Intel Itaniumシステムで使用可能です。ディザスタリカバリプロセス後に残ったすべての起動記述子を削除します。
- `Manual disk selection`:Intel Itaniumシステムで使用可能です。ディスク設定が大幅に変更された場合、ディザスタリカバリモジュールはブートディスクを見つけることができなくなる可能性があります。このオプションは、正しいブートディスクを選択するために使用します。

段階2

4. 復旧の対象範囲を選択すると、Data ProtectorはDR OSのセットアップを開始します。この処理の進行状況はモニター可能です。DR OSのセットアップが完了するとシステムは再起動します。Windows Vista以降のリリースの場合、システムの再起動は実行されません。

   `To start recovery of the machine Hostname press F12`のメッセージが表示されたら、10秒間待機してからF12キーを押します。これにより、CDからではなく、ハードディスクからシステムがブートされます。

   Windows XPおよびWindows Server 2003上で、DR OSが正常にブートしない場合、またはネットワークにアクセスできない場合は、kb.cfgファイルを編集する必要があります。

   ディザスタリカバリウィザードが表示されます。ディザスタリカバリオプションを変更するには、カウントダウン中に任意のキーを押してウィザードを停止した後、オプションを変更します。

以下のオプションを使用できます。

- `Debugs...`:デバッグを有効にします。「ディザスタリカバリセッションのデバッグ、ページ 121」を参照してください。
- `Omit deleted files`:連続増分バックアップ間に削除されたファイルは復元されません。これにより、復旧処理が低下することがあります。
- `Install only`:このオプションを選択すると、対象のシステムに一時オペレーティングシステムのみがインストールされて、ディザスタリカバリの段階1を完了できます。ディザスタリカバリの段階2は自動的に開始されません。SRDファイルを編集するなどの場合は、このオプションを使用できます。

また、レジストリエディター、コマンドライン、タスクマネージャーを対応するボタンで起動できます。

[完了]をクリックして、ディザスタリカバリを続行します。

5. DR OSイメージがパスワードで保護されている場合は、パスワードを入力してリカバリを続行します。
6. ディザスタリカバリバックアップが暗号化され、Cell ManagerまたはCell Managerにアクセスできないクライアントを復元している場合、以下のプロンプトが表示されます。

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   [y]キーを押します。

   クライアントでキーストア(`DR-ClientName-keys.csv`)が使用できるようにします(たとえば、CD-ROM、フロッピーディスク、またはUSBフラッシュドライブを挿入します)。その後、キーストアファイルへのフルパスを入力します。キーストアファイルは、DR OSのデフォルトの場所にコピーされ、Disk Agentによって使用されます。以降は何の操作も必要なく、ディザスタリカバリが続行されます。
7. SRDファイル内の情報が最新でない場合(たとえば、障害後にバックアップデバイスを変更したなどの場合)、オフライン復旧を実行するには、この手順を続行する前にSRDファイルを編集します。
8. 選択した復旧対象範囲内で以前の記憶域構造が再確立され、重要なボリュームがすべて復元されます。一時的なDR OSは、最初のログイン後に自動的に削除されます。ただし、以下の場合は例外です。
   - `Minimal Recovery`が選択されている。
   - ディザスタリカバリウィザードがDRのインストールとバックアップメディア上のSRDファイルを発見した後、10秒以内にウィザードを中断し、**[Debugs]**オプションを選択した場合。
   - `omnidr`コマンドを`-no_reset`オプションまたは`-debug`オプションを指定して手動で実行した場合。
   - ディザスタリカバリが失敗した場合。

   Windows Vista以降のリリースの場合、一時DR OSが残されることはありません。

   Data Protectorは、最初にオンライン復旧を実行しようとします。Data Protectorでは、Cell Managerまたはネットワークサービスが使用できない、あるいはファイアウォールによりCell Managerへのアクセスが拒否されるなどの理由でオンライン復旧が失敗すると、リモートオフライン復旧が試みられます。リモートオフライン復旧も失敗した場合(Media Agentホストが Cell Managerからの要求しか受け付けないなど)、ローカルオフライン復旧が実行されます。
9. 手順1で作成したクライアントのローカル管理者アカウントをCell ManagerのData Protector Adminユーザーグループから削除します(ディザスタリカバリ前にそのアカウントがCell Manager上に存在していた場合を除く)。
10. Cell Managerを復旧する場合は、IDBの整合性を確保します。

段階3

10. Data Protectorの標準復元手順でユーザーデータとアプリケーションデータを復元します。

> **注：**
> Data Protectorでは、復旧後にボリューム圧縮フラグが復元されません。バックアップ時に圧縮されていたファイルは、すべて圧縮状態で復元されますが、今後作成するファイルについても必ず圧縮したい場合は、ボリューム圧縮を手動で設定する必要があります。

11. Microsoft Cluster Serverですべてのノードのディザスタリカバリを実行する場合は、追加作業が必要になります。

ワンボタンディザスタリカバリ(OBDR)

ワンボタンディザスタリカバリ(OBDR)とは、Windows Data Protectorクライアント用に自動化されたData Protector復旧方法で、ユーザーの操作は最小限に抑えられています。サポートされているオペレーティングシステムの詳細については、https://softwaresupport.hpe.com/manualsにある最新のサポート一覧を参照してください。

OBDRでは、環境に関連するすべてのデータがバックアップ時に自動収集されます。バックアップの際に、一時DR OSのセットアップと構成に必要なデータが、1つの大きなOBDRイメージファイルにパックされ、バックアップテープに保存されます。障害が発生した場合には、OBDRデバイス(CD-ROMをエミュレートできるバックアップデバイス)を使用して、OBDRイメージファイルとディザスタリカバリ情報を含むテープからターゲットシステムを直接ブートします。

DR OSイメージのブート後、ディスクのフォーマットとパーティション作成が自動的に実行され、最終的に、オリジナルシステムがData Protectorとともにバックアップ時の状態に復元されます。Data Protector

> **重要：**
> ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行します。これは、IPアドレスやDNSサーバーの変更など、ネットワーク構成が変更された場合も同じです。

復旧対象となるパーティションを以下に示します。

- ブートパーティション
- システムパーティション
- Data Protectorインストールデータを格納するパーティション

その他のパーティションは、通常のData Protector復旧手順を使って復旧できます。

概要

準備の章に記載されている一般的な準備手順すべてを実行しておく必要があります。Windowsクライアントのワンボタンディザスタリカバリの一般的手順は以下のとおりです。

1. **段階1**
   復旧用テープからブートし、復旧範囲を選択します。

2. **段階2**

   選択した復旧範囲に応じて、選択したボリュームが自動的に復元されます。

   クリティカルボリューム(ブートパーティションとオペレーティングシステム)は常に復元されます。

3. **段階3**

   Data Protector標準復元手順を使用して、残りのパーティションを復元します。

> **重要:**
> OBDRブートメディアへのアクセスを制限することをお勧めします。

以下の項で、Windowsシステム上でのワンボタンディザスタリカバリに関する必要条件、制限事項、準備、および、復旧について説明します。「拡張復旧タスク」も参照してください。

要件

- この方法による復旧を可能にするシステムには、Data Protectorの自動ディザスタリカバリをインストールしておく必要があります。詳細は、『*HPE Data Protectorインストールガイド*』を参照してください。
- クライアントシステムは、OBDRで使用するテープデバイスからのブートをサポートする必要があります。

  サポートされるシステム、デバイス、メディアの詳細については、HPEのテープとハードウェアの互換性一覧表および最新のサポート一覧(https://softwaresupport.hpe.com/manuals)を参照してください。
- ターゲットシステムのハードウェア構成がオリジナルシステムのハードウェア構成と同じ必要があります。これには、SCSI BIOSの設定(セクターの再マッピング)も含まれます。
- 新しいディスクのサイズは、リカバリ対象ディスク以上である必要があります。元のディスクのサイズよりも大きい場合、余った分に対しては割り当てが行われません。
- 同じバスの同じホストバスアダプターに交換用ディスクが接続されている必要があります。
- Windows XP、Windows Server 2003の場合: バックアップ時には、ブートパーティション上に200MBの空き領域が追加で必要になります。このディスクスペースを使用できないと、ディザスタリカバリが失敗します。元のパーティションに圧縮ドライブを適用した場合は、400MBの空き領域が必要になります。
- OBDRバックアップを実行するには、Data Protectorがインストールされているパーティションに少なくとも500MBの一時的な空きスペースが必要です。このスペースは、一時イメージの作成に使用されます。
- Windows Server 2003場合: ブートに必要なドライバーがすべて*%SystemRoot%*フォルダーに置かれている必要があります。
- メディアの使用ポリシーが[追加不可能]でメディア割り当てポリシーが[緩和]のメディアプールをOBDR対応のデバイスに対して作成する必要があります。ディザスタリカバリに使用できるメディアは、このプールに所属しているメディアだけとなります。
- Windows XP、Windows Server 2003: オペレーティングシステムは、バックアップ時にアクティブ化する必要があります。そうでない場合は、アクティベーション期間が期限切れになったときにディザスタリカバリは失敗します。
- Windows Vista以降のリリース用のDR OSイメージを作成するには、イメージを作成するシステムに適切なバージョンのWindows Automated Installation Kit (WAIK)またはアセスメントおよびデプロイメントキットをインストールしておく必要があります。

  Windows VistaおよびWindows Server 2008の場合:

  Windows Vista SP1およびWindows Server 2008用のAutomated Installation Kit (AIK)

  Windows 7およびWindows Server 2008 R2の場合:

- Windows Automated Installation Kit (AIK) for Windows 7
- Windows Automated Installation Kit (AIK) Supplement for Windows 7 SP1(Microsoft Windows 7 SP1およびWindows Server 2008 R2 SP1用は、オプション)

Windows 8およびWindows Server 2012の場合:

- Windows 8およびWindows Server 2012用のアセスメントデプロイメントキット(ADK 1.0)

Windows 8.1およびWindows Server 2012 R2の場合:

- Windows 8.1およびWindows Server 2012用のアセスメントデプロイメントキット(ADK 1.1)

- Windows Vista、Windows 7またはWindows Server 2008システム上にあるIIS構成オブジェクトをバックアップするには、IIS 6 Metabase Compatibilityパッケージをインストールしてください。

制限事項

- ワンボタンディザスタリカバリ(OBDR)は、Data Protector Cell Managerでは使用できません。
- Microsoftのブートローダーを使用しないマルチブートシステムはサポートされていません。
- Windows XPおよびWindows Server 2003では、SANブート構成の復旧はサポートされていません。
- 論理ボリュームのVSSディスクイメージバックアップをディザスタリカバリに使用できるのは、Windows Vista以降のリリースのみです。
- Windows XPおよびWindows Server 2003では、HPE Data Protectorディザスタリカバリの GUIの代わりにコンソールインターフェイスが使用できます。
- Windows XPおよびWindows Server 2003では、ネットワークチーミングアダプターのある構成の復旧はサポートされていません。
- Windows Vista以降のリリースの場合、元々の暗号化されたフォルダーを非暗号化フォルダーとしてのみ復元できます。
- Internet Information Serverデータベース、ターミナルサービスデータベースおよびCertificate Serverデータベースは、段階2で自動的には復元されません。標準のData Protector復元手順を使用して、ターゲットシステムに復元できます。
- DRM復元モニターは、VRDAプロセスによってディスクに書き込まれたすべてのバイト数を監視します。ディスクに書き込まれたすべてのバイト数が、Data Protectorセッションマネージャーに表示されるバイト数と一致しないこともあります。

  > **注:**
  > 新しい復旧セッションモニターは、Windows Vista以降のリリースにのみ実装されています。

- スパースファイルはオフライン復元中にフルサイズに復元されます。これにより、ターゲットボリュームのスペースが不足することがあります。

ディスクとパーティションの構成

- ダイナミックディスクは、(Windows NTからアップグレードしたミラーセットも含め)サポートされていません。
- 新しいディスクのサイズは、クラッシュしたディスクのサイズ以上でなければなりません。元のディスクのサイズよりも大きい場合、余った分に対しては割り当てが行われません。
- OBDRでサポートされているベンダー固有のパーティションは、タイプ0x12 (EISAを含む)とタイプ0xFEだけです。

- OBDRはData ProtectorがNTFSボリュームにインストールされているシステムでサポートされています。
- Intel Itaniumシステムでは、ブートディスクの復旧はローカルのSCSIディスク向けにのみサポートされています。

ワンボタンディザスタリカバリの準備(WindowsシステムとLinuxシステムの場合)

ディザスタリカバリを成功させるには、このトピックに記載された手順を完了する前に、ディザスタリカバリ方法の一般的な準備手順に従ってください。ディザスタリカバリを迅速かつ効率的に実行するには、事前の準備作業が欠かせません。

> **重要:**
> 障害が発生する前にディザスタリカバリを準備します。

準備手順

ディザスタリカバリの一般的な準備を完了したら、以下の手順に従ってOBDRの準備をします。

1. DDSメディアまたはLTOメディア用として、メディアプールを作成します。メディア使用ポリシーは**[追加不可能]**、メディア割り当てポリシーは**[緩和]**(バックアップメディアはOBDRバックアップ時にフォーマットされるため)です。さらに、このメディアプールをOBDRデバイスのデフォルトのメディアプールに指定します。『*HPE Data Protectorヘルプ*』のキーワード「メディアプールの作成」で表示される内容を参照してください。このプールのメディアのみが、OBDRで使用できます。
2. OBDRを使用する復旧を可能にするシステム上で、OBDRバックアップをローカルに実行します。

   考慮事項

   Windows Vista以降のリリースの場合: システムボリューム(例:ブートボリューム)が存在している場合は、必ずそのバックアップを作成してください。

   Windows Server 2012 (R2)の場合: 次の場合、ディスクイメージバックアップを使用してボリュームをバックアップします。

   - 重複排除ボリューム

     ファイルシステムの復元では、ボリュームはリハイドレートされるため、リカバリ中に復元先ボリュームのスペースが不足することがあります。ディスクイメージの復元では、ボリュームのサイズは維持されます。

   - Resilient File System (ReFS)ボリューム

   Microsoft Cluster Serverの場合: 整合性のあるバックアップには、(同じバックアップセッションに)以下のものが含まれている必要があります。

   - すべてのノード
   - (管理者が定義した)管理用の仮想サーバー
   - Data Protectorをクラスター対応アプリケーションとして構成している場合、クライアントシステムの仮想サーバー

OBDRでMSCS内の全共有ディスクボリュームの自動復元を可能にするには、ボリュームをすべてOBDRブートテープの準備作業に使用するノードに一時的に移動します。そうすることで、OBDRバックアップ中に共有ディスクボリュームが他のノードによりロックされることはなくなります。バックアップ時に他のノードによってロックされる共有ディスクボリュームに関しては、段階1でディスクの構成に十分な情報を収集するのは事実上不可能です。

クラスター共有ボリューム: クライアントシステムのフルバックアップを実行する前に、まずData Protector仮想環境を使用して仮想ハードドライブ(VHD)ファイルおよびCSV構成データをバックアップしてください。『*HPE Data Protectorインテグレーションガイド*』を参照してください。バックアップは別個のデバイス上で実行する必要があります。OBDRバックアップは、追加不可能メディア上でのみ実行できるためです。

一貫性を確保するには、仮想ハードドライブ(VHD)をアンマウントする必要があります。

フルクライアントバックアップが暗号化されている場合は、ディザスタリカバリで使用できるように暗号キーをリムーバブルメディアに格納します。Cell Managerへの接続を確立できない場合このキーが必要になります。

3. クライアントのデザスタリカバリを実行する前に、オンライン復旧のためにCell Manager上で、オフライン復旧のためにメディアホスト上で次のコマンドを実行します。
   ```
   omnicc -secure_comm -configure_for_dr <hostname_of_client being_recovered>
   ```
4. クライアントのオンライン復旧後に、Cell Manager上で次のコマンドを実行します。
   ```
   omnicc -secure_comm -configure_peer <client_host_name> -overwrite
   ```
5. ディザスタリカバリテスト計画を実施します。
6. Windowsシステムでは、一部のサービスまたはドライバーがシステムの起動後に動作しない場合、`kb.cfg`ファイルを手動で編集する必要があります。

ワンボタンディザスタリカバリ用のバックアップ仕様を作成する

利用者は、OBDRブートテープを準備するためにワンボタンディザスタリカバリ(OBDR)のバックアップ仕様を作成する必要があります。

前提条件

- OBDRデバイスを追加する前に、DDSまたはLTOメディア用のメディアプールを作成します。使用ポリシーは[追加不可能]、メディア割り当てポリシーは[緩和]です。このメディアプールは、OBDRデバイス用のデフォルトメディアプールとして選択する必要があります。
- デバイスは、OBDRによる復旧を可能にしたいシステムにローカルに接続する必要があります。
- OBDRによる復旧を可能にしたいシステムには、Data Protectorの自動ディザスタリカバリコンポーネントとユーザーインターフェイスコンポーネントをインストールしておく必要があります。
- このバックアップ仕様は、OBDRによる復旧を可能にしたいシステム上でローカルに作成する必要があります。

> **ヒント:**
> OBDRブートテープを準備するノードにすべてのボリュームを一時的に移動しておくと、MS Cluster内のすべての共有ディスクボリュームをOBDRで自動的に復元できるようになります。他のノードによってロックされる共有ディスクボリュームに関しては、段階1でディスクの構成に十分な情報を収集するのは事実上不可能です。

制限事項

- ワンボタンディザスタリカバリ(OBDR)は、Data Protector Cell Managerでは使用できません。

このバックアップ仕様は、ワンボタンディザスタリカバリ方法に対して一意のものとなります。デフォルトで、必要なボリュームがファイルシステムとしてバックアップされます。ただし、Windows Vista以降のリリースの場合、VSSライターを使用すると、論理ボリュームをディスクイメージとしてバックアップできます。この方法では、バックアップ中のボリュームがロック解除されたままの状態で、他のアプリケーションからアクセスできます。論理ボリュームをディスクイメージとしてバックアップするには、OBDR用に作成したバックアップ仕様を変更する必要があります。

OBDR用のバックアップ仕様を作成する

ディスクイメージのバックアップを使用するためにOBDRバックアップ仕様を変更する

OBDR用のバックアップ仕様を作成する

手順

1. Data Protectorコンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで**[タスク]**をクリックし、次に**[ワンボタンディザスタリカバリウィザード]**をクリックします。
3. [結果エリア]で、OBDRバックアップのローカル実行の対象となるクライアントをドロップダウンリストから選択し、**[次へ]**をクリックします。
4. 必ずバックアップしなければならない重要なボリュームは既に選択されています。**[次へ]**をクリックします。

   > **重要:**
   > 重要なボリュームは自動的に選択されており、これらを選択解除することはできません。なお復旧手順を実行すると、システム上のすべてのパーティションがData Protectorにより削除されるため、そのほかにも保存が必要なパーティションがあれば、ここで選択しておいてください。

5. バックアップに使用するローカルなデバイスまたはドライブを選択します。ここでは1つのデバイスまたはドライブしか選択できません。**[次へ]**をクリックします。
6. **Windows Vista以降のリリースの場合:**

   DR OSイメージに挿入するドライバーのリストを確認して、必要に応じて変更します。

   このオプションを使用して、見つからないドライバーをDR ISOイメージに追加することができます。ドライバーを手動で追加または削除するには、**[追加]**または**[削除]**をクリックします。元のドライバーを再読み込みするには、**[再読み込み]**をクリックします。リカバリセットの`%Drivers%`の部分からドライバーが自動的にDR OSイメージに挿入されます。

   必要に応じて、バックアップオプションを選択します。

   > **重要:**
   > バックアップ手順で収集されてリカバリセットの`%Drivers%`ディレクトリに保存されたドライバーが、DR OSでの使用に適しているとは限りません。場合によっては、復旧時にハードウェアが適切に機能するように、Windows Preinstallation Environment (WinPE)固有のドライバーを追加する必要があります。

Linux: バックアップオプションを選択します。使用可能なオプションの詳細については、『HPE Data Protectorヘルプ』のキーワード「バックアップオプション」で表示される内容を参照してください。

[次へ]をクリックします。

7. [バックアップサマリー]ページでバックアップ仕様の設定を確認し、**[次へ]**をクリックします。

   あらかじめ選択されているバックアップデバイスを変更したり、バックアップ仕様の実行順序を変更することはできません。ここでは必須でないOBDRバックアップオブジェクトの削除と、一般的なオブジェクトプロパティの確認のみが可能です。また、バックアップオブジェクトの説明は変更も可能です。
8. 修正したバックアップ仕様は、ワンボタンディザスタリカバリ固有の形式が保持されるように、OBDRバックアップ仕様として保存してください。必要に応じて、**[保存とスケジュール]**オプションを使用してバックアップをスケジュールできます。
9. a. [バックアップ開始]をクリックして、バックアップを対話形式で実行します。[バックアップ開始]ダイアログボックスが表示されます。[OK]をクリックしてバックアップを開始します。

      バックアップが暗号化されている場合、実行後コマンドとして実行されるomnisrdupdateユーティリティによって暗号化IDが自動的にエクスポートされます。

一時DR OSのインストールと構成に必要な情報がすべて含まれているシステム用ブート可能イメージはテープの先頭に書き込まれ、これによりテープからのブートが可能となります。

> **重要：** ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行してブート可能なバックアップメディアを作成します。これは、IPアドレスやDNSサーバーの変更など、ネットワーク構成が変更された場合も同じです。

ディスクイメージのバックアップを使用するためにOBDRバックアップ仕様を変更する

手順

1. Scopingペインで、作成したOBDRバックアップ仕様をクリックします。OBDRバックアップ仕様または通常のバックアップ仕様として処理するかを確認するメッセージが表示されたら、**[いいえ]**をクリックします。

   > **注：**
   > OBDRバックアップ仕様を通常のバックアップ仕様として保存しても、OBDRとして使用できます。
2. [バックアップオブジェクトのサマリー]ページで、ディスクイメージとしてバックアップする論理ボリュームを選択し、**[削除]**をクリックします。

   > **注：**
   > 論理ボリュームのみをバックアップできます。マウントされていないボリュームまたはNTFSフォルダーとしてマウントされているボリューム同様、構成オブジェクトもファイルシステムのバックアップと共にバックアップする必要があります。
3. **[手動で追加]**をクリックして、ウィザードを起動します。
4. [バックアップオブジェクトの選択]ページで**[ディスクイメージオブジェクト]**オプションをクリックし、**[次へ]**をク

リックします。

5. [一般的な選択項目]ページで、バックアップするディスクイメージのあるクライアントを選択し、適切な説明を入力します。**[次へ]**をクリックします。

   > **注：**
   > 説明は、各ディスクイメージオブジェクトについて一意である必要があります。`[Disk Image C] for C: volume`のようなわかりやすい名前を使用します。

6. [一般オブジェクトオプション]プロパティページで、[データ保護]を**[なし]**に設定します。**[次へ]**をクリックします。

   > **注：**
   > データ保護を**[なし]**に設定すると、テープの内容を新しいOBDRバックアップで上書きできます。

7. [拡張オブジェクトオプション]プロパティページでは、ディスクイメージオブジェクトの拡張バックアップオプションを指定できます。**[次へ]**をクリックします。
8. [ディスクイメージオブジェクトオプション]プロパティページでは、バックアップ対象のディスクイメージセクションを指定できます。以下の形式で指定します。

   `\\.\`*`DriveLetter`*`:`、例：`\\.\E:`

   > **注：**
   > ボリューム名をドライブ名として指定すると、バックアップ中にボリュームがロックされません。マウントされていないボリュームまたはNTFSフォルダーとしてマウントされているボリュームは、ディスクイメージのバックアップに使用できません。

9. **[完了]**をクリックしてウィザードを終了します。
10. [バックアップオブジェクトのサマリー]ページで、バックアップ仕様のサマリーを表示します。ディスクイメージとして指定した論理ボリュームの種類は、ディスクイメージである必要があります。**[適用]**をクリックします。

暗号化キーの準備

Cell Managerのリカバリまたはオフラインクライアントのリカバリに対しては、暗号化キーをリムーバブルメディアに保存して、ディザスタリカバリの際に使用できるようにする必要があります。Cell Managerのリカバリの場合は、障害が発生する前に、あらかじめリムーバブルメディアを準備してください。

暗号化キーは、DR OSイメージファイルの一部ではありません。ディザスタリカバリイメージの作成において、キーは自動的にCell Managerへ、ファイル*`Data_Protector_program_data`*`\Config\Server\export\keys\DR-`*`ClientName`*`-keys.csv`(Windowsシステム)または`/var/opt/omni/server/export/keys/DR-`*`ClientName`*`-keys.csv`(UNIXシステム)にエクスポートされます。*`ClientName`*はイメージが作成されているクライアント名となります。

ディザスタリカバリのために準備したバックアップごとに、正しい暗号化キーがあることを確認します。

ワンボタンディザスタリカバリを使用してWindowsシステムを復旧する

Windowsシステムのワンボタンディザスタリカバリ(OBDR)を成功させるには、事前にすべての準備手順を完了しておかなければなりません。

OBDR用にサポートされているオペレーティングシステムの詳細は、『HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照してください。

前提条件

- 影響があったディスクと交換するための新しいハードディスクが必要です。
- 復旧するクライアントの重要なオブジェクトをすべて含む起動可能なOBDRバックアップメディアが必要です。OBDRバックアップは、クライアントでローカルに実行する必要があります。
- OBDRデバイスがターゲットシステムにローカルに接続されている必要があります。

手順

段階1

1. オフラインディザスタリカバリを行う場合を除き、ターゲットシステムのオペレーティングシステムに応じて、Cell Manager上のData Protector `admin`ユーザーグループに、以下のプロパティを持つアカウントを追加します。

   Windows Vista以降のリリースの場合:

   - 種類:`Windows`
   - 名前:`SYSTEM`
   - グループ/ドメイン:`NT AUTHORITY`
   - クライアント: 復旧するシステムの一時的なホスト名

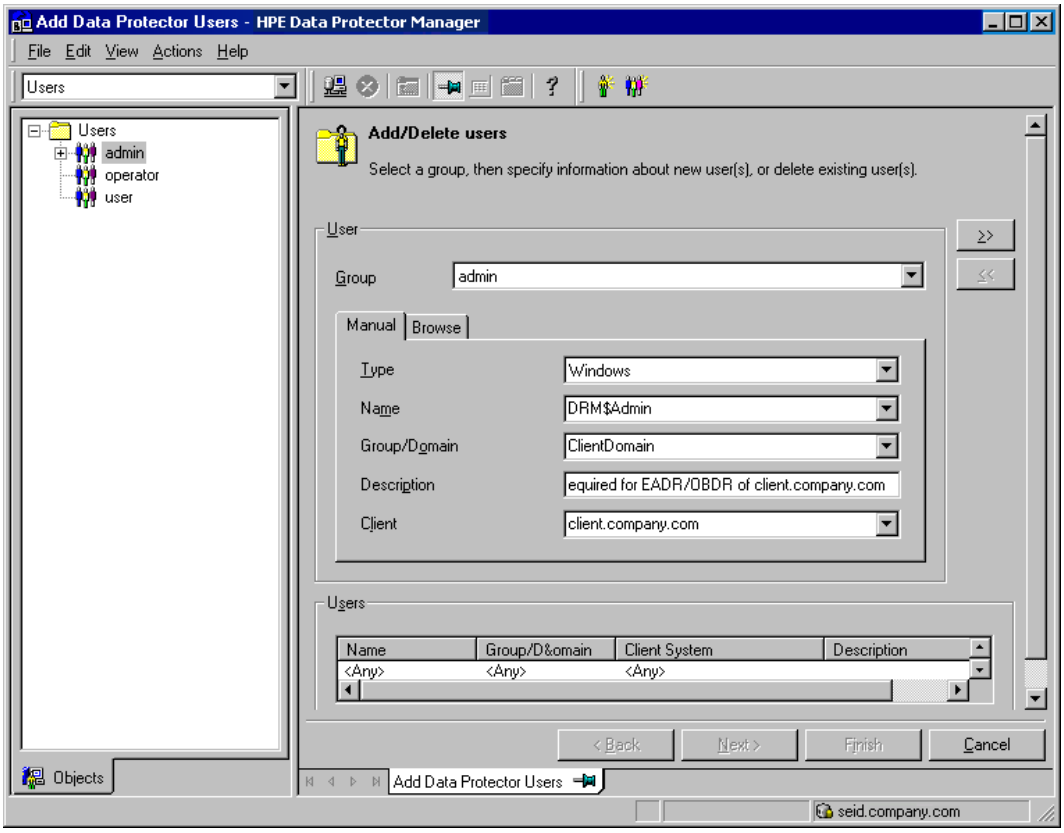
     一時ホスト名は、Windows Preinstallation Environment (WinPE)によってシステムに割り当てられます。WinPEのコマンドプロンプトウィンドウで`hostname`コマンドを実行することによって、ホスト名を取得できます。

   Windows XP、Windows Server 2003の場合:

   - 種類:`Windows`
   - 名前:`DRM$Admin`
   - グループ/ドメイン: ターゲットシステムのホスト名
   - クライアント: ターゲットシステムの完全修飾ドメイン名 (FQDN)

ユーザーの追加方法の詳細については、『HPE Data Protectorヘルプ』のキーワード「追加、Data Protectorユーザー」で表示される内容を参照してください。

ユーザーアカウントの追加



2. イメージファイルとバックアップデータが格納されたテープをOBDRデバイスに挿入します。
3. ターゲットシステムをシャットダウンし、テープデバイスの電源を切ります。復旧手順を開始する前に、システムに外付けのUSBディスク(USBキーを含む)が接続されていないことを確認してください。
4. ターゲットシステムの電源を入れます。ターゲットシステムが初期化されている間に、テープデバイス上の**取り出し**ボタンを押してテープデバイスの電源を入れます。詳細については、デバイスのドキュメントを参照してください。
5. 復旧の対象範囲と復旧オプションを選択します。次の手順は、オペレーションシステムによって異なります。

   Windows Vista以降のリリースの場合:

   a. ディザスタリカバリGUI(インストーラーウィザード)が起動し、オリジナルシステムの情報が表示されます。**[次へ]**をクリックします。

   > **ヒント:**
   > プログレスバーが表示されたときに利用可能になるキーボードオプションがあります。プログレスバーにカーソルを移動すると、利用可能になるオプションとそれらのオプションについての説明を確認できます。

   b. [復旧の対象範囲]ページで、復旧の対象範囲を選択します。

      - `Default Recovery`:重要なボリューム(システムディスク、ブートディスク、およびData Protectorインストールボリューム)が復旧されます。それ以外のすべてのディスクは、パーティ

ション化されてフォーマットされ、段階3のために空のままになります。

- Minimal Recovery:システムディスクおよびブートディスクのみが復旧されます。
- Full Recovery:重要なボリュームだけでなく、復元セット内のすべてのボリュームが復元されます。
- Full with Shared Volumes:Microsoft Cluster Server (MSCS)の場合に選択できるオプションです。MSCS内のすべてのノードが障害の影響を受けた場合、最初のノードのEADRを実行するときにこのオプションを選択する必要があります。復元セットに含まれているボリュームがすべて復旧されます。バックアップ時にバックアップ対象のノードでロックされていたクラスター共有ボリュームもこれに含まれます。1つ以上のノードが機能しており、MSCSサービスが稼動している場合、共有ボリュームはアクティブノードによってロックされているため、復元されません。この場合はDefault Recoveryを選択してください。

c. 必要に応じて、復旧設定を変更するには、**[設定]**をクリックして[復旧設定]ページを開きます。

次の追加の復旧オプションが使用できます。オプションによっては、ディザスタリカバリが完全に終了しない場合や、追加手順が必要な場合に使用するものもあります。

- Use original network settings:元のネットワーク構成の復元が必要な場合(DHCPサーバーが見つからない場合など)、このオプションを選択してください。デフォルトで、このオプションは選択されていません。DR OSリカバリ環境はDHCPネットワーク構成を使用します。
- Restore BCD:このオプションを選択すると、Boot Configuration Data (BCD)ストアも、Data Protector復元セッションで復元される前のディザスタリカバリセッションの際にData Protectorによって復元されます。このオプションは、デフォルトで選択されています。
- Restore DAT:このオプションを選択すると、Data Protectorディザスタリカバリモジュールは Microsoft VSSライターのデータも復元します。デフォルトでは、DRモジュールはVSSライターのデータの復元をスキップします。VSS以外のバックアップ中にData Protectorがクリティカルライターのバックアップに失敗する場合、このオプションを使用してください。DRモジュールの復元前にデータを復元するには、Preを選択します。Data Protectorの後にデータを復元するには、Postを選択します。
- Initialize Disks Manually:このオプションでは、元のシステムディスクと現在のシステムディスクを手動でマップして、それらを初期化して元の構成に一致させることができます。デフォルトではこのオプションは選択されていません。

  このオプションを選択すると、復旧プロセスを開始したときに新しいディスクのマッピングと初期化ページが表示されます。ディザスタリカバリモジュールにより、最初のディスクマッピングが実行され、マッピングの試行結果が表示されます。ディスクマッピングを変更するには提供されているオプションを使用します。マッピングが完了すると、ボリュームが初期化され、システムが再起動されます。
- Restore Storage Spaces:デフォルトでは、ストーレジスペースが復元されます。ストレージ構成によって可能であれば、復旧時にこのオプションの選択を解除して、仮想ディスクを直接物理ディスクに復元できます。ストレージスペースを異なるハードウェアまたはUSBディスクに復元する場合ディスクを手動で初期化する必要があるので、注意してください。
- Enable Dissimilar Hardware Restore:このオプションを有効にすると、Data Protectorは復旧中にシステムをスキャンして、見つからないドライバーを検索します。このオプションを有効にするには、ドロップダウンリストから次のいずれかの方法を選択します。
  - Unattend(デフォルト):このモードは、定義済みの構成ファイルを使用して各種のハードウェアプラットフォームに対してオペレーティングシステムを自動的に構成します。これは、異なるハードウェアでの復旧のプライマリモードです。最初のインスタンスではこのモードを使用してください。

  - Generic:無人モードが失敗した場合(復元したオペレーティングシステムの誤った構成が原因である可能性が高い)、このオプションを選択します。これは、異なるハードウェアに対する、復元されたOSレジストリ、およびOSのドライバーとサービスの適用に基づきます。
- Remove Devices:このオプションを使用できるのは、Dissimilar Hardwareオプションが有効な場合です。このオプションを選択すると、Data Protectorは、復元したオペレーティングシステムのレジストリからオリジナルのデバイスを削除します。
- Connect iSCSI Devices:このオプションは、元のマシンがiSCSIを使用していた場合に有効になり、選択されます。このオプションを選択すると、Data Protectorはバックアップ時点のiSCSIの基本構成を自動的に復元します。このオプションを選択しないと、iSCSI構成はスキップされます。

  ネイティブのMicrosoft iSCSI構成ウィザードを使用して、より複雑なiSCSI構成を管理することもできます。DR GUIによって手動構成を必要とするiSCSI機能(セキュリティオプションなど)が検出されると、Microsoft iSCSI構成ウィザードを実行するためのオプションが表示されます。
- Map Cluster Disks Manually:Windows Server 2008以降のリリースで使用可能です。選択すると、クラスターボリュームを手動でマップできます。選択しないと、ボリュームは自動的にマップされます。自動マッピング後にすべてのボリュームが適切にマップされているかどうかを確認することをお勧めします。
- Remove Boot Descriptor:Intel Itaniumシステムで使用可能です。ディザスタリカバリプロセス後に残ったすべての起動記述子を削除します。
- Manual disk selection:Intel Itaniumシステムで使用可能です。ディスク設定が大幅に変更された場合、ディザスタリカバリモジュールはブートディスクを見つけることができなくなる可能性があります。このオプションは、正しいブートディスクを選択するために使用します。

これらのオプションをデフォルト設定に戻るには、**[デフォルト設定を元に戻す]**をクリックします。

[保存]をクリックして、変更内容を保存します。

d. 復旧プロセスが開始され、このプロセスの進行状況を監視できます。

BitLockerドライブ暗号化を使用してボリュームが暗号化されている場合、暗号化されたドライブのロックを解除することを促すメッセージが表示されます。

> **ヒント:**
> ディザスタリカバリGUIで**[タスク]**をクリックすると、以下を実行できます。
> - コマンドプロンプト、タスクマネージャー、またはディスクアドミニストレーターの実行
> - Map Network DrivesおよびLoad Driversツールへのアクセス
> - ディザスタリカバリプロセス固有のログファイルの表示
> - DRM構成ファイルの有効化または無効化、このファイルのテキストエディターでの表示、このファイルの編集
> - WinPE復旧環境のホストファイルの編集
> - ヘルプへのアクセスと、GUIアイコンの凡例の表示

Windows XP、Windows Server 2003の場合:

a. 以下のメッセージが表示されたら、**F12**を押します。`To start recovery of the machine HOSTNAME press F12`

b. ブートプロセスの開始時に範囲選択メニューが表示されます。復元の対象範囲を選択し、**Enter**を押します。5つの異なる復元対象範囲があります。

- `Reboot`:ディザスタリカバリは実行されず、システムが再起動されます。
- `Default Recovery`:重要なボリューム(システムディスク、ブートディスク、および`OBInstall`ボリューム)が復旧されます。それ以外のすべてのディスクは、パーティション化されてフォーマットされ、段階3のために空のままになります。
- `Minimal Recovery`:システムディスクおよびブートディスクのみが復旧されます。
- `Full Recovery`:重要なボリュームだけでなく、復元セット内のすべてのボリュームが復元されます。
- `Full with Shared Volumes`:Microsoft Cluster Server (MSCS)の場合に選択できるオプションです。MSCS内のすべてのノードが障害発生によって影響を受けると、最初のノードのOBDRを実行する場合に、このオプションを選択する必要があります。復元セットに含まれているボリュームがすべて復旧されます。バックアップ時にバックアップ対象のノードでロックされていたクラスター共有ボリュームもこれに含まれます。1つ以上のノードが機能しており、MSCSサービスが稼動している場合、共有ボリュームはアクティブノードによってロックされているため、復元されません。この場合は`Default Recovery`を選択してください。

次の追加の復旧オプションが使用できます。オプションによっては、ディザスタリカバリが完全に終了しない場合や、追加手順が必要な場合に使用するものもあります。

- `Remove Boot Descriptor`:Intel Itaniumシステムで使用可能です。ディザスタリカバリプロセス後に残ったすべての起動記述子を削除します。
- `Manual disk selection`:Intel Itaniumシステムで使用可能です。ディスク設定が大幅に変更された場合、ディザスタリカバリモジュールはブートディスクを見つけることができなくなる可能性があります。このオプションは、正しいブートディスクを選択するために使用します。

段階2

6. 復旧の対象範囲を選択すると、Data Protectorはハードディスクに対して直接DR OSのセットアップを開始します。この処理の進行状況はモニター可能です。DR OSのセットアップが完了するとシステムは再起動します。DR OSが正常にブートしない場合、またはネットワークにアクセスできない場合は、kb.cfgファイルを編集する必要があります。Windows Vista以降のリリースでは、DR OSはインストールされず、システムの再起動は行われません。
7. ディザスタリカバリバックアップが暗号化され、Cell Managerにアクセスできないクライアントを復元している場合、以下のプロンプトが表示されます。

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   [y]キーを押します。

   クライアントでキーストア(`DR-ClientName-keys.csv`)が使用できるようにします(たとえば、CD-ROM、フロッピーディスク、またはUSBフラッシュドライブを挿入します)。その後、キーストアファイルへのフルパスを入力します。キーストアファイルは、DR OSのデフォルトの場所にコピーされ、Disk Agentによって使用されます。以降は何の操作も必要なく、ディザスタリカバリが続行されます。
8. SRDファイル内の情報が最新でない場合(たとえば、障害後にバックアップデバイスを変更したなどの場合)、オフライン復旧を実行するには、この手順を続行する前にSRDファイルを編集します。
9. 選択した復旧対象範囲内で以前の記憶域構造が再確立され、重要なボリュームがすべて復元されます。一時的なDR OSは、最初のログイン後に自動的に削除されます。ただし、以下の場合は例外です。

- `Minimal Recovery`が選択されている。
- ディザスタリカバリウィザードがDRのインストールとバックアップメディア上のSRDファイルを発見した後、10秒以内にウィザードを中断し、**[Debugs]**オプションを選択した場合。
- `omnidr`コマンドを`-no_reset`オプションまたは`-debug`オプションを指定して手動で実行した場合。
- ディザスタリカバリが失敗した場合。

Data Protectorは、最初にオンライン復旧を実行しようとします。Cell Managerまたはネットワークサービスが使用できない、あるいはファイアウォールによりCell Managerへのアクセスが拒否されるなどの理由でオンライン復旧が失敗すると、Data Protectorによってリモートオフライン復旧が試みられます。Media Agentホストが Cell Managerからの要求しか受け付けないなどの理由でリモートオフライン復元にも失敗すると、ローカルオフライン復元が実行されます。

10. 手順1で作成したクライアントのローカルアカウントをCell ManagerのData Protector `admin`ユーザーグループから削除します(ディザスタリカバリ前にそのアカウントがCell Manager上に存在していた場合を除く)。

段階3

12. Data Protectorの標準復元手順でユーザーデータとアプリケーションデータを復元します。

> **注:**
> Data Protectorでは、復旧後にボリューム圧縮フラグが復元されません。バックアップ時に圧縮されていたファイルは、すべて圧縮状態で復元されますが、今後のファイルについても必ず圧縮したい場合は、ボリューム圧縮を手動で設定する必要があります。

13. Microsoft Cluster Serverですべてのノードのディザスタリカバリを実行する場合は、追加作業が必要になります。

拡張タスク

Microsoft Cluster Serverのディザスタリカバリ

Microsoft Cluster Serverのディザスタリカバリについて

Microsoft Cluster Server (MSCS)の復旧には、ディスクデリバリーによるディザスタリカバリ以外の任意のディザスタリカバリ方法を使用できます。特定のディザスタリカバリ方法に関する固有事項、制限、および必要条件は、MSCSのディザスタリカバリにも当てはまります。実際のクラスターに適したディザスタリカバリ方法を選定し、ディザスタリカバリ計画に含めてください。どの方法を使用するかを決定する前に、それぞれのディザスタリカバリ方法の制限と必要条件を十分に検討し、テスト計画に基づいてテストを実施してください。

サポートされているオペレーティングシステムの詳細は、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。

MSCSを復旧するには、ディザスタリカバリのすべての前提条件(整合性がある最新のバックアップ、更新されたSRDファイル、故障したハードウェアの交換など)を満足する必要があります。

考えられるシナリオ

MSCSのディザスタリカバリに関しては、2通りのシナリオが考えられます。

- クラスター内の単一または一部の非アクティブノードに障害が発生した場合
- クラスター内のすべてのノードに障害が発生した場合

Microsoft Cluster Serverのディザスタリカバリの準備

Microsoft Cluster Server (MSCS)を復旧するには、ディザスタリカバリのすべての前提条件(整合性がある最新のバックアップイメージ、更新されたSRDファイル、故障したハードウェアの交換など)を満たす必要があります。特定のディザスタリカバリ方法に関する固有事項、制限、および必要条件は、MSCSのディザスタリカバリにも当てはまります。

MSCSの整合性のあるバックアップイメージを次に示します。

- すべてのノード
- 仮想サーバー
- Data Protectorがクラスター対応アプリケーションとして構成されている場合は、Cell Managerがバックアップ仕様に含まれる必要があります。

EADRの固有事項

バックアップ時に他のノードによってロックされる共有ディスクボリュームに関しては、段階1でディスクの構成に十分な情報を収集するのは事実上不可能です。ただし、すべての共有クラスターボリュームの復元を可能にするには、この情報が必要です。クラスター内のすべてのノードのP1Sファイルに共有クラスターボリュームに関する情報を含めるには、以下のいずれかを実行します。

- フルクライアントバックアップの実行後に、クラスター内のすべてのノードのP1Sファイルに含まれている共有クラスターボリューム情報をマージして、各ノードのP1Sファイルに共有クラスターボリューム構成に関する情報を含めます。
- バックアップ対象のノードにすべての共有クラスターボリュームを一時的に移動しておきます。これによって、すべての共有クラスターボリュームに関する必要情報を収集できるようになりますが、そのノードだけをプライマリノードとして使用できます。

OBDRの固有事項

実行後コマンドとして`omnisrdupdate`コマンドを使用し、OBDRバックアップの実行後にSRDファイルを更新すると、復元を高速化できます。OBDRの実行時、更新したSRDファイルを書き込んだフロッピーディスクをフロッピーディスクドライブに挿入し、テープ上のバックアップオブジェクトの位置をData Protectorに認識させます。これにより、Data Protectorがテープ上のMSCSデータベースの位置を検索しなくなるので、MSCSデータベースの復元が高速化されます。

OBDRブートテープを準備するノードにすべてのボリュームを一時的に移動すると、MSCS内のすべての共有ディスクボリュームを自動的に復元できるようになります。バックアップ時にほかのノードによってロックされる共有ディスクボリュームに関しては、段階1でディスクの構成に十分な情報を収集するのは不可能です。

Microsoft Cluster Serverを復旧する

Microsoft Cluster Server (MSCS)のディザスタリカバリに関しては、2通りのシナリオが考えられます。

クラスター内にまだ稼動しているノードが1つ以上ある場合

クラスター内のすべてのノードに障害が発生した場合

クラスター内にまだ稼動しているノードが1つ以上ある場合

MSCSのディザスタリカバリでは、これが基本的なシナリオになります。ディザスタリカバリの他の前提条件に加え、以下の前提条件も満たされている必要があります。

前提条件

- 少なくとも1つのクラスターノードが正常に機能していること(アクティブノード)
- そのノード上でクラスターサービスが実行されていること
- すべての物理ディスクリソースがオンラインになっていること(つまり、クラスターによって所有されていること)
- 通常のクラスター機能がすべて使用可能であること(クラスター管理グループがオンラインになっていること)
- Cell Managerがオンラインであること

この場合、クラスターノードのディザスタリカバリはData Protectorクライアントのディザスタリカバリと同じです。影響があった非アクティブノードの復元にどのディザスタリカバリ方法を使用するかに応じて、適切な手順を実施してください。

障害が発生すると、共有ディスクはすべてアクティブノードに移動され、ロックされます。したがって、復元されるのはローカルディスクだけです。

復旧が完了したセカンダリノードは、ブート後にクラスターに追加されます。

すべてのノードの復旧が完了し、それらをクラスターに追加し終えたら、統一性を確保するためにMSCSデータベースを復元することができます。MSCSデータベースは、WindowsシステムのCONFIGURATIONオブジェクトの一部です。

クラスター内のすべてのノードに障害が発生した場合

MSCS内のすべてのノードが使用不能で、クラスターサービスが稼動していない場合が、このシナリオに該当します。

ディザスタリカバリの他の前提条件に加え、以下の前提条件も満たされている必要があります。

前提条件

- プライマリノードからクォーラムディスクへの書き込みアクセスが可能であること(クォーラムディスクがロックされていないこと)
- Cell Managerを復旧するとき、プライマリノードからすべてのIDBボリュームにアクセスできること

この場合は、最初にクォーラムディスクを復元した後、プライマリノードを復元する必要があります。クラスター内にCell Managerがインストールされているのであれば、IDBも復元する必要があります。必要に応

じて、MSCSデータベースを復元することもできます。プライマリノードの復元が完了したら、ほかのノードを復元できます。

AMDRの場合、MSCSサービスは、すべてのハードディスクのMBRに書き込まれているハードディスク署名を使用して物理ディスクを識別します。共有クラスターディスクを交換した場合は、ディザスタリカバリの段階1が終了します。MSCS Service側では、交換したディスクが有効なクラスターリソースとして認識できなくなり、それらのリソースに依存しているクラスターグループが機能しなくなります。これを防ぐには、共有クラスターディスクを交換した場合は、オリジナルのハードディスク署名を復元します。

手順

1. クォーラムディスクを含めて、プライマリノードのディザスタリカバリを実行します。

   半自動ディザスタリカバリ(AMDR):

   クォーラムディスク上のすべてのユーザーデータとアプリケーションデータが、`drstart -full_clus`コマンドによって自動的に復元されます。

   拡張自動ディザスタリカバリ(EADR)とワンボタンディザスタリカバリ(OBDR):

   復旧の対象範囲を確認するように促すダイアログが表示されたら、**[共有ボリュームを含む完全復旧]**を選択して、クォーラムディスクを復元します。
2. システムを再起動します。
3. WindowsシステムのCONFIGURATIONオブジェクトの一部であるMSCSデータベースを復元します。MSCSデータベースを復旧できるようにするには、MSCSサービスが実行中である必要があります。したがって、ディザスタリカバリの段階2では自動的には復旧されません。しかし、段階2の最後にData Protectorの標準復元手順を使用すると、クラスターデータベースを手動で復旧できます。
4. **ワンボタンディザスタリカバリ(OBDR)以外の方法:**

   Cell Managerを復旧する場合は、IDBの整合性を確保します。
5. クォーラムボリュームおよびIDBボリュームが復元されます。その他のボリュームは、復元処理の対象外となり、復旧したプライマリノードが破損していなければ、プライマリノードによって再使用されます。復旧したプライマリノードが破損している場合は、以下の手順に従ってください。
   a. クラスターサービスとクラスターディスクドライバーを無効化します。詳細については、MSDN Q176970を参照してください。
   b. システムを再起動します。
   c. 以前の記憶域構造を再確立します。
   d. クラスターディスクドライバーとクラスターサービスを有効化します。
   e. システムを再起動し、ユーザーデータおよびアプリケーションデータを復元します。
6. ほかのノードを復元します。

Microsoft Cluster Server用のP1Sファイルをマージする

拡張自動ディザスタリカバリ(EADR)でアクティブノードを復元するには、バックアップの実行後に特別な作業が必要になります。Microsoft Cluster Server (MSCS)のすべてのノードに対するP1Sファイル内の共有クラスターボリュームの情報をマージして、各ノードのP1Sファイルに共有クラスターボリューム構成に関する情報を含める必要があります。すべての共有クラスターボリュームの復元を可能にするには、P1Sファイルのマージが必要となります。バックアップ対象のノードにすべての共有クラスターボリュームを一時的に移動しておくと、バックアップ後のP1Sファイルのマージを回避できます。この場合は、すべての共有クラスター

ボリュームに関する必要なすべての情報が収集されます。これによって、そのノードのみがプライマリノードになることができます。

Windows

すべてのノードのP1Sファイルをマージするには、*Data_Protector_home*\bin\drim\binディレクトリからmerge.exeコマンドを実行します。

```
merge p1sA_path ... p1sX_path
```

ここで、p1sAは最初のノードのP1Sファイルのフルパス、p1sXはMSCS内の最後のノードのP1Sファイルのフルパスです。

更新したP1Sファイルのファイル名の末尾には、.mergedが付加されます(例: computer.company.com.merged)。マージしたP1Sファイルの名前を元の名前に戻しておきます(.merged拡張子を削除します)。

たとえば、2つのノードからなるMSCSのP1Sファイルをマージするには、以下のように入力します。

```
merge Data_Protector_program_data\Config\server\dr\p1s\node1.company.com Data_
Protector_program_data\Config\server\dr\p1s\node2.company.com.
```

マージしたファイルの名前は、node1.company.com.mergedとnode2.company.com.mergedになります。

UNIX

merge.exeコマンドは、Data Protector自動ディザスタリカバリコンポーネントがインストールされているWindowsシステムでのみ動作します。UNIX Cell Managerの場合は、次の手順に従ってください。

手順

1. 自動ディザスタリカバリコンポーネントがインストールされているWindowsクライアントにP1Sファイルをコピーします。
2. ファイルをマージします。
3. マージしたP1Sファイルを元の名前に戻します。
4. マージしたP1SファイルをUNIX Cell Managerにコピーします。

Windowsシステム上でオリジナルのハードディスク署名を復元する

Microsoft Cluster Server(MSCS)サービスでは、各ハードディスクのMBR内に書き込まれたハードディスク署名を使用して物理ディスクを識別します。共有クラスターディスクを交換した場合は、ディザスタリカバリの段階1が終了します。クラスターサービス側では、交換したディスクが有効なクラスターリソースとして認識できなくなり、それらのリソースに依存しているクラスターグループが機能しなくなります。少なくとも1つのノードが稼動しており、リソースの所有権を保持していれば、共有クラスターリソースは稼動状態にあるからです。また、EADR/OBDRではクリティカルディスクの元のディスク署名が自動的に復旧されるため、この問題はEADRとOBDRのクリティカルディスクには当てはまりません。その他のディスクを交換した場合は、それらのディスクのハードディスク署名も復元する必要があります。

最も重要な共有ディスクは、クラスターのクォーラムリソースです。クォーラムディスクを交換した場合は、オリジナルのディスク署名を復元しないと、クラスターサービスを起動できません。段階2では、MSCSデータ

ベースはシステムボリュームの\TEMP\ClusterDatabaseディレクトリに復元されます。この場合、段階1でハードディスク署名が変更されているため、クォーラムリソースが認識されません。したがって、システムの再ブート後にクラスターサービスが起動されません。

Windows上でオリジナルのハードディスク署名を復元する

Windowsシステムでは、*Data_Protector_home*\bin\utilnsにあるclubarユーティリティを実行すると、オリジナルのハードディスク署名が復元されるので、クラスターサービスが起動しないという問題を解決できます。clubarの実行が正常に完了すると、クラスターサービスが自動的に起動されます。

たとえば、C:\temp\ClusterDatabaseからMSCSデータベースを復元するには、コマンドプロンプトに次のように入力します。

```
clubar r C:\temp\ClusterDatabase force q:.
```

clubarの使用方法と構文の詳細については、*Data_Protector_home*\bin\utilnsにあるclubar.txtファイルを参照してください。

Cell ManagerのData Protector共有ディスクがクォーラムディスクと異なる場合、同様に復元する必要があります。Data Protector共有ディスクおよびその他のアプリケーションディスクの署名を復元するには、Windowsリソースキットに用意されているdumpcfgユーティリティを使用します。dumpcfgの使用についての詳細を調べるには、dumpcfg /?を実行するか、Windowsリソースキットのドキュメントを参照してください。Windowsシステム上のハードディスク署名に関する問題の詳細については、MSDNの文書番号Q280425を参照してください。

オリジナルのハードディスク署名を取得する

SRDファイルからオリジナルのハードディスク署名を取得できます。SRDファイル内では、先頭に-volumeキーワードが付いた番号としてハードディスク署名が示されます。

クォーラムディスクは、アクティブノードによってロックされ、ほかのノードからアクセスできません。このため、クォーラムディスクの署名は、アクティブノードのSRDファイルにのみ(バックアップ時に)書き込まれます。共有ディスクボリュームに対する段階1では、すべてのSRDファイルを組み合わせることによってのみ、ディスクの構成に十分な情報を取得できます。つまり、クラスター内のすべてのノードのSRDファイルが必要になります。したがって、常にクラスター全体をバックアップしておくことをお勧めします。なお、SRDファイル内ではハードディスク署名が10進値として表されるのに対し、dumpcfgには16進値を渡す必要があります。

SRDファイル内のハードディスク署名の例

SRDファイルからオリジナルのハードディスク署名を取得できます。SRDファイル内では、先頭に-volumeキーワードが付いた番号としてハードディスク署名が示されます。SRDファイル内のハードディスク署名の例を以下に示します。

```
-volume 5666415943 -number 0 -letter C -offslow 32256 -offshigh 0 -lenlow 320430592
-lenhigh 2 -fttype 4 -ftgroup 0 -ftmember 0
```

```
-volume 3927615943 -number 0 -letter Q -offslow 320495104 -offshigh 2 -lenlow
1339236864 -lenhigh 0 -fttype 4 -ftgroup 0 -ftmember 0
```

先頭に-volumeキーワードが付いた番号がハードディスク署名です。この例では、ローカルハードディスク(ドライブ文字Cとクォーラムディスク(ドライブ文字Q)の署名がSRDファイルに含まれています。

Data Protector Cell Manager固有の情報の復元

この項では、Windows Cell Managerの復元に必要な、特別な手順を説明します。

IDBの整合性をとる(すべての復旧方法)

この項に記載されている手順は、一般的なディザスタリカバリ手順の実行後にのみ使用します。

IDBの整合性をとるには、最新のバックアップがあるメディアをインポートして、バックアップされたオブジェクトの情報をIDBにインポートします。これを行うには以下の手順を実行してください。

1. 復元対象として残っているボリュームのバックアップが保存されたメディア(1つ以上)をData Protector GUIを使ってリサイクルして、IDBへメディアをインポートできるようにします。詳細については、『HPE Data Protectorヘルプ』のキーワード「メディアのリサイクル」で表示される内容を参照してください。

   メディアがData Protectorによってロックされているためにリサイクルできない場合があります。このような場合には、プロセスを中止し、以下のコマンドを実行して\tmpディレクトリを削除します。

   a. `omnisv -stop`
   b. `del Data_Protector_program_data\tmp\*.*`
   c. `omnisv -start`
2. 復元対象として残っているボリュームのバックアップが保存されたメディア(1つ以上)をData Protector GUIを使ってエクスポートします。詳細については、『HPE Data Protectorヘルプ』のキーワード「エクスポート、メディア」で表示される内容を参照してください。
3. 復元対象として残っているパーティションのバックアップが保存されたメディア(1つ以上)をData Protector GUIを使ってインポートします。詳細については、『HPE Data Protectorヘルプ』のキーワード「インポート、メディア」で表示される内容を参照してください。

拡張自動ディザスタリカバリに固有の手順

拡張自動ディザスタリカバリを使用して、Windows Cell Managerを復元する場合には、段階0で2つの特別な手順が必要です。

- ディザスタリカバリCD、またはCell ManagerのDR OSイメージを格納しているUSBドライブ、またはCell Managerのネットワークブート可能イメージをあらかじめ準備する必要があります。

  > **重要:**
  > ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行して新しいDR OSイメージを作成します。これは、IPアドレスやDNSサーバーの変更など、ネットワーク構成が変更された場合も同じです。

- ディザスタリカバリの準備作業の一環として、Cell Managerの更新済みのSRDファイルは、IDB以外の場所にも保存しておく必要があります。なぜなら、SRDファイルはData Protectorで唯一、オブジェクトとメディアに関する情報が保存されているファイルだからです。SRDファイルをCell Managerだけにしか保存していないと、Cell Managerに障害が発生した場合に利用できなくなります。「準備」(ページ27)を参照してください。
- バックアップが暗号化されている場合は、障害が発生する前に暗号化キーをリムーバブルメディアに保存しておく必要があります。暗号化キーをCell Managerだけにしか保存していないと、Cell Managerに

障害が発生した場合に利用できなくなります。暗号化キーが使用できないと、ディザスタリカバリは実行できなくなります。「準備」(ページ27)を参照してください。

> **重要:**
> バックアップメディア、リカバリセットファイル、SRDファイル、暗号化キーが保存されたリムーバブルメディア、ディザスタリカバリCD、DR OSデータを格納しているUSBドライブへのアクセスを制限しておくことをお勧めします。

Internet Information Serverを復旧する

Internet Information Server (IIS)では、ディザスタリカバリがサポートされていません。IISを復旧するには、半自動ディザスタリカバリの要件に加え、以下の要件が満たされていなければなりません。

要件

- システムのクリーンインストール中にIISをインストールしないこと。

半自動ディザスタリカバリの手順に加え、以下の手順に従ってください。

手順

1. IIS管理サービスを停止またはアンインストールします(現在稼動している場合)。
2. `drstart`コマンドを実行します。

デフォルトのIISパス(*%SystemRoot%*\system32\inetsrv)に、IISデータベースが`DisasterRecovery`というファイル名のプレーンファイルとして復元されます。

ブートが正常に完了したら、Data Protectorの標準復元手順に従うか、またはIISバックアップ/復元スナップインを使用してIISデータベースを復元します。なお、この復元には多少時間がかかります。

kb.cfgファイルの編集

`kb.cfg`ファイルは*Data_Protector_home*\bin\drim\configディレクトリに格納されています。このファイルには、*%SystemRoot%*ディレクトリのドライバーファイルの場所に関する情報が保存されます。このファイルの目的は、特定のブート関連ハードウェアまたはアプリケーション構成を持つシステム用に、ドライバー(および他の必要ファイル)をData Protector DR OSに含めるための柔軟な方法を提供することです。デフォルトの`kb.cfg`ファイルには、あらかじめ業界標準のハードウェア構成に必要なすべてのファイルが含まれています。

たとえば、ドライバーの機能が複数のファイルに分割されていることがありますが、ドライバーを正常に動作させるには、すべてのファイルが必要です。すべてのドライバーファイルが`kb.cfg`ファイルに含まれていない場合は、Data Protectorがすべてのドライバーファイルを識別できないことがあります。その場合、それらのファイルはDR OSに追加されません。デフォルトの`kb.cfg`ファイルを使用したテストプランを作成し実行します。DR OSが正常にブートされない場合、またはネットワークにアクセスできない場合は、ファイルを変更する必要があることがあります。

これらのドライバーをバックアップする場合は、依存ファイルに関する情報を`kb.cfg`ファイルの先頭に記載されている形式で`kb.cfg`ファイルに追加します。既存の行をコピーして貼り付けてから関連する情報で置き換えると、このファイルを簡単に編集できます。

パスの区切り文字は"/"(スラッシュ)です。スペースは、引用符で囲まれたパス名に含まれる場合を除いて無視されるため、関連するエントリを複数行にまたがらせることも可能です。"#"(シャープ)記号で始まるコメント行を追加することもできます。

kb.cfgファイルの編集が終了したら、元の場所に保存します。次に、追加したファイルをリカバリセットに含めるために、フルクライアントバックアップを再度実行します。

重要:
システムのハードウェアやアプリケーションの構成はさまざまであるため、すべての構成に対して「出来合い」の解決法を提供することはできません。したがって、作業者自身の責任でこのファイルを変更して、ドライバーやその他のファイルを追加してください。

このファイルの変更は作業者自身の責任で行うことになっており、HPEではサポートしておりません。

注意:
kb.cfgファイルの編集後にディザスタリカバリが正常動作するかを確認するため、テストプランを作成して実行することをお勧めします。

SRDファイルを編集する

バックアップデバイスまたはメディアに関する情報(更新されたSRDファイル(recovery.srd)に格納されている)は、ディザスタリカバリを実行する時点では古くなっている可能性があります。オンライン復旧を実行する場合には、必要な情報がIDB (Cell Manager上)に保存されているため、これは問題となりません。しかし、オフライン復旧を実行している場合は、IDBに格納された情報にはアクセスできません。

たとえば、障害は、Cell Managerだけでなく、Cell Managerに接続されているバックアップデバイスにも発生します。障害発生後にバックアップデバイスを別のバックアップデバイスに交換した場合、SRDファイルに格納されている情報が正しくないため、復旧が失敗します。この場合は、段階2を実行する前に更新済みのSRDファイルを編集して、正常な復旧ができるように正しくない情報を更新します。

SRDファイルを編集するには、テキストエディターでSRDファイルを開き、変更されている情報を更新します(SRDファイルの場所については、以下の方法を参照してください)。

ヒント:
デバイス構成に関する情報を表示するには、devbra -devコマンドを使います。

たとえば、ターゲットシステムのクライアント名が変更されている場合は-hostオプションの値を修正します。以下に関する情報も編集できます。

- Cell Managerクライアント名(-cm)
- Media Agentクライアント(-mahost)
- デバイス名(-dev)
- デバイスの種類(-type)
- アドレス(-devaddr)
- ポリシー(-devpolicy)
- ロボティクスのSCSIアドレス(-devioctl)
- ライブラリスロット(-physloc)、その他

ファイルを編集し終えたら、元の場所にUnicode(UTF-16)形式で保存します。

編集したSRDファイルをディザスタリカバリに使用する手順は、ディザスタリカバリ方法やオペレーティングシステムによって異なります。以下で、特定のディザスタリカバリ方法の詳細について説明します。

> **重要:**
> SRDファイルへのアクセスは、セキュリティ維持のため制限しておく必要があります。

AMDR

EADR/OBDR

AMDR

SRDファイル内の情報が古い場合は、通常のAMDRリカバリ手順を実行する前に、以下の作業を行います。

手順

1. テキストエディターで(1枚目の`drsetup`/ASRフロッピーディスク上の)`recovery.srd`ファイルを開き、必要な変更を行います。
2. ファイルを元の場所にUnicode(UTF-16)形式で保存します。

EADR/OBDR

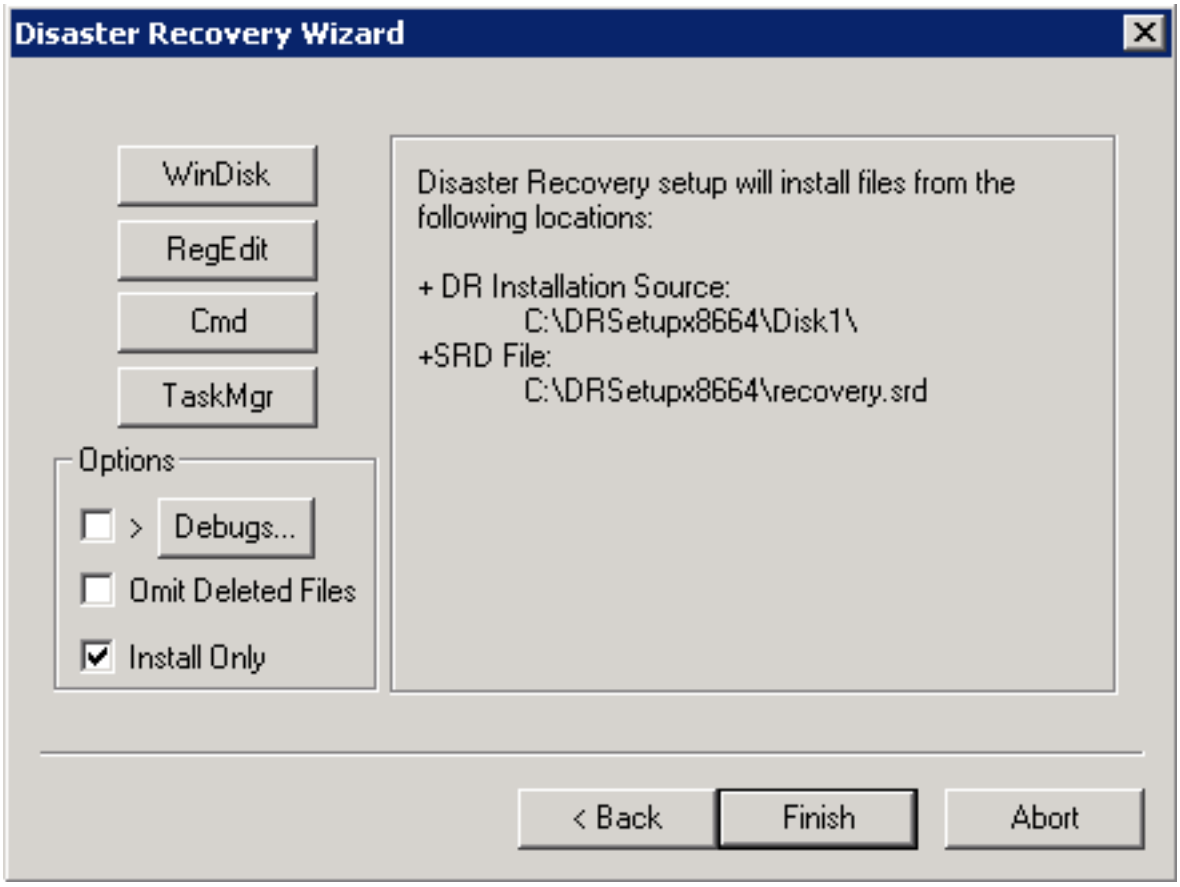
SRDファイル内の情報が古い場合は、通常のEADR/OBDR手順を開始する前に、以下の追加作業を行います。

手順

Windowsシステム

1. ディザスタリカバリウィザードが表示されたら、カウントダウン中にいずれかのキーを押してウィザードを停止し、**[Install only]**オプションを選択して、`[Finish]`をクリックします。このオプションを選択すると、対象のシステムに一時オペレーティングシステムのみがインストールされて、ディザスタリカバリの段階1を完了できます。ディザスタリカバリの段階2は、**[Install only]**オプションを選択した場合は自動的に開始されません。

   ディザスタリカバリウィザードのInstall Onlyオプション



2. **[削除済みファイルを除外]**オプションを選択します。このオプションを使用すると、連続する増分バックアップの間で削除されたファイルを復元時に除外できます。このオプションを指定すると、増分バックアップの場合、`omnidr` バイナリは同じオプションをData Protector復元ツール(`omnir` および `omniofflr`)に送ります。このオプションは、フルバックアップオブジェクトバージョンの復元には影響しません。ただし、このオプションを選択すると、復元時間が大幅に長くなる可能性があります。
3. **Windowsタスクマネージャー**を実行します(**Ctrl+Alt+Del**を押し、**[タスクマネージャー]**を選択します)。
4. Windowsタスクマネージャーで、**[ファイル]**をクリックし、**[新しいタスクの実行]**をクリックします。
5. [ファイル名を指定して実行]ダイアログから次のコマンドを実行します。`notepad C:\DRSYS\System32\OB2DR\bin\recovery.srd` **[Enter]**を押します。SRDファイルがメモ帳で開きます。
6. SRDファイルを編集します。
7. SRDファイルを編集して元の場所に保存した後、`C:\DRSYS\System32\OB2DR\bin`から次のコマンドを実行します。

   ```
   omnidr -drimini C:\$DRIM$.OB2\OBRecovery.ini
   ```
8. 通常のEADR/OBDRの復旧手順の次の作業を開始します。

Linuxシステム

1. ディザスタリカバリウィザードが表示されたら、カウントダウン中に**[Q]**キーを押してこのウィザードを停止し、**[Install Only]**オプションを選択します。このオプションを選択した場合、ターゲットシステムにインストールされるのは、最小バージョンのData Protectorのみです。ディザスタリカバリの段階2は、[Install only]オプションを選択した場合は自動的に開始されません。
2. 別のシェルに切り替えます。

   SRDファイル`/opt/omni/bin/recovery.srd`を編集します。詳細は、『*HPE Data Protectorディザスタリカバリガイド*』を参照してください。
3. SRDファイルを編集、保存した後、以下を実行します。

   ```
   omnidr -srd recovery.srd -drimini /opt/omni/bin/drim/drecovery.ini
   ```
4. 復旧が終了して以前のシェルに戻ったら、通常のEADR/OBDRリカバリ手順の次のステップに進みます。

SRDファイルを編集する場合の例

SRDファイル内の情報が最新でない場合(たとえば、バックアップデバイスを変更した場合)、更新されたSRDファイル(`recovery.srd`)を、段階2(ディザスタリカバリの)を実行する前に変更して、正常な復旧ができるように正しくない情報を更新します。

`devbra -dev`コマンドを使用すると、一部のデバイス構成情報を表示できます。

MAクライアントの変更

クライアント`old_mahost.company.com`に接続されているバックアップデバイスを使って、ディザスタリカバリ用のバックアップを実行したとします。しかし、ディザスタリカバリ時には、同じバックアップデバイスが同じSCSIアドレスのクライアント`new_mahost.company.com`に接続されているとします。ディザスタリカバリを実行するには、ディザスタリカバリの段階2を実行する前に、更新後のSRDファイル内の`-mahost old_mahost.company.com`という文字列を`-mahost new_mahost.company.com`に置き換えます。

新しいMAクライアントバックアップデバイスに異なるSCSIアドレスが使用されている場合は、更新後のSRDファイル内の`-devaddr`オプションの値も変更します。

ファイルを編集し終えたら、元の場所にUnicode(UTF-16)形式で保存します。

バックアップデバイスの変更

バックアップに使用したデバイスとは別のデバイスを使ってディザスタリカバリを実行するには、更新後のSRDファイル内の以下のオプション値を変更します。

`-dev`、`-devaddr`、`-devtype`、`-devpolicy`、`-devioctl`、`-physloc`

ここで:

`-dev`	バックアップに使用するバックアップデバイスまたはドライブ(ライブラリ)の論理名を指定します。
`-devaddr`	SCSIアドレスを指定します。

-devtype	Data Protectorのデバイスの種類を指定します。
-devpolicy	デバイスのポリシーを指定します。1(スタンドアロン)、3(スタッカー)、5(ジュークボックス)、6(外部制御)、8 (Grau DASエクスチェンジャーライブラリ)、9 (STK Siloメディアライブラリ)、または10 (SCSI-IIライブラリ)のいずれかを定義できます。
-devioctl	ロボティクスのSCSIアドレスを指定します。
-physloc	ライブラリスロットを指定します。
-storname	論理ライブラリ名を指定します。

たとえば、MAホストdagnja (Windowsシステム)に接続されていてデバイス名がUltrium_dagnjaであるHPE Ultriumスタンドアロンデバイスを使用して、ディザスタリカバリ用のバックアップを実行したとします。ただし、ディザスタリカバリには、MAクライアントkerala(Linuxシステム)に接続されているUltrium_keralaというドライブを使用し、論理ライブラリ名がAutoldr_keralaであるHPE Ultriumロボティクスライブラリを使用するとします。

最初に、kerala上でdevbra -devコマンドを実行し、構成済みデバイスと構成情報のリストを表示します。この情報は、更新後のSRDファイル内の以下のオプション値を置き換える場合に必要です。

```
-dev "Ultrium_dagnja" -devaddr Tape4:1:0:1C -devtype 13 -devpolicy 1 -mahost
dagnja.company.com
```

これを次のように置き換えます。

```
-dev "Ultrium_kerala" -devaddr /dev/nst0 -devtype 13 -devpolicy 10 -devioctl
/dev/sg1 -physloc " 2 -1" -storname "AutoLdr_kerala" -mahost kerala.company.com.
```

ファイルを編集し終えたら、元の場所にUnicode(UTF-16)形式で保存します。

Windows BitLockerドライブ暗号化

Windows Vista以降のリリースシステムでのディザスタリカバリプロセス中、BitLockerドライブ暗号化で暗号化されたボリュームのロックを解除できます。

制限事項

特定のボリュームをロック解除しない場合、あるいはボリュームが損傷していてロック解除できず、フォーマットする必要がある場合、ディザスタリカバリ後にボリュームは暗号化されていない状態になります。このような場合、ボリュームをもう一度暗号化する必要があります。

なお、システムボリュームは常に暗号化されない状態で復元されます。

手順

1. ディザスタリカバリモジュールが暗号化されたボリュームを検出すると、そのボリュームのロック解除を促すメッセージが表示されます。

   [はい]をクリックすると、ロック解除ウィザードを起動します。**[いいえ]**をクリックすると、暗号化されたボリュームはロックされたままになります。
2. [ロックされたボリュームの選択]ページに、検出された暗号化されたボリュームが一覧されます。ロック

を解除するボリュームを選択し、**[次へ]**をクリックします。

3. [ボリュームのロック解除]ページで(選択したボリュームごとに1ページ表示される)、ロック解除方法を指定するように要求されます。以下のロック解除方法を使用できます。
   - *パスワード(Windows 7以降のリリースで使用可能)*

     ボリュームを暗号化したときに使用した文字列。
   - パスフレーズ

     ボリュームを暗号化したときに使用した、通常のパスワードより長い文字列。
   - リカバリキー

     暗号化したボリュームごとに作成した特殊な非表示キー。リカバリキーにはBEK拡張子が付き、リカバリキーテキストファイルに保存されます。**[ブラウズ]**をクリックして、リカバリキーファイルを指定できます。

   テキストボックスに要求された情報を入力し、**[次へ]**をクリックします。
4. ボリュームが正常にロック解除されたことを確認して、**[完了]**をクリックします。

> **注:**
> ロック解除プロセスが失敗した場合は、エラー情報を確認して、ロック解除手順を再試行するか、スキップしてください。

異なるハードウェアへの復旧

> **注:**
> 異なるハードウェアへの復旧は、拡張自動ディザスタリカバリの拡張です。ここに記載されている情報と併せてそちらも参照してください。

ハードウェア障害または同様の障害が発生した後で、一部またはすべてのハードウェアがオリジナルのハードウェアと異なるシステム(**異なるハードウェア**)に対してバックアップを復元する必要がある場合があります。

異なるハードウェアの復旧では、標準的なEADRとOBDRの手順に次の手順を追加します。

1. バックアップ時にディザスタリカバリモジュールは、ネットワーク構成情報とハードウェア情報も収集します。
2. これにより、DR OSイメージへのクリティカルデバイスのドライバーの挿入が可能になり、これらのドライバーが復元時に使用可能になります。見つからないドライバーがある場合は、復元時にそれらを手動で挿入することもできます。
3. 復元中ネットワークとハードウェア情報は、復元されたOSに対してネットワークを適切に構成およびマッピングし、さらに見つからない不可欠なハードウェアを検出するために使用されます。

異なるハードウェアの復旧が必要になる場合

- **ハードウェア障害**

異なるハードウェアの復旧が必要になるのは、ストレージコントローラーやプロセッサー、マザーボードなどのブートに必要なハードウェアの一部に障害が発生し、同一でないハードウェアとの交換が必要になったときです。

- **障害**

  マシン全体の障害が発生して次のような状況になった場合、異なるハードウェアの復旧が必要になります。

  - 予算に対する制限や、障害が発生しているマシンの使用期間、またはその他の原因により、適合するマシンが見つからない。
  - システムの停止期間が長期間にならないようにするため、システムをすぐに稼働させる必要がある。

  このような状況で、異なるハードウェアの復旧を使用すると、オリジナルシステムの正確なクローンが必要なくなるため、経費を低減させることができます。

- **移行**

  次の状況では、異なるハードウェアの復旧が必要になります。

  - OSの再インストールおよび再構成を選択できない、より高速またはより新しいハードウェアである別のマシンへの移行。
  - 物理システムから仮想環境へ、またはその逆への移行。

    ディザスタリカバリモジュールの見地では、仮想環境は、他の仮想プラットフォームまたは物理プラットフォーム上で作成されたシステムバックップを復元するために、重要なドライバーを用意するのに必要となる別のハードウェアプラットフォームとなります。仮想環境には、後述する制限と要件も適用されます。

概要

異なるハードウェアの復旧フェーズは標準のディザスタリカバリフェーズですが、*次の点で異なります*。

- **段階0:**ネットワーク構成とハードウェアについての追加情報を収集します。
- **段階1:**マシンは、ディザスタリカバリ実行可能ファイルがディスク、ファイルシステム、ネットワーク、WIN32 APIにアクセスできる状態になります。復旧に必要なデバイスがチェックされます。見つからないドライバーがあると、それらを用意するよう促すメッセージが表示されます。
- **フェーズ2**: OSの復元は同じ処理を実行しますが、その後、さらに次のサブフェーズが発生します。
  - **段階2a**:重要なドライバーの挿入、レジストリの更新、ネットワークのマッピングを通して、復元されたオペレーティングシステムを準備し、ハードウェアに適用します。
- **フェーズ3**: 同じ処理を実行しますが、段階2で復元されなかったデータを復元します。

要件

- ターゲットマシンに対して少なくともブートに必要なドライバー(ネットワークドライバーなど)をすべて用意する必要があります。これらのドライバーは、イメージ作成時に直接イメージに追加する(推奨)ことも、復元(段階1)時に読み込むこともできます。また、ローカルの復元を試行する場合は、ローカルに接続しているテープデバイスなどのバックアップデバイスのドライバーも使用可能にする必要があります。

  詳細については、ドライバー、ページ 83を参照してください。

- 復元されたOSの自動ネットワーク構成復元では、復元時にネットワークドライバーを用意しておく必要があります。
- システム復元を行うには、少なくとも、バックアップシステムと同じディスク数(ディスクサイズが同じまたはそれ以上)が必要になります。
- オリジナルのOSは、ターゲットマシン(サーバーまたはワークステーション)上でハードウェアメーカーによってサポートされる必要があります。
- 異なるハードウェアを復旧する前に、ターゲットマシンのシステムファームウェアを最新の状態にすることをお勧めします。
- バックアップ中に異なるハードウェアのサポートを無効にする場合、バックアップするシステム上で`drm.cfg`ファイルを編集し`enable_disshw`オプションを`0`に設定します。
- システムには少なくとも1つのNTFSボリュームを含める必要があります。NTFSボリュームはバックアップフェーズ中に、VSSのストレージポイントとして機能します。

制限事項

[シャドウコピーを使用]オプションを選択してバックアップを実行した場合(サポートされているプラットフォームではデフォルトで選択されています)、ディザスタリカバリモジュールは異なるハードウェアの復旧のみをサポートします。

- 異なるハードウェアのサポートは、以下のオペレーティングシステムのリリースのEADRおよびOBDRにのみ提供されます。
  - Windows Vista
  - Windows 7の場合
  - Windows Server 2008
  - Windows Server 2008 R2の場合
  - Windows 8の場合
  - Windows 8.1の場合
  - Windows Server 2012
  - Windows Server 2012 R2の場合

  詳細については、最新のサポート一覧(https://softwaresupport.hpe.com/)を参照してください。
- 次のクロスプラットフォームの復元の組み合わせがサポートされています。

開始	この行を、以下のように変更します。
64ビット(x64)のオペレーティングシステム	64ビット(x64)のハードウェアアーキテクチャー
32ビットのオペレーティングシステム	32ビットまたは64ビット(x64)のハードウェアアーキテクチャー

アップグレードされたオペレーティングシステムの異なるハードウェアの復旧は、“ジェネリック”リカバリモードオプションを使用する場合にのみサポートされます(回復手順、ページ84を参照)。

- ネットワークカードのチーミング構成はサポートされていません。必要な場合は、OSを復元した後に再構成する必要があります。ディザスタリカバリモジュールは、物理的なネットワークカード構成のみを復元します。
- ディザスタリカバリモジュールは、INFファイルを提供するドライバーのみを挿入できます。グラフィックドライバーのように独自のインストール手順があるドライバーはサポートされておらず、これらのドライバーは段階1または段階2a時には挿入できません。ただし、ブートに必要なデバイスドライバーについては、一般にメーカーがINFファイルを提供します。
- ターゲットマシンのディスクは、同じホストアダプターバスタイプ(SCSIまたはSASなど)に接続しておく必要があり、そうでない場合は、復旧が失敗する場合があります。
- “無人”モードを使用してドメインコントローラーを復旧する場合、手動でログインしてsysprepクリーンアップを完了する必要があります。クリーンアップが完了すると、OSが自動的に再起動し、システムが使用可能になります。

推奨事項

異なるハードウェアを復旧する前に、ターゲットマシンのシステムファームウェアを最新の状態にしておく必要があります。

ドライバー

> **注:**
> DR OSイメージには、汎用の重要なドライバー(特にストレージコントローラー)の大規模なデータベースが含まれます。挿入するオリジナルドライバーが見つからない場合、汎用のドライバーがDR OSイメージに既に存在している可能性が高いです。

異なるハードウェアの復旧を可能にするには、新しいシステムの復元と起動に不可欠なドライバーを入手する必要があります。以下のドライバーを用意する必要があります。

- ターゲットシステムのすべてのストレージコントローラーのドライバー。このドライバーによって、復元またはブート時での基盤となるストレージの検出が可能になります。
- ネットワークの復元を可能にし、既存のドライバーの保存場所にアクセスするためのネットワークカードドライバー、およびローカルの復元を試行する場合は、ローカルに接続されているバックアップデバイス(テープドライブなど)のドライバー。

準備フェーズ(段階0)のバックアップ中にオリジナルのハードウェアのドライバーをDR OSイメージに含めることも、イメージの作成中に新しいハードウェアのドライバーを追加することもできます。また、復元プロセス中にこれらのドライバーを手動で追加することもできます。

ディザスタリカバリモジュールは復元プロセス中にブートに必要なドライバーのみを検索しますが、ブートに必要でないドライバーをDR OSイメージに追加し、その後「ドライバーの読み込み」タスクメニューオプションを使用して復元中に挿入できます。

オペレーティングシステムをブートしたら、その他の見つからないハードウェアドライバーをインストールする必要があります。

準備

> **注:**
> この準備は、システムに対して各ハードウェア構成を変更した後に実行する必要があります。

準備は、EADR(「EADRの準備」を参照)およびOBDR(「OBDRの準備」を参照)の場合と同じですが、以下の変更点があります。

- ディザスタリカバリモジュールは、ネットワーク構成とハードウェア情報も収集します。
- ストレージやネットワーク、テープなどの重要なデバイスドライバーを用意する必要があります。したがって、ディザスタリカバリモジュールは、イメージの作成時にドライバーをDR OSイメージに挿入できます。「ドライバー、前のページ」を参照してください。

回復手順

HPE Data Protectorディザスタリカバリ GUIの[リカバリオプション]ページで異なるハードウェアの復旧を有効にすると、復旧プロセス中にシステムがスキャンされ、見つからないドライバーが検索されます。重要なドライバー(ストレージ、テープ、ネットワークドライバー、またはディスクコントローラー)で見つからないドライバーがあると、見つからないドライバーを読み込むよう促すメッセージが表示されます。

手順

1. ディザスタリカバリ手順中に見つからないドライバーを読み込むことを促すメッセージが表示されたら、**[はい]**をクリックして異なるハードウェアウィザードを開始します。**[いいえ]**をクリックすると、ドライバーの挿入手順がスキップされます。
2. [デバイスの選択]ページで、ドライバーを読み込むデバイスを選択します。**[次へ]**をクリックします。
3. [ドライバーの検索場所]ページで、ドライバーを保存している実行中のシステム上の検索場所を指定します。デバイスドライバーをブラウズするか、[ドライバーのパス]テキストボックスに場所を入力して、**[パスの追加]**をクリックして指定したパスをリストに追加します。システム固有の特性に合わせて検索を調整するために、**[検索ツリーの深さ]**オプションを使用できます。

   > **注:**
   > 検索リストから指定した場所を削除するには、この場所を右クリックして、**[削除]**を選択します。

   指定した場所に対して検索を実行して、見つからないドライバーを探します。**[次へ]**をクリックします。
4. 指定した場所を検索して見つからないドライバーを探すと、次のような結果が考えられます。
   - デバイスドライバーが見つかった場合:[ドライバーのパス]テキストボックスに、対応するドライバー情報ファイル(`*.inf`)への完全パスが指定されます。このドライバーが適切であるかどうかを検証し、**[次へ]**をクリックしてこのドライバーを読み込みます。
   - デバイスドライバーが見つからなかった場合: [ドライバーのパス]テキストボックスは空になります。次のいずれかの作業を行います。

     別のドライバーを検索する場合は、**[ブラウズ]**をクリックします。[ファイルのブラウズ]ダイアログで、デバイスドライバーのパスを選択して、**[次へ]**をクリックします。

このデバイスに対してドライバーを読み込まない場合は、[ドライバーのパス]テキストボックスを空のままにして、**[次へ]**をクリックして次のページに進むか、または**[スキップ]**をクリックしてウィザードを終了します。

> **注:**
> デバイスに対応しないドライバーを指定すると、このドライバーは無効となり、読み込むことはできません。このドライバーが適切でない場合、変更するか、または読み込みをスキップできます。

5. [ドライバーインストールの進行状況]ページで、デバイスドライバーが正常に読み込まれたどうかを確認できます。エラーが報告された場合、**[再試行]**をクリックしてドライバーの読み込みを試してください。**[完了]**をクリックします。

OSの復元と準備

OSの復元プロセスは、標準的なEADR(手順5)およびOBDR(手順6)プロセスでの処理と同じです。復元プロセスでは、このOSの復元プロセスの後のアプリケーションとファイルの復元に向けてOSを準備するために、復元したOSを異なるハードウェアに対して準備し、適合させます。このプロセスでは、ブートに必要なドライバーの挿入、復元したOSのレジストリの更新、ネットワークのマッピングを実行します。

段階0で実行中のDR OSイメージに読み込むか、OSの復元中に手動で追加したことにより、ブートに必要なドライバーがすべて存在しているはずなので、これらのドライバーの挿入は自動的に実行されます。ただし、ネットワークのマッピングを修正するには、ユーザーの操作が必要になる場合があります。

ネットワークマッピングの修正

異なるハードウェアへの復旧が完了したら、ディザスタリカバリモジュールによって、復元しようとするシステム上のネットワークアダプターが、オリジナルシステムのネットワークアダプターと同じであるかどうかをチェックされます。ディザスタリカバリモジュールは、オリジナルシステムのネットワーク構成をターゲットシステムのネットワーク構成に常にマッピングできるわけではありません。たとえば、ターゲットシステムに1つのネットワークカードが搭載されているが、オリジナルシステムに複数のネットワークカードが搭載されている場合や、ターゲットシステムにネットワークアダプターを追加した場合などがそうです。こうした不一致が検出されたり、または適切なネットワークマッピングが自動的に決定できない場合、オリジナルのネットワークアダプターをターゲットシステム上で検出されたネットワークアダプターにマッピングできます。

> **注:**
> ネットワークマッピングは、使用可能なネットワークアダプターにのみ実行されます。ドライバーが存在しないネットワークアダプターはマッピングできません。このため、復旧プロセスを開始する前に、ネットワークカードドライバーを読み込む必要があります。

手順

1. [ネットワークアダプターマッピング]ページで、[オリジナルネットワークアダプター]ドロップダウンリストからオリジナルシステムのネットワークアダプターを選択します。[現在のネットワークアダプター]ドロップダウンリストで、ターゲットシステムで使用可能なネットワークアダプターのいずれか1つを選択します。**[マッピングの追加]**をクリックします。作成したマッピングがリストに追加されます。

   > **注:**
   > リストからマッピングを削除するには、マッピングを右クリックして、**[削除]**を選択します。

2. 必要なネットワークアダプターすべてをマッピングしたら、**[完了]**をクリックします。

OSを正常に復元した後

異なるハードウェアを復旧すると、OSのアクティブ化はリセットされます。OSを正常に復元したら、次の操作を実行する必要があります。

- OSを再アクティブ化します。
- 確認し、必要に応じて、見つからないシステムドライバーを再インストールします。

ユーザーデータとアプリケーションデータの復元

この段階は、EADRで実行する処理と同じです。拡張自動ディザスタリカバリ(EADR)、ページ 36を参照してください。

> **注:**
> OSのブート後に、サードパーティ製アプリケーションサービスおよびドライバーの読み込みが失敗することがあります。これらのアプリケーションは再インストールして再構成する必要があります。これらのアプリケーションが不要な場合は、現在のシステムから削除する必要があります。

物理システムから仮想マシン(P2V)への復旧

Data Protectorは、VMware vSphere、Microsoft Hyper-V、またはCitrix XenServerなど、オリジナルのオペレーティングシステムをサポートする仮想環境への復旧をサポートしています。

前提条件

ターゲット仮想マシンの要件は以下のとおりです。

- ゲストオペレーティングシステムは元のオペレーティングシステム(Windows、Linuxなど)と同じタイプであることが必要です。
- 仮想マシンは、元のシステムと同数またはそれ以上のディスクを装備している必要があります。
- ディスクは対応する元のディスクと同じまたはそれ以上のサイズであることが必要です。
- ディスク順序は、元のシステム上の順序と同じであることが必要です。
- 仮想マシンに割り当てられるメモリ容量は、リカバリ処理に影響することがあります。このため、最低1GB以上のメモリを仮想マシンに割り当てることを推奨します。
- 仮想ビデオカードのメモリサイズは、元のシステムのディスプレイ解像度に基づいて元のシステムの要件を満たしている必要があります。可能であれば、自動設定を使用します。
- 元のマシン上のネットワークアダプターと同数のネットワークアダプターを追加します。それらのアダプターは元のシステムと同じネットワークに接続する必要があります。

手順

DR OSイメージを使用して仮想マシンをブートし、異なるハードウェアに対し標準のディザスタリカバリ手順を実行します。

仮想マシンから物理システム(V2P)への復旧

仮想マシンから物理システムへのディザスタリカバリは、異なるハードウェアに対する標準のディザスタリカバリを使用して実行します。

第4章: UNIXシステム上でのディザスタリカバリ

手動によるディザスタリカバリ(MDR)

手動によるディザスタリカバリは、基本的な復旧方法です。これは、最初にインストールしたときと同じ方法でシステムを再インストールすることにより、システムを復旧しようというものです。オペレーティングシステムを含むすべてのファイルの復元には、Data Protectorを使用します。

HP-UXクライアントの手動によるディザスタリカバリは、Ignite-UX製品をベースにしています。これは主にHP-UXシステムのインストールと構成作業用に開発されたアプリケーションで、(システム管理用の強力なインターフェイスに加え)システム障害に対する準備と復旧のための機能を備えています。

ターゲットクライアントのディザスタリカバリにIgnite-UXを使用するとともに、ユーザーデータおよびアプリケーションデータの復元にData Protectorを使用することで、ディザスタリカバリの段階3を実現できます。

> **注:**
> この項では、Ignite-UXの全機能を網羅しているわけではありません。詳細については、『*Ignite-UX管理ガイド*』を参照してください。

概要

Ignite-UXには、システムのディザスタリカバリを準備し、システムを障害から復旧するための2通りのアプローチがあります。

- カスタムインストールメディアを使用する(Golden Image)
- システム復旧ツールを使用する(make_tape_recovery、make_net_recovery)

ハードウェアの構成とOSのリリースが共通するシステムが多数含まれるIT環境では、カスタムインストールメディアが威力を発揮します。これに加え、システム復旧ツールを使用すると、個々のシステムに応じてカスタマイズされた復旧アーカイブを作成できます。

どちらの方法でも、DDSテープやCDなどの起動可能なインストールメディアを作成できます。これらのメディアを使用すると、障害が発生したクライアントのシステムコンソールから直接、ローカルディザスタリカバリを実行できます。

さらに、どちらの方法でも、障害の発生したクライアントに適切なGolden Image、または事前に作成した復旧アーカイブを割り当てることで、ネットワークに基づくクライアントの復旧を実行できます。この場合、クライアントは、Igniteサーバーから直接ブートされ、割り当てられているデポからインストールが実行されます。このデポは、ネットワーク上のNFS共有上に存在する必要があります。

サポートされている場合は、Ignite-UX GUIを使用してください。

手動によるディザスタリカバリの準備(HP-UX Cell Manager)

ディザスタリカバリを成功させるには、一般的な準備手順に加えて、その方法固有の要件にも従っておく必要があります。ディザスタリカバリを迅速かつ効率的に実行するには、事前の準備作業が欠かせません。

手動によるCell Managerのディザスタリカバリの準備には、次の作業が含まれます。

- バックアップ仕様の情報を収集します。
- バックアップ仕様を準備します(実行前スクリプトを使用)。
- バックアップを実行します。
- 内部データベースバックアップセッションを定期的に実行します。

Cell Managerに対するディザスタリカバリを実行するには、事前にこれらの準備作業をすべて行っておく必要があります。

1回のみ必要な準備作業

障害発生時に必要な情報をすばやく探し出せるように、ディザスタリカバリ計画の中でこれらのファイルの保管場所を文書に明記しておかなければなりません。さらにバージョン管理の方法についても検討が必要です(個々のバックアップごとに一連の"補助情報"が存在します)。

バックアップするシステム上に低い実行レベルで実行されるアプリケーションプロセスが存在する場合は、整合性のある形でCell Managerをバックアップできるように、システムを`minimal activity`状態(修正された`init 1 run-level`)に移行する必要があります。

HP-UXシステム

- ブートアップセクションに対する変更を補完するために、一部の抹消リンクを`/sbin/rc1.d to /sbin/rc0.d`から移動します。これらの抹消リンクに含まれる基本サービスは、バックアップ時に必要なものであり、このようにしておかなければ実行レベル1に移行した時点で停止されてしまいます。
- システム上に`rpcd`が構成されていることを確認します(`/etc/rc.config.d/dce`ファイル内にオプション`RPCD=1`を構成)。

これにより、次の特徴を持った最小アクティビティ状態にシステムを移行できます。

- Init-1 (`FS_mounted, hostname_set, date_set, syncer_running`)
- 実行中のプロセス: `network`、`inetd`、`rpcd`、`swagentd`

システムのバックアップ

バックアップ仕様の準備ができたら、バックアップ手順を実行します。バックアップは定期的に実行するか、少なくとも主要なシステム構成の変更時にその都度実行しなければなりません(特に物理ボリューム構造または論理ボリューム構造を変更した場合)。IDBおよびファイルシステムのバックアップについては、以下に示すような特別な注意が必要です。

- IDBは定期的にバックアップしてください。このための専用のバックアップ仕様を作成し、Cell Manager自体のバックアップ後に実行するようスケジュール設定できれば理想的です。
- IDBとファイルシステムは、Cell Managerシステムに接続された特定のデバイス上にバックアップするようにしてください。こうしておけば、このデバイス内のメディアにIDBの最新のバックアップバージョンが保存されていることが保証されます。

HP-UXシステムを手動でインストールおよび構成する(Cell Manager)

障害が発生したら、最初にオペレーティングシステムをインストールして構成する必要があります(段階1)。これで、Cell Managerを復旧できます。

手順

段階1

1. 影響があったディスクを交換します。
2. オペレーティングシステムのインストール用メディアからシステムをブートします。
3. オペレーティングシステムを再インストールします。インストール中に、準備段階で収集したデータ(実行前スクリプト)を使用して、物理的および論理的な記憶領域/ボリューム構造、ファイルシステム、マウントポイント、ネットワーク設定などを再作成して構成します。

システムデータを手動で復元する(HP-UX Cell Manager)

オペレーティングシステムをインストールして構成したら(段階1)、Data Protectorを使用してCell Managerを復元できます。

前提条件

- Cell Managerシステムのルートボリュームの最新バックアップイメージと、IDBの最新バックアップイメージを保存したメディアが必要です。
- Cell Managerシステムに接続されたデバイスが必要です。

手順

段階2

1. Cell Manager上にData Protectorソフトウェアを再インストールします。
2. IDBと`/etc/opt/omni`ディレクトリを、それぞれの最新のバックアップイメージから一時ディレクトリに復元します。これにより、バックアップメディアから他のすべてのファイルを容易に復元できます。次に、`/etc/opt/omni/`ディレクトリを削除し、一時ディレクトリの`/etc/opt/omni`ディレクトリで置き換えてく

ださい。これにより以前の構成が再構築されます。

3. `omnisv -start`コマンドを使ってData Protectorプロセスを起動します。

段階3

4. Data Protector GUIを起動して、バックアップイメージから必要なファイルを復元します。
5. システムを再起動します。

以上の操作によりCell Managerが適正に復旧されます。

手動によるディザスタリカバリの準備(HP-UXクライアント)

Ignite-UXには、システムのディザスタリカバリを準備し、システムを障害から復旧するための2通りのアプローチがあります。

カスタムインストールメディアを使用する(Golden Image)

システム復旧ツールを使用する(make_tape_recovery、make_net_recovery)

カスタムインストールメディアを使用する(Golden Image)

大規模なIT環境には、同じハードウェアとソフトウェアをベースとするシステムが多数含まれることがよくあります。このような場合は、インストール済みのシステムの完全なスナップショットを他のシステムのインストールに使用すると、新しいシステムのOS、アプリケーション、および必要パッチのインストールに要する時間を大幅に短縮できます。Ignite-UXには、Golden Imageを別のシステムに割り当てる前に、ネットワークやファイルシステムの設定などのパラメーターを修正したり、Data Protectorなどのソフトウェアをイメージに追加する機能が用意されています(`make_config`コマンドを使用)。この機能は、システムを障害から復旧するときに使用できます。

カスタムインストールメディアの使用手順の概要は、以下のとおりです。

1. **段階0**
   a. クライアントシステムのゴールドイメージを作成します。
2. **段階1**および**2**
   a. 問題のあるディスクを交換ディスクと交換します。
   b. HP-UXクライアントをIgnite-UXサーバーからブートし、ネットワークを構成します。
   c. ゴールドイメージをIgnite-UXサーバーからインストールします。
3. **段階3**
   a. Data Protectorの標準復元手順で、ユーザーデータとアプリケーションデータを復元します。

Golden Imageの作成

1. `/opt/ignite/data/scripts/make_sys_image`ファイルをIgnite-UXサーバーからクライアントシステム上の一時ディレクトリにコピーします。
2. クライアントノードで、次のコマンドを実行して別のシステム上にクライアントの圧縮イメージを作成し

ます。make_sys_image -d *directory of the archive* -n *name of the archive*.gz -s *IP address of the target system*

このコマンドを実行すると、-dオプションと-sオプションで定義した特定のシステム上の特定のディレクトリにgzipファイルデポが作成されます。使用するHP-UXクライアントがターゲットシステムに対するパスワードなしアクセス権を持っていること(クライアントシステムの名前がターゲットシステム上の.rhostsファイルにエントリとして記述されていること)を確認してください。このアクセス権がないと、コマンドを実行できません。

3. ターゲットシステム上の/etc/exportsディレクトリにターゲットディレクトリを追加し、そのディレクトリをターゲットサーバーにエクスポートします(exportfs -av)。
4. 構成用Ignite-UXサーバー上で、アーカイブテンプレートファイルcore.cfgをarchive_*name*.cfgにコピーします。cp /opt/ignite/data/examples/core.cfg /var/opt/ignite/data/*OS_Release*/archive_*name*.cfg.

   例：cp /opt/ignite/data/examples/core.cfg /var/opt/ignite/data/Rel_B.11.31/archive_HPUX11_31_DP70_CL.cfg
5. コピーした構成ファイル内で、以下のパラメーターをチェックし適切に変更します。
   - sw_sourceセクション:

     load_order = 0

     source_format = archive

     source_type="NET"

     # change_media=FALSE

     post_load_script = "/opt/ignite/data/scripts/os_arch_post_l"

     post_config_script = "/opt/ignite/data/scripts/os_arch_post_c"

     nfs_source = "*IP Target System*:*Full Path*
   - 対応するOSアーカイブセクション:

     archive_path = "*archive_name*.gz
6. 以下のarchive_impactコマンドをイメージファイルに対して実行して、“impacts”エントリの値を決定し、出力を構成ファイルの同じ“OS archive”セクションにコピーします。
   /opt/ignite/lbin/archive_impact -t -g *archive_name*.gz

   例：/opt/ignite/lbin/archive_impact -t -g /image/archive_HPUX11_31_DP70_CL.gz

   impacts = "/" 506Kb

   impacts = "/.root" 32Kb

   impacts = "/dev" 12Kb

   impacts = "/etc" 26275Kb

   impacts = "/opt" 827022Kb

   impacts = "/sbin" 35124Kb

   impacts = "/stand" 1116Kb

   impacts = "/tcadm" 1Kb

   impacts = "/usr" 729579Kb

   impacts = "/var" 254639Kb
7. 新規作成したデポをIgnite-UXが認識できるように、以下のレイアウトで/var/opt/ignite/INDEX

ファイルにcfgエントリを追加します。

```
cfg "This_configuration_name" {
description "Description of this configuration”
"/opt/ignite/data/OS/config"
"/var/opt/ignite/data/OS/ archive_name.cfg"
}
```

例：

```
cfg "HPUX11_31_DP70_Client" {
description "HPUX 11.i OS incl Patches and DP70 Client"
"/opt/ignite/data/Rel_B.11.31/config"
"/var/opt/ignite/data/Rel_B.11.31/archive_HPUX11_31_DP70_CL.cfg"
}
```

8. ブートクライアントに対して予約する1つまたは複数のIPアドレスが、/etc/opt/ignite/instl_boottabファイル内で構成されていることを確認します。IPアドレスの数は、並行ブートクライアントの数と同じになります。

上記の手順により、HP-UXクライアント用のGolden Imageを作成できます。このGolden Imageは、特定のハードウェア構成とソフトウェア構成を反映しており、レイアウトが類似している任意のクライアントの復旧に使用できます。

ハードウェア構成とソフトウェア構成の違いに応じて上記の手順を繰り返し、すべてのシステムに対応するGolden Imageを作成する必要があります。

Ignite-UXでは、作成済みのGolden Imageに基づいて起動可能テープ/CDを作成できます。詳細については、『*Ignite-UX Administration Guide*』を参照してください。

HP-UXクライアントを復旧する

手動によるディザスタリカバリ(MDR)を使用するHP-UXクライアントの復旧には、次の3つの方法があります。

Golden Imageを使った復旧

起動可能バックアップテープからの復旧

ネットワークからの復旧

Golden Imageを使った復旧

ネットワーク上のNFS共有上に置いたGolden Imageを適用して、HP-UXクライアントを復旧することができます。

クライアント上での操作

手順

1. 故障したハードウェアを交換します。
2. Ignite-UXサーバーからHP-UXクライアントをブートします。`boot lan.IP-address Ignite-UX server install.`
3. [Welcome to Ignite-UX]画面が表示されたら、**[Install HP-UX]**を選択します。
4. [GUI Option]画面から**[Remote graphical interface running on the Ignite-UX server]**を選択します。
5. ネットワーク構成ダイアログボックスに応答します。
6. 以上の手順で、システムに対してIgnite-UXサーバーによるリモートインストールを行う準備が完了します。

Ignite-UXサーバー上の操作

手順

1. Ignite-UX GUI内でクライアントのアイコンを右クリックし、**[Install Client - New Install]**を選択します。
2. インストールするGolden Imageを選択し、設定(ネットワーク、ファイルシステム、タイムゾーン、など)をチェックして、**[Go!]**をクリックします。
3. クライアントのアイコンを右クリックして**[Client Status]**を選択すると、インストールの進行状況をチェックできます。
4. インストールが完了したら、Data Protectorの標準復元手順で、その他のユーザーデータやアプリケーションデータを復元します。

起動可能バックアップテープからの復旧

ブート可能バックアップテープは、make_tape_recoveryコマンドによって作成されます。

手順

1. 故障したハードウェアを交換します。
2. 影響があったHP-UXクライアントにテープデバイスがローカルに接続されていることを確認した上で、復元するアーカイブが書き込まれているメディアを挿入します。
3. 準備した復旧テープからブートします。このテープからブートするには、ブート管理メニューにSEARCHと入力して、使用可能なすべてのブートデバイスのリストを表示します。どのデバイスがテープドライブかを特定し、ブートコマンド: `boot hardware path`または`boot Pnumber`と入力します。
4. 復旧処理が自動的に開始します。
5. 復旧が正常に完了したら、Data Protectorの標準復元手順で、その他のユーザーデータやアプリケーションデータを復元します。

ネットワークからの復旧

Ignite-UXサーバーにある復旧アーカイブファイルから、ネットワーク経由でターゲットシステムをブートできます。Golden Imageを使った復旧の手順に従い、インストールするアーカイブを正しく選択してください。

システム復旧ツールを使用する(make_tape_recovery、make_net_recovery)

Ignite-UXにバンドルされているシステム復旧ツールにより、ディスク障害の復旧を迅速かつ容易に行うことができます。デフォルトでシステム復旧ツールの復旧アーカイブに含まれるのは、HP-UXの運用に不可欠なディレクトリのみです。しかし、復旧をより迅速に行うために、他のファイルやディレクトリ(追加のボリュームグループもしくはData Protectorのファイルおよびディレクトリなど)をアーカイブに含めることも可能です。

`make_tape_recovery` は、ブート可能な復旧(インストール)テープを作成するツールです。この復旧テープは使用しているシステム用にカスタマイズされており、バックアップデバイスをターゲットシステムに直接接続して、ターゲットシステムをこのブート可能な復旧テープから起動することで、無人のディザスタリカバリが可能となります。アーカイブ作成時とクライアント復旧時は、バックアップデバイスをクライアントにローカル接続しておく必要があります。

`make_net_recovery` は、ネットワーク上のIgnite-UXサーバーまたは他の指定システム上に、復旧アーカイブを作成するツールです。ターゲットシステムは、Ignite-UXの`make_boot_tape`コマンドで作成したブート可能なテープから起動するか、またはIgnite-UXサーバーから直接ブートした後、サブネットを通じて復旧することができます。Ignite-UXサーバーからの直接の起動は、Ignite-UXのbootsysコマンドで自動的に行うか、またはブートコンソールから対話的に指定して行うことができます。

システム復旧ツールの使用手順の概要は、以下のとおりです。

1. **段階0**
   a. Ignite-UXサーバー上のIgnite-UX GUIを使用して、HP-UXクライアントの復旧アーカイブを作成します。
2. **段階1**および**2**
   a. 問題のあるディスクを交換ディスクと交換します。
   b. ローカル復元の場合は、準備した復旧用テープからブートします。
   c. ローカル復元の場合は、復元プロセスが自動的に開始されます。
      ネットワーク復元の場合は、Ignite-UXクライアントからブートし、ネットワークとUIを構成します。
      ネットワーク復元の場合は、ゴールドイメージをIgnite-UXサーバーからインストールします。
3. **段階3**
   a. Data Protectorの標準復元手順で、ユーザーデータとアプリケーションデータを復元します。

前提条件

システムのディザスタリカバリのための準備作業を行うには、Ignite-UXサーバーがクライアントと通信できるように、クライアント上にIgnite-UXファイルセットをインストールしておく必要があります。

Ignite-UXサーバーとクライアントの両方に同じリビジョンのIgnite-UXファイルセットがインストールされていなければなりません。Ignite-UXファイルセットの整合性を確保するには、Ignite-UXサーバー上のデポからIgnite-UXをインストールするのが最も簡単な方法になります。このデポを構築するには、Ignite-UXサーバーで`pkg_rec_depot -f`次のコマンドを実行します。これにより、Ignite-UXのデポが`/var/opt/ignite/depots/recovery_cmds`ディレクトリに作成されます。クライアントで`swinstall`コマンドによりIgnite-UXをインストールする際に、このディレクトリをソースディレクトリとして指定します。

クライアントノードへのIgnite-UXのインストールが完了したら、Ignite-UXサーバー上のGUIからmake_net_recoveryまたはmake_tape_recoveryを使用して復旧アーカイブを作成できます。

make_tape_recoveryによるアーカイブの作成

1. HP-UXクライアントにバックアップデバイスが接続されていることを確認します。
2. 次のコマンドを実行して、Ignite-UX GUIを起動します。`/opt/ignite/bin/ignite &`
3. クライアントアイコンを右クリックし、`Create Tape Recovery Archive`を選択します。
4. HP-UXクライアントに複数のデバイスが接続されている場合は、テープデバイスを選択します。
5. アーカイブに含めたいボリュームグループを選択します。
6. テープ作成処理が開始します。クライアントのアイコンを右クリックし、`Client Status`を選択してIgnite-UXサーバー上のステータスとログファイルをチェックします。

> **注：**
> Ignite-UXでは、あらゆるDDSドライブに対応できるように90m DDS1バックアップテープの使用が推奨されています。

make_net_recoveryによるアーカイブの作成

`make_net_recovery`では、`make_tape_recovery`を使用する場合と基本的に同じ手順で復旧アーカイブを作成できますが、このコマンドでは、復旧アーカイブがデフォルトでIgnite-UXサーバー上に保存されるので、ローカル接続されたバックアップデバイスが必要ではないという利点があります。

1. 次のコマンドを実行して、Ignite-UX GUIを起動します。`/opt/ignite/bin/ignite &`
2. クライアントアイコンを右クリックし、`Create Network Recovery Archive`を選択します。
3. あて先のシステムとディレクトリを選択します。圧縮アーカイブを保存するのに十分なスペースがあることを確認してください。
4. アーカイブに含めたいボリュームグループを選択します。
5. アーカイブ作成処理が開始します。アイコンを右クリックし、`Client Status`を選択してIgnite-UXサーバー上のステータスとログファイルをチェックします。

> **注：**
> Ignite-UXでは、圧縮アーカイブファイルから起動可能なアーカイブテープを作成できます。`Ignite-UX Administration Guide`の`Create a Bootable Archive Tape via the Network`章を参照してください。

ディスクデリバリーによるディザスタリカバリ(DDDR)

ディスクデリバリーによるディザスタリカバリには2通りの方法があります。1つ目は、作業用のData Protectorクライアントシステムを使用し、このクライアントに新しいディスクを接続してディスクの準備をする方法です。また別の方法として、追加の作業用クライアントなしに補助ディスクを使用することも可能です。ディスクを適切にフォーマットしてパーティションを作成するには、障害発生前に十分なデータを収集しておく必要があります。

概要

UNIXクライアントのディスクデリバリーでは、持ち運び可能な補助ディスクを使用します。この補助ディスクには、最小限のオペレーティングシステムとネットワークおよびData Protectorエージェントをインストールしておきます。

準備の章に記載されている一般的な準備手順すべてを実行しておく必要があります。UNIXクライアントに対して補助ディスクを使用する手順の概要は、以下のとおりです。

1. **段階1**
   a. 障害が発生したディスクを交換ディスクと交換し、補助ディスクをターゲットディスクに接続した後、補助ディスクにインストールされている最小限のオペレーティングシステムでシステムを再起動します。
   b. 交換したディスクに手動でパーティションを作成して、記憶データ構造を再確立し、交換ディスクをブート可能にします。
2. **段階2**
   a. Data Protector標準復元手順でオリジナルシステムのブートディスクを交換ディスクに復元します(**Restore into**オプションを使用します)。
   b. システムをシャットダウンして、補助ディスクを取り外します。なお、ホットスワップが可能なハードディスクドライブを使用している場合は、システムをシャットダウンする必要はありません。
   c. システムを再起動します。
3. **段階3**
   a. Data Protectorの標準復元手順で、ユーザーデータとアプリケーションデータを復元します。

制限事項

- ターゲットシステムと同じハードウェアクラスのシステム上に、補助ディスクを用意する必要があります。
- クラスター環境を復旧する場合は、標準とは異なる作業が必要になることがあります。クラスター環境の構成によっては、追加の作業や環境に対する変更が必要になります。
- RAIDはサポートされていません。

UNIXクライアントに対するディスクデリバリーによるディザスタリカバリの準備

ディザスタリカバリを成功させるには、一般的な準備手順に加えて、その方法固有の要件にも従っておく必要があります。ディザスタリカバリを迅速かつ効率的に実行するには、事前の準備作業が欠かせません。サポートされているオペレーティングシステムの詳細は、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。

ディスクデリバリーによるディザスタリカバリの準備では、次の操作を行います。

- バックアップ仕様の情報を収集します。
- 補助ディスクを準備します。
- バックアップ仕様を準備します(実行前スクリプトを使用)。
- バックアップを実行します。

クライアントシステムに対してディザスタリカバリを実行するには、事前にこれらの準備作業をすべて実施しておく必要があります。

1回のみ必要な準備作業

実行前コマンドの中で情報を収集する場合は、障害発生時にこれらの情報をすばやく探し出せるように、ディザスタリカバリ計画の中でこれらのファイルの保管場所を文書に明記しておかなければなりません。さらにバージョン管理の方法についても検討が必要です(個々のバックアップごとに一連の"補助情報"が存在します)。

整合性のとれたバックアップを実行し、復旧後の問題を回避するには、バックアップ対象の各クライアントで`minimal activity`状態(修正された`init 1 run-level`)を確立することも必要です。詳細については、ご使用のオペレーティングシステムのマニュアルを参照してください。

HP-UXの場合の例

- ブートアップセクションに対する変更を補完するために、一部の抹消リンクを`/sbin/rc1.d to /sbin/rc0.d`から移動します。これらの抹消リンクに含まれる基本サービスは、バックアップ時に必要なものであり、このようにしておかなければ実行レベル1に移行した時点で停止されてしまいます。
- システム上に`rpcd`が構成されていることを確認します(`/etc/rc.config.d/dce`ファイル内にオプション`RPCD=1`を構成)。

これにより、次の特徴を持った最小アクティビティ状態にシステムを移行できます。

- Init-1 (`FS_mounted, hostname_set, date_set, syncer_running`)
- ネットワークが稼動している必要があります。
- 実行中のプロセス: `network`、`inetd`、`rpcd`、`swagentd`

Solarisの場合の例

- ブートアップセクションに対する変更を補完するために、一部の抹消リンクを`/etc/rc1.d to /etc/rc0.d`から移動します。これらの抹消リンクに含まれる基本サービスは、バックアップ時に必要な

ものであり、このようにしておかなければ実行レベル1に移行した時点で停止されてしまいます。

- rpcbindがシステム上で構成されていることを確認します。

これにより、次の特徴を持った最小アクティビティ状態にシステムを移行できます。

- Init-1
- ネットワークが稼動している必要があります。
- 実行中のプロセス: network, inetd, rpcbind

AIX

システムをアクティビティ最小の状態にしなくても、alt_disk_installコマンドで補助ディスクを準備するとディスクイメージの整合性が確保されるので、特別な処置は不要です。

補助ディスクの準備

補助ディスクを使用する場合は、事前にディスクを準備しておく必要があります。起動可能な補助ディスクは、各セル内のプラットフォームごとに1つしか必要ありません。このディスクには、オペレーティングシステムとネットワーク構成が含まれていて、起動可能である必要があります。

システムのバックアップ

バックアップ仕様の準備ができたら、バックアップ手順を実行します。バックアップは定期的に実行するか、少なくとも主要なシステム構成の変更時にその都度実行しなければなりません(特に物理ボリューム構造または論理ボリューム構造を変更した場合)。

UNIXクライアントのディザスタリカバリ用のバックアップ仕様を作成する

バックアップ仕様をUNIXクライアントのディザスタリカバリ用に構成するには、既存の仕様を変更するか、実行前および実行後スクリプトを指定して新しい仕様を作成します。サポートされているオペレーティングシステムの詳細は、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。

手順

1. 以下を実行する実行前スクリプトを作成します。
   - 環境に関して必要なすべての情報を収集して、収集した情報をディザスタリカバリが必要になったときに使用できる場所に格納します。必要情報は以下のとおりです。
     - システムの物理的および論理的な記憶領域構造
     - 現在の論理ボリューム構造(HP-UXシステムの場合の例: vgcfgbackupおよびvgdisplay -vを使用)
     - クラスターの構成データ、ディスクのミラー化情報、ストライプ化情報
     - ファイルシステムおよびマウントポイントの概要(HP-UXシステムの場合の例: bdfや/etc/fstab

のコピーを使用)
- システムページングスペース情報(HP-UXシステムの場合の例: `swapinfo`コマンドの出力)
- I/O構造の概要(HP-UXシステムの場合の例: `ioscan -fun`や`ioscan -fkn`を使用)
- 現在のネットワーク設定

データの緊急コピーを、バックアップ自体の中に含めることも可能です。その場合は、復旧作業を実施する前にこの情報を抽出してください。

- すべてのユーザーをシステムからログアウトさせます。
- アプリケーションデータを個別にバックアップする場合でない限り、データベースのオンラインバックアップなどを使ってすべてのアプリケーションを停止します。
- 必要に応じて、システムに対するネットワークアクセスを制限し、バックアップの実行中はシステムへのログオンができないようにします(HP-UXシステムの場合の例: `inetd.sec`の上書きおよび`inetd -c`)を使用)。
- 必要に応じて、システムの動作状態を最小限にします(たとえば、HP-UXシステムの場合は、`sbin/init 1; wait 60`;を使用して、`run-level 1`に到達したかどうかをチェックします)。これは、修正された"init 1"状態であることに注意してください。

2. システムの実行レベルを標準に戻したり、アプリケーションを再起動したりする実行後スクリプトを用意します。
3. 実行前および実行後スクリプトを使用して、Data Protector Cell Manager上のクライアントのバックアップ仕様を構成します。これにはすべてのディスクが含まれる必要があります。
4. バックアップ手順を実行します。この手順は、定期的に繰り返し実行するか、または少なくともシステム構成に主要な変更があった場合、特に論理ボリューム構造に何らかの変更があった場合に実行します(HP-UXでは、LVMを使用)。

DDDRを使用してUNIXクライアントをインストールおよび構成する

障害が発生したら、まず、問題のあるクライアントに対して新しいディスクをインストールして構成する必要があります(段階1)。

前提条件

- 影響があったディスクと交換するための新しいハードディスクが必要です。
- ターゲットシステムと同じハードウェアクラスのシステム上に、補助ディスクを用意する必要があります。
- 補助ディスクには、UNIXオペレーティングシステムとData Protectorエージェントをインストールしておく必要があります。
- 復旧するクライアントの有効なフルバックアップが必要です。

手順

1. 障害が発生したディスクを同じサイズの新しいディスクと交換します。
2. オペレーティングシステムとData Protectorクライアントがインストールされている補助ディスクをシステムに接続し、これをブートデバイスにします。
3. 補助のオペレーティングシステムからブートします。
4. 必要に応じて、論理ボリューム構造を再構築します(HP-UXシステムの場合の例: LVMを使用)。この作業には、非ルートボリュームグループのバックアップデータを使用します(HP-UXシステムの場合の例: `vgcfgrestore`または`SAM`を使用)。
5. さらに修復されたディスク上に復元するルートボリュームグループを作成します(HP-UXシステムの場合の例: `vgimport`を使用)。復元プロセス中は、補助ディスク上のオペレーティングシステムが実行されているため、このグループはルートボリュームグループのようには見えません。
6. UNIXのコマンドを使用して、新しいディスクを起動可能にします。
7. バックアップ時に二次記憶デバイスに保存したデータから、他のデータ記憶構造(ミラー、ストライピング、HPE ServiceGuardなど)を再構築します。
8. バックアップデータからの要求に従って、ファイルシステムを作成してマウントします。マウントポイントの名前には、元の名前そのものではなく、それに類似した名前を使用してください。たとえば、元の名前が`/etc_restore`であれば、`/etc`のようにします。
9. 復元するマウントポイント内のファイルを削除します。マウントポイントは空にする必要があります。
10. システムデータの復元を開始します。

DDDRを使用してシステムデータを復元する(UNIXクライアント)

最後にバックアップを実施した時点の状態にシステムを復元できます。最初にUNIXクライアントをインストールして構成する必要があります(段階1)。サポートされているオペレーティングシステムの詳細は、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。

前提条件

- 適切なオペレーティングシステムがインストールおよび構成されていること。
- Data Protectorがインストールされていること。
- 復旧するクライアントの有効なフルバックアップが必要です。
- 復元に必要なメディアが使用可能なこと。

手順

段階2

1. Data Protectorユーザーインターフェイスを開始して、Data Protector Cell Managerとの接続を開きます。

2. 補助ディスクを使って、システムをセルにインポートします。
3. 復元に使用するバックアップのバージョンを選択します。
4. [**別名で復元** *new_mountpoint*]オプションを使って、(今後)システムに対してルートボリュームとなるボリュームを含む必要なマウントポイントをすべて復元します。

   バックアップのルートボリュームは"修復ディスク"上のルートボリュームに復元されます。補助ディスク上の現在実行中の補助オペレーティングシステムに対して、何らかの復元が行われることはありません。
5. 上で復元したシステムをいったんシャットダウンしてから再起動します。
6. 補助ディスクをシステムから取り外します。
7. システムを新しい(または修復された)ディスクから再起動します。

段階3

8. Data Protectorの標準復元手順でユーザーデータとアプリケーションデータを復元します。

拡張自動ディザスタリカバリ(EADR)

Data Protectorには、Linux Data Protector Cell ManagerやLinuxクライアント用の拡張ディザスタリカバリの手順が用意されています。サポートされているオペレーティングシステムの詳細については、https://softwaresupport.hpe.com/manualsにある最新のサポート一覧を参照してください。

EADRでは、環境に関連するすべてのデータがバックアップ時に自動収集されます。クライアントシステムのフルバックアップの際に、一時DR OSのセットアップと構成に必要なデータが、1つの大きなリカバリセットファイルにパックされ、バックアップテープ(および、オプションでCell Manager上)にセル内のバックアップクライアントごとに保存されます。

イメージファイルに加え、ディスクの適切なパーティションとフォーマット作成に必要な段階1開始ファイル(P1Sファイル)がバックアップメディア上およびCell Manager上に保存されます。障害発生時には、拡張自動ディザスタリカバリウィザードを使用して、バックアップメディアからリカバリセットを復元し(フルバックアップ中にCell Managerに保存されていない場合)、それをディザスタリカバリCD ISOイメージに変換します。CD ISOイメージは、任意のCD書き込みツールを使用してCDに記録し、ターゲットシステムのブートに使用することができます。

DR OSイメージのブート後、ディスクのフォーマットとパーティション作成が自動的に実行され、最終的に、オリジナルシステムがData Protectorとともにバックアップ時の状態に復旧されます。

> **重要:**
> バックアップメディア、リカバリセットファイル、SRDファイル、ディザスタリカバリCDへのアクセスを制限しておくことをお勧めします。

概要

準備の章に記載されている一般的な準備手順すべてを実行しておく必要があります。Linuxクライアントに対して拡張自動ディザスタリカバリを行う手順の概要は、以下のとおりです。

1. **段階1**
   a. 故障したハードウェアを交換します。
   b. ディザスタリカバリCDまたはUSBフラッシュドライブからターゲットシステムをブートし、復旧範囲を選択します。完全に無人状態での復旧が可能です。
2. **段階2**
   a. 選択した復旧範囲に応じて、選択したボリュームが自動的に復元されます。重要なボリューム(ブートボリューム、ルートボリューム、Data Protectorのインストールと構成情報を含むボリューム)は常に復元されます。
3. **段階3**
   a. Data Protectorの標準復元手順で、ユーザーデータとアプリケーションデータを復元します。

> **重要:**
> 最初に復元する必要のあるクリティカルなシステム(特にDNSサーバー、Cell Manager、Media Agentクライアント、ファイルサーバーなど)のそれぞれについて、事前にDRイメージを準備します。

Cell Managerを復旧する場合は、暗号化キーを保存したリムーバブルメディアを事前に準備します。

以降の項では、Linuxクライアントの拡張自動ディザスタリカバリに関する制限事項、準備手順、および復旧手順を説明します。

要件

- この方法による復旧を可能にするシステムおよびDR OSイメージを準備するシステムには、Data Protectorの自動ディザスタリカバリコンポーネントをインストールしておく必要があります。詳細は、『*HPE Data Protectorインストールガイド*』を参照してください。
- ターゲットシステムのハードウェア構成がオリジナルシステムのハードウェア構成と同じ必要があります。これには、SCSI BIOSの設定(セクターの再マッピング)も含まれます。
- 同じバスの同じホストバスアダプターに交換用ディスクが接続されている必要があります。
- バックアップ時には、ブートパーティション上に200MBの空き領域が追加で必要になります。このディスクスペースを使用できないと、ディザスタリカバリが失敗します。
- EADRバックアップの準備中は、Data Protectorがインストールされているボリュームに少なくとも800MBの一時的な空き領域が必要です。このスペースは、一時イメージの作成に使用されます。
- システムのBIOSがEl-Torito規格に準拠した起動可能CD拡張機能をサポートしており、INT13h関数XXh経由でのLBAアドレス指定によるハードディスクドライブへの読み取り/書き込みアクセスをサポートしている必要があります。BIOSのオプションについては、システムのユーザーマニュアルを参照するか、ブート時に表示されるシステムセットアップ情報をチェックしてください。

制限事項

- 拡張自動ディザスタリカバリ(EADR)とワンボタンディザスタリカバリ(OBDR)は、Linuxシステムのみで使用できます。
- Linuxシステム上にLinuxシステム用のDR ISOイメージを作成する必要があります。他のシステム(Windowsシステム、HP-UXシステム、Solarisシステム)用のDR ISOイメージを作成することはできません。この制限事項はSRDファイルの更新や他のタスクには適用されません。

- CONFIGURATIONという名前のマウントポイントがあり、そこにSystemRecoveryDataディレクトリが含まれている場合、SystemRecoveryDataディレクトリ内のデータはバックアップされません。
- ディスクIDは一意であり、ディスクのシリアル番号によって異なるため、ディスクIDを使用してディスクをマウントしないでください。障害発生時に、ディスクを交換して新しいディスクに新しいIDを割り当てることも可能ですが、その場合は結果的にディザスタリカバリが失敗します。
- カスタムカーネルのインストールまたは構成はサポートされていません。配布で提供された元のカーネルのみがサポートされています。
- SELINUXのenforcingモードを有効にしてLinuxクライアントを復元する場合、復元後にすべてのシステムファイルの再ラベル付けを行う必要があります。システム構成によってはこの処理を完了するのに時間がかかることがあります。permissiveモードを使用すると、システムログには大量のSELINUX警告メッセージが記録されます。
- CONFIGRATION/SYSTEMRECOVERYDATAオブジェクトを選択してバックアップ仕様を作成すると、/opt/omni/bin/drim/logと/opt/omni/bin/drim/tmpフォルダーはデフォルトでバックアップから除外されます。
- このようなバックアップの整合性を保証できないので、再開されたオブジェクトバックアップを復旧に使用することはサポートされていません。
- Fusion IOディスクはMiniOSのブート時に自動的に接続されないため、復旧前に手動で接続する必要があります。この作業は、古いFusion IOディスクを新しいFUsion IOディスクに置き換えるときや、Fusion IOディスクの内部エラーが発生したときに必要となります。これらのディスクは、MiniOSに接続する前に、専用ツールでフォーマットする必要があります。Fusion IOディスクを手動でフォーマットし、システムに接続するには、復旧を開始する前にMiniOSに含まれるLinuxシェルで次のコマンドを実行する必要があります。
  - fio-status - すべてのFusion IOディスクの状態を表示します。
  - fio-format [path] - Fusion IOディスクのローレベルフォーマットを実行します。
  - fio-attach [path] - Fusion IOディスクをシステムに接続します。
- スパースファイルはオフライン復元中にフルサイズに復元されます。これにより、ターゲットボリュームのスペースが不足することがあります。
- SLES 11.3では複数のデバイスがサポートされていないので、AUTODRでは複数のデバイス上のbtrfs(さまざまなbtrfs RAID構成)の復旧はサポートされません。
- SLES 11.3で稼働する現在のbtrfsツールは、新しく作成されたbtrfsファイルシステム上でUUIDを設定しません。したがって、AUTODRはバックアップで設定したように復旧中にbtrfsファイルシステム上で同じUUIDを設定することはできません。

  デバイス名の代わりにUUIDでbtrfsファイルシステムをマウントする場合、復元後に手動で/etc/fstabファイルを編集する必要があります。この手動による編集は、復元されたbtrfsデバイスの新規の正しいUUIDを反映するために実行する必要があります。同じことがUUIDを回避するためにGRUB構成にも適用できます。

  システムの復旧後、btrfsにはバックアップ時のUUIDとは別のUUIDが割り当てられます。システムの前回の復旧前に作成されたバックアップから別の復旧を実行すると、AUTODRは正常なbtrfsファイルシステムを識別し、btrfsファイルシステムの再作成をスキップしようとします。
- AUTODRは、UUIDによって復旧されている現在のシステム内のbtrfsデバイスにバックアップ内のbtrfsデバイスの構成しかマップしない場合があります。AUTODRは間違ったデバイスや再作成されたデバイスの復旧をスキップすることがあります。

これを回避するには、btrfsファイルシステムを前回のシステムの復旧後に作成されたバックアップからのみ復旧するか、システムの復旧前に存在していたbtrfsファイルシステムを手動で破壊してください。前回のバックアップ後にユーザーが手動で再作成したbtrfsファイルシステムについても同じことが当てはまります。

> **注：**
> 復旧プロセスの開始前に、ユーザーに対してこのことを警告するメッセージが表示されます。

- btrfsスナップショットはバックアップ可能ですが、通常のサブボリュームとしてのみ復元可能です。このようなインスタンス中は、スナップショットと、スナップショットの作成元のサブボリューム間ではデータの共有はありません。親とそのスナップショットの間のすべてのコピーオンライト(COW)の関係が失われます。したがって、スナップショットからのデータが重複し、復元中に元になるデバイス上で領域不足となるため、完全なデータセットの復元ができない場合もあります。
- マウントされたbtrfsサブボリュームからのデータのみが保護されます。OSファイルシステムのインターフェイスからアクセス可能な子サブボリュームと、マウントされている親サブボリュームを考えてみてください。このような場合、Disk Agent (DA)は異なるファイルシステムとしてサブボリュームを検出し、これらのサブボリュームには専用のマウントポイントがないためにこれらをスキップしてしまうため、サブボリュームを保護しません。
- `/etc/fstab`ファイル内のマウントオプション`subvolid`(*btrfsのドキュメント*を参照)を使用してマウントしたサブボリュームは、復旧されたサブボリュームの`subvolid`はバックアップ時のものと同じである必要がないので、復旧されたシステム内のマウントからスキップされたり、間違ったマウントポイントにマウントされたりする場合があります。すべてのサブボリュームが再作成されても、HPE Data Protectorはこのようなサブボリュームでの復元をスキップするか、または間違ったサブボリューム内でデータを復元する可能性があります。

  > **注：**
  > `subvolid`の代わりに`fstab`の`subvol`オプションを使用します。

- Fibre Channel over Ethernet(FCoE)LUNおよびFibre Channel over Ethernet(FCoE)SANブートを搭載したシステムのEADRはサポートされていません。

ディスクとパーティションの構成

- 新しいディスクのサイズは、クラッシュしたディスクのサイズ以上でなければなりません。元のディスクのサイズよりも大きい場合、余った分に対しては割り当てが行われません。
- EADRでサポートされているベンダー固有のパーティションは、タイプ0x12 (EISAを含む)とタイプ0xFEだけです。

拡張自動ディザスタリカバリの準備

ディザスタリカバリを成功させるには、このトピックに記載された手順を完了する前に、すべてのディザスタリカバリ方法の一般的な準備手順に従ってください。ディザスタリカバリを迅速かつ効率的に実行するには、事前の準備作業が欠かせません。Cell Managerのディザスタリカバリの準備は、特に慎重に行う必要があります。

> **重要：**
> 障害が発生する前にディザスタリカバリを準備します。

一般的な準備作業

1. クライアントシステム全体のフルバックアップを実行します。クライアント全体のバックアップを実行することをお勧めしますが、少なくとも次の重要なボリュームとオブジェクトを選択する必要があります。
   - ブートおよびシステムボリューム
   - Data Protectorインストールボリューム
   - CONFIGURATIONオブジェクトを格納しているボリューム

   *Data Protector Cell Manager*システムの場合は、『Cell Managerのための追加の準備作業、下』を参照してください。

   『*HPE Data Protectorヘルプ*』のキーワード「バックアップ、UNIXの場合」および「バックアップ、構成」で表示される内容を参照してください。

   フルクライアントバックアップ中には、リカバリセットおよびP1Sファイルがバックアップメディアに書き込まれます。さらに、Cell Managerに書き込むように指定することもできます。
2. 障害発生後、EADRウィザードを使用してDRイメージをディザスタリカバリCD ISOイメージに変換します。
3. ISO9660形式をサポートしているCD書き込みツールを使用して、ディザスタリカバリCD ISOイメージをCDに記録します。このディザスタリカバリCDは、ターゲットシステムのブートと重要なボリュームの自動復元に使用できます。
4. ディザスタリカバリテスト計画を実施します。

Cell Managerのための追加の準備作業

Cell Managerのディザスタリカバリを成功させるには、追加の準備作業が必要になります。

- IDBを定期的にバックアップします。ファイルシステムより古いIDBセッションを指定しないでください。
- Cell ManagerのSRDファイルは、安全な場所(Cell Manager以外の場所)に保管しておいてください。
- Cell Manager用のディザスタリカバリCDイメージを事前に準備しておきます。

リカバリセットをCell Managerに保存する

リカバリセットは、大きな単一ファイルにパックされてバックアップメディアに格納され、オプションでCell Managerにも保存されます(これはフルクライアントバックアップ中に行われます)。ディザスタリカバリCDをCell Manager上で記録する場合は、リカバリセットファイルをCell Manager上のハードディスクに保存しておくと、バックアップメディアからリカバリセットを復元する場合に比べて復元速度が大幅に向上します。

バックアップ中にCell Manager上にリカバリセットファイルを保存した場合は、デフォルトのData Protector `P1S`ファイルの場所に保存されます。

デフォルトの場所を変更するには、新しいグローバルオプション`EADRImagePath = valid_path`(たとえば、`EADRImagePath = /home/images`または`EADRImagePath = C:\temp`)を指定します。

『HPE Data Protectorヘルプ』のキーワード「グローバルオプション、変更」を参照してください。

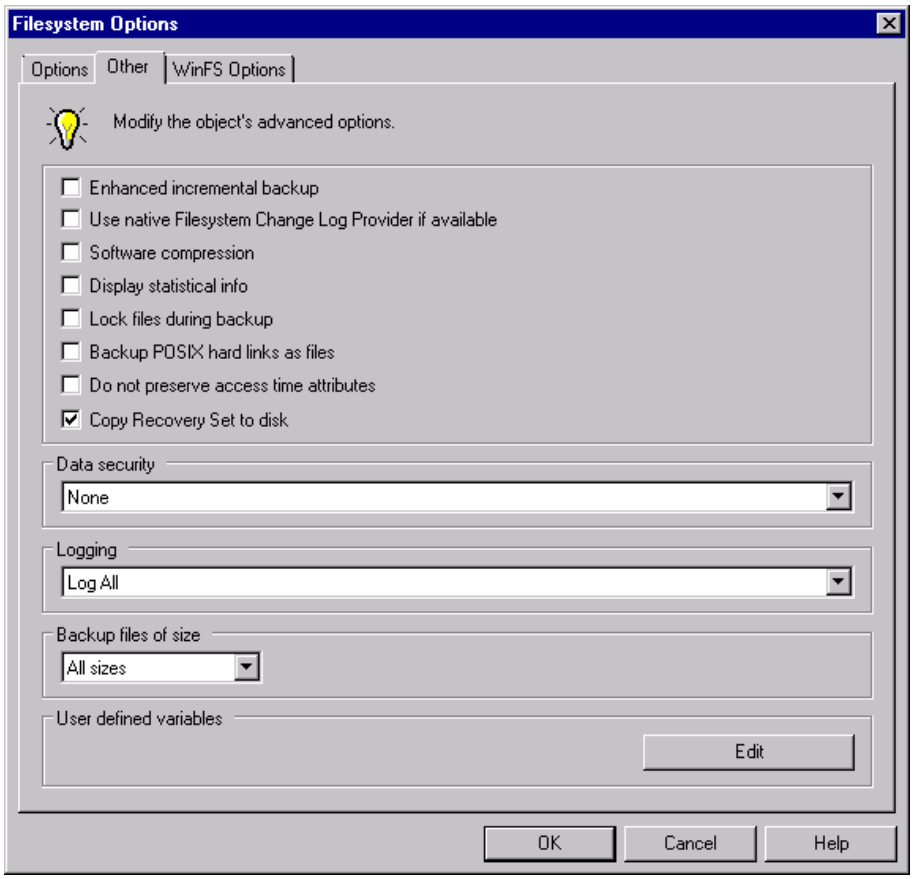
ヒント：
あて先ディレクトリに十分な空きディスクスペースがない場合には、マウントポイントを作成する(Windowsシステム)か、他のボリュームへのリンクを作成します(UNIXシステム)。

バックアップ仕様に含まれているすべてのクライアントのリカバリセットをCell Managerに保存する

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで**[バックアップ仕様]**→**[ファイルシステム]**の順に展開します。
3. フルクライアントバックアップに使用するバックアップ仕様を選択します(まだ作成していない場合は、作成してから選択します)。詳細については、『HPE Data Protectorヘルプ』のキーワード「作成、バックアップ仕様」で表示される内容を参照してください。
4. 結果エリアで**[オプション]**をクリックします。
5. **[ファイルシステムオプション]**で、**[拡張]**をクリックします。
6. **[その他]**のページで、**[リカバリセットをディスクにコピー]**を選択します。

[その他]オプションタブ



バックアップ仕様に含まれている特定のクライアントのリカバリセットをCell Managerに保存する

バックアップ仕様内の特定クライアントのリカバリセットファイルだけをコピーする場合は、以下の手順を実行します。

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで**[バックアップ仕様]**→**[ファイルシステム]**の順に展開します。
3. フルクライアントバックアップに使用するバックアップ仕様を選択します(まだ作成していない場合は、作成してから選択します)。詳細については、『HPE Data Protectorヘルプ』のキーワード「作成、バックアップ仕様」で表示される内容を参照してください。
4. 結果エリアで**[バックアップオブジェクトのサマリー]**をクリックします。
5. リカバリセットファイルをCell Managerに保存するクライアントを選択し、**[プロパティ]**をクリックします。
6. **[その他]**のページで、**[リカバリセットをディスクにコピー]**を選択します。

暗号化キーの準備

Cell Managerのリカバリまたはオフラインクライアントのリカバリに対しては、暗号化キーをリムーバブルメディアに保存して、ディザスタリカバリの際に使用できるようにする必要があります。Cell Managerのリカバリの場合は、障害が発生する前に、あらかじめリムーバブルメディアを準備してください。

暗号化キーは、DR OSイメージファイルの一部ではありません。ディザスタリカバリイメージの作成において、キーは自動的にCell Managerへ、ファイル*Data_Protector_program_data*\Config\Server\export\keys\DR-*ClientName*-keys.csv(Windowsシステム)または/var/opt/omni/server/export/keys/DR-*ClientName*-keys.csv(UNIXシステム)にエクスポートされます。*ClientName*はイメージが作成されているクライアント名となります。

ディザスタリカバリのために準備したバックアップごとに、正しい暗号化キーがあることを確認します。

DR OSイメージを準備する

障害が発生する前に、ディザスタリカバリCDに記録または起動可能なUSBドライブに保存するためのDR OSイメージを準備する必要があります。このDR OSイメージは、後で拡張自動ディザスタリカバリに使用できます。または、起動可能なネットワークイメージを準備することができます。

DR OSイメージを準備するシステムには、Data Protectorの自動ディザスタリカバリコンポーネントをインストールしておく必要があります。

ハードウェア、ソフトウェア、または構成の変更を行った場合には、その都度新しいディザスタリカバリOSを準備する必要があります。

最初に復元する必要のある重要システムのそれぞれについて、DR OSイメージを事前に準備します。特に、ネットワークが正しく機能するために必要なシステム(DNSサーバー、ドメインコントローラー、ゲートウェイなど)、Cell Manager、Media Agentクライアント、ファイルサーバーなどです。

バックアップメディア、およびOSイメージが格納されているディザスタリカバリCDまたはUSBドライブへのアクセスは、セキュリティ維持のため制限しておくことをお勧めします。

手順

1. Data Protectorコンテキストリストで**[復元]**をクリックします。
2. Scopingペインで**[タスク]**をクリックし、**[ディザスタリカバリ]**をクリックしてディザスタリカバリウィザードを開始します。
3. [結果]エリアで、**[復旧するホスト]**ドロップダウンリストからDR OSイメージを準備するクライアントを選択し、**[検証]**をクリックしてクライアントを検証します。

   > **注:**
   > 検証されたクライアントは**[復旧するホスト]**ドロップダウンリストに追加されます。

4. **[リカバリメディア作成ホスト]**ドロップダウンリストから、DR OSイメージを準備するクライアントを選択します。デフォルトでは、これはDR OSイメージを準備するクライアントと同じクライアントになっています。DR OSイメージを準備するクライアントには、同じOSタイプ(Windows、Linux)をインストールし、またDisk Agentをインストールしておく必要があります。
5. **[拡張自動ディザスタリカバリ]**を選択しておき、ボリュームリカバリセットをバックアップセッションから作成するか、ボリュームのリストから作成するかを選択します。デフォルトでは、**[バックアップセッション]**が選択されています。

   [次へ]をクリックします。
6. リカバリセットの作成方法によって、以下を選択します。
   - バックアップセッションを選択した場合、ホストバックアップセッションを選択します。Cell Managerの場合はIDBセッションを選択します。
   - ボリュームのリストを選択した場合は、重要な各オブジェクトに対して、適切なオブジェクトのバージョンを選択します。

   [次へ]をクリックします。
7. リカバリセットファイルの場所を選択します。デフォルトで、**[バックアップからリカバリセットファイルを復元]**が選択されています。

   バックアップ中にCell Manager上にリカバリセットファイルを保存した場合は、**[リカバリセットファイルへのパス]**を選択してその場所を指定します。**[次へ]**をクリックします。
8. イメージ形式を選択します。以下のオプションを使用できます。
   - **起動可能ISOイメージの作成**: DR ISOイメージ(デフォルトで、`recovery.iso`)
   - **起動可能USBドライブの作成:起動可能なUSBドラ**イブ上のDR OSイメージ
   - **起動可能ネットワークイメージの作成**: ネットワークブートに使用可能なDR OSイメージ(デフォルトで、`recovery.wim`)
9. 起動可能なISOイメージまたは起動可能なネットワークイメージを作成する場合、作成したイメージの保存先となるディレクトリを選択します。

   起動可能なUSBドライブを作成する場合、作成したイメージの保存先となるUSBドライブまたはディスク番号を選択します。

   > **重要:**
   > 起動可能なUSBドライブの作成時には、ドライブ上に格納されたすべてのデータが消失し

> ます。

10. また、パスワードを設定して、DR OSイメージを不正使用から保護することもできます。鍵アイコンが、パスワードが設定されていることを示します。

    [パスワード]をクリックして[イメージのパスワード保護]ダイアログウィンドウを開き、パスワードを入力します。パスワードを削除するには、このフィールドをクリアします。
11. **[完了]**をクリックしてウィザードを終了します。これにより、DR OSイメージが作成されます。
12. 起動可能なCDまたはDVDを作成する場合は、ISO9660形式をサポートしている記録ツールを使用して、ISOイメージをCDまたはDVDに記録します。

EADRを使用してLinuxシステムを復旧する

Linuxシステムの拡張自動ディザスタリカバリを成功させるには、事前にすべての準備手順を完了しておかなければなりません。Cell Managerを準備する場合、まず内部データベースがそのバックアップイメージから復元され、その次にボリュームとCONFIGURATIONオブジェクトがそのバックアップイメージから復元されます。サポートされているオペレーティングシステムの詳細は、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。

前提条件

- 影響があったディスクと交換するための新しいハードディスクが必要です。
- 復元するシステム全体の有効なフルファイルシステムバックアップ(クライアントバックアップ)が必要です。
- Cell Managerのディザスタリカバリでは、ファイルシステムバックアップイメージより新しい有効な内部データベースバックアップイメージが必要です。
- ディザスタリカバリCDが必要です。

手順

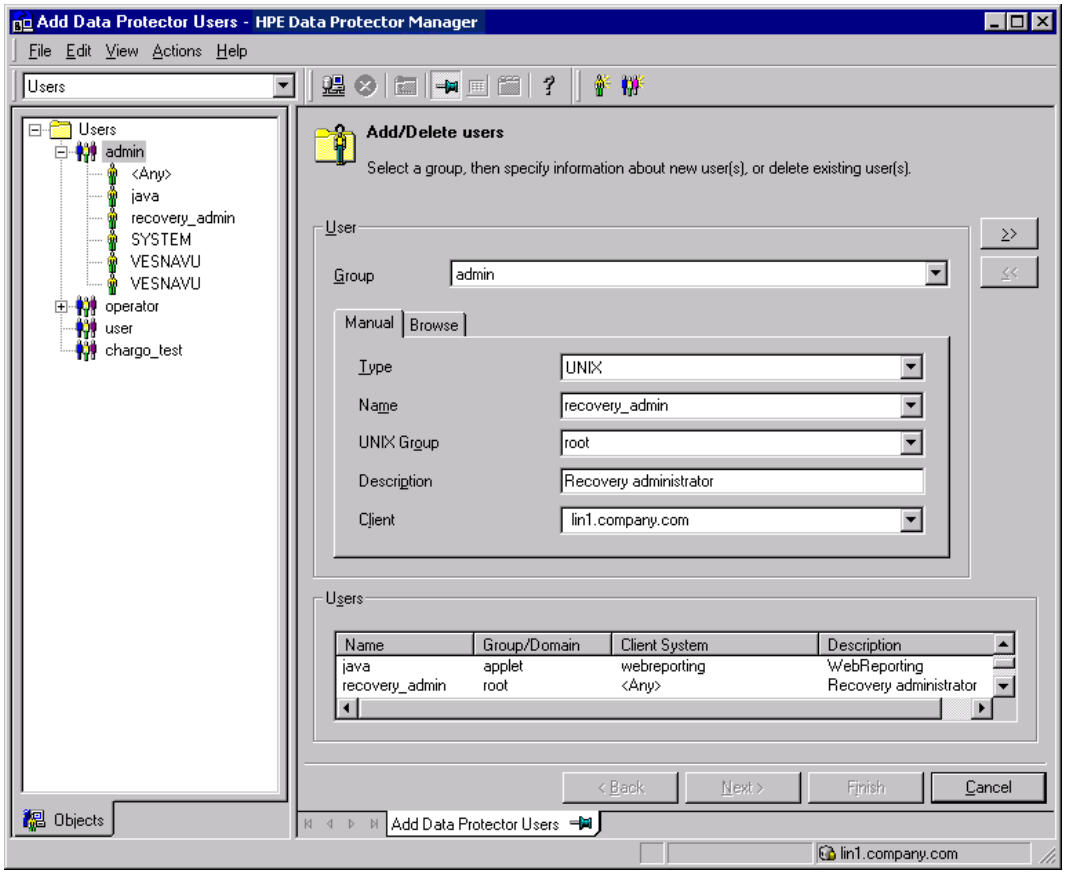
段階1

1. オフラインディザスタリカバリを行う場合を除き、Cell Manager上のData Protectorの`admin`ユーザーグループに、以下のプロパティを持つData Protector `admin`アカウントを追加します。
   - 復元の開始
   - 別のクライアントへ復元
   - ルートユーザーとして復元

   > **注：**
   > ディザスタリカバリ手順を実行できるのは、ルートユーザーのみです。

   ユーザーの追加方法の詳細については、『HPE Data Protectorヘルプ』のキーワード「Data Protectorユーザーの追加」で表示される内容を参照してください。

   ユーザーアカウントの追加



2. オリジナルシステムのディザスタリカバリCDからクライアントシステムをブートします。
3. 次のメッセージが表示されたら**[Enter]**キーを押します。[Enter]キーを押してリカバリCDからブートしてください。
4. 先にDR OSがメモリにロードされてから、範囲メニューが表示されます。復旧の対象範囲を選択します。4つの異なる復旧対象範囲があり、2つの追加オプションがあります。
   - `Reboot`: ディザスタリカバリは実行されず、コンピューターが再起動されます。
   - `Default Recovery`: Data Protectorインストールファイルと構成ファイルが格納されている`/boot`ボリュームと/(ルート)ボリューム(`/opt`、`/etc`、および`/var`)を復旧します。他のすべてのディスクはパーティション作成やフォーマットが行われず、段階3に備えた状態になります。
   - `Minimal Recovery`: `/boot`//(ルート)ボリュームだけが復旧されます。
   - `Full Recovery`: 重要なボリュームだけでなく、すべてのボリュームが復元されます。
   - `Full with Shared Volumes`: ボリュームがすべて復旧されます。バックアップ時にロックされていた共有ボリュームもこれに含まれます。
   - `Run shell`: Linuxシェルを実行します。これは、詳細な構成や復旧タスクに使用できます。

> **注：**
> 選択した復旧範囲(デフォルト、最小限、または完全な復旧)に関係なく、すべてのBTRFS

> ボリュームおよびサブボリュームがディザスタリカバリによって復旧されます。

段階2

5. ディザスタリカバリウィザードが表示されます。ディザスタリカバリオプションを変更するには、カウントダウン中に任意のキーを押してウィザードを停止した後、オプションを変更します。ディザスタリカバリを続行するには、**[復元の実行]**を選択します。

   > **注: 注記**: Cell Managerとメディア(バックアップ)ホストに到達できることを確認します。到達できない場合、NICおよびMACアドレスを修正する必要があります。詳細については、Cell ManagerとRMAホストが応答しないを参照してください。

6. ディザスタリカバリバックアップが暗号化され、Cell ManagerまたはCell Managerにアクセスできないクライアントを復元している場合、以下のプロンプトが表示されます。

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   [y]キーを押します。

   クライアントでキーストア(DR-*ClientName*-keys.csv)が使用できるようにします(たとえば、CD-ROM、フロッピーディスク、またはUSBフラッシュドライブを挿入します)。その後、キーストアファイルへのフルパスを入力します。キーストアファイルは、DR OSのデフォルトの場所にコピーされ、Disk Agentによって使用されます。以降は何の操作も必要なく、ディザスタリカバリが続行されます。
7. SRDファイル内の情報が最新でない場合(たとえば、障害後にバックアップデバイスを変更したなどの場合)、オフライン復旧を実行するには、この手順を続行する前にSRDファイルを編集します。
8. Data Protector選択した復旧対象範囲内で以前の記憶域構造が再確立され、重要なボリュームがすべて復元されます。

   Data Protectorは、最初にオンライン復旧を実行しようとします。Cell Managerまたはネットワークサービスが使用できない、あるいはファイアウォールによりCell Managerへのアクセスが拒否されるなどの理由でオンライン復旧が失敗すると、リモートオフライン復旧が試みられます。Data Protectorリモートオフライン復旧も失敗した場合(Media Agentホストがcell Managerからの要求しか受け付けないなど)、ローカルオフライン復旧が実行されます。Data Protector
9. 手順1で作成したクライアントのローカルData ProtectorアカウントをCell ManagerのData Protector adminユーザーグループから削除します(ディザスタリカバリ前にそのアカウントがCell Manager上に存在していた場合を除く)。
10. Cell Managerを復旧する場合は、IDBの整合性を確保します。

段階3

11. Data Protectorの標準復元手順でユーザーデータとアプリケーションデータを復元します。
12. クラスターですべてのノードのディザスタリカバリを実行する場合は、追加作業が必要になります。

ワンボタンディザスタリカバリ(OBDR)

ワンボタンディザスタリカバリ(OBDR)とは、Linux Data Protectorクライアント用に自動化されたData Protector復旧方法で、ユーザーの操作は最小限に抑えられています。サポートされているオペレーティングシステムの詳細については、https://softwaresupport.hpe.com/manualsにある最新のサポート一覧を参照してください。

OBDRでは、環境に関連するすべてのデータがバックアップ時に自動収集されます。バックアップの際に、一時DR OSのセットアップと構成に必要なデータが、1つの大きなOBDRイメージファイル(リカバリセット)にパックされ、バックアップテープに保存されます。障害が発生した場合には、OBDRデバイス(CD-ROMをエミュレートできるバックアップデバイス)を使用して、OBDRイメージファイルとディザスタリカバリ情報を含むテープからターゲットシステムを直接ブートします。

Data Protectorその後、ディザスタリカバリオペレーティングシステム(DR OS)が実行され構成されます。ディスクのパーティションとフォーマット作成も実行され、最終的に、オリジナルのオペレーティングシステムがData Protectorとともにバックアップ時の状態に復旧されます。

> **重要:**
> ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行します。これは、IPアドレスやDNSサーバーの変更など、ネットワーク構成が変更された場合も同じです。

OBDRの手順では、選択した復旧範囲に応じてボリュームが復旧されます。

その他のボリュームは、Data Protectorの標準復元手順で復旧できます。

概要

準備の章に記載されている一般的な準備手順すべてを実行しておく必要があります。Windowsクライアントに対してワンボタンディザスタリカバリを行う手順の概要は、以下のとおりです。

1. **段階1**
   復旧用テープからブートし、復旧範囲を選択します。
2. **段階2**
   選択した復旧範囲に応じて、選択したボリュームが自動的に復元されます。
   クリティカルボリューム(ブートパーティションとオペレーティングシステム)は常に復元されます。
3. **段階3**
   Data Protector標準復元手順を使用して、残りのパーティションを復元します。

> **重要:**
> OBDRブートメディアへのアクセスを制限することをお勧めします。

以下の項で、Windowsシステム上でのワンボタンディザスタリカバリに関する必要条件、制限事項、準備、および、復旧について説明します。

要件

- この方法による復旧を可能にするシステムには、Data Protectorの自動ディザスタリカバリコンポーネントをインストールしておく必要があります。また、DR OSイメージを準備するシステムには、自動ディザスタリカバリコンポーネントをインストールしておく必要があります。詳細は、『*HPE Data Protectorインストールガイド*』を参照してください。
- クライアントシステムは、OBDRで使用するテープデバイスからのブートをサポートする必要があります。
  サポートされるシステム、デバイス、メディアの詳細については、HPEのテープとハードウェアの互換性一覧表および最新のサポート一覧(https://softwaresupport.hpe.com/manuals)を参照してください。
- ターゲットシステムのハードウェア構成がオリジナルシステムのハードウェア構成と同じ必要があります。

これには、SCSI BIOSの設定(セクターの再マッピング)も含まれます。

- 同じバスの同じホストバスアダプターに交換用ディスクが接続されている必要があります。
- Data Protectorがインストールされているボリュームの空きスペースは800MB以上でなければなりません。このスペースは、一時イメージの作成に使用されます。
- メディアの使用ポリシーが[追加不可能]でメディア割り当てポリシーが[緩和]のメディアプールをOBDR対応のデバイスに対して作成する必要があります。ディザスタリカバリに使用できるメディアは、このプールに所属しているメディアだけとなります。
- SANブート構成では、ターゲットシステムの次の項目が、オリジナルシステムの項目と同一であることを確認します。
  - ローカルのHBAのBIOSパラメーター
  - SANディスクのLUN数
- マルチパスSANディスク構成では、ターゲットシステムのディスクのLUNとWWIDはオリジナルシステムのディスクのLUNとWWIDと同一でなければなりません。

制限事項

- ワンボタンディザスタリカバリ(OBDR)は、Data Protector Cell Managerでは使用できません。
- ワンボタンディザスタリカバリバックアップセッションは、同じOBDRデバイス上で一度に1つのクライアントまたはCell Managerに対してのみ実行できます。このセッションは、ローカルに接続された単一のOBDR対応デバイスに対して実行する必要があります。
- USBテープストレージデバイスはサポートされていません。
- `CONFIGURATION`という名前のマウントポイントがあり、そこに`SystemRecoveryData`ディレクトリが含まれている場合、`SystemRecoveryData`ディレクトリ内のデータはバックアップされません。
- ディスクIDは一意であり、ディスクのシリアル番号によって異なるため、ディスクIDを使用してディスクをマウントしないでください。障害発生時に、ディスクを交換して新しいディスクに新しいIDを割り当てることも可能ですが、その場合は結果的にディザスタリカバリが失敗します。
- SELINUXのenforcingモードを有効にしてLinuxクライアントを復元する場合、復元後にすべてのシステムファイルの再ラベル付けを行う必要があります。システム構成によってはこの処理を完了するのに時間がかかることがあります。permissiveモードを使用すると、システムログには大量のSELINUX警告メッセージが記録されます。
- CONFIGRATION/SYSTEMRECOVERYDATAオブジェクトを選択してバックアップ仕様を作成すると、`/opt/omni/bin/drim/log`と`/opt/omni/bin/drim/tmp`フォルダーはデフォルトでバックアップから除外されます。
- Fusion IOディスクはMiniOSのブート時に自動的に接続されないため、復旧前に手動で接続する必要があります。この作業は、古いFusion IOディスクを新しいFUsion IOディスクに置き換えるときや、Fusion IOディスクの内部エラーが発生したときに必要となります。これらのディスクは、MiniOSに接続する前に、専用ツールでフォーマットする必要があります。Fusion IOディスクを手動でフォーマットし、システムに接続するには、復旧を開始する前にMiniOSに含まれるLinuxシェルで次のコマンドを実行する必要があります。
  - `fio-status` - すべてのFusion IOディスクの状態を表示します。
  - `fio-format [path]` - Fusion IOディスクのローレベルフォーマットを実行します。

- `fio-attach [path]` - Fusion IOディスクをシステムに接続します。

- スパースファイルはオフライン復元中にフルサイズに復元されます。これにより、ターゲットボリュームのスペースが不足することがあります。

ディスクとパーティションの構成

- 新しいディスクのサイズは、クラッシュしたディスクのサイズ以上でなければなりません。元のディスクのサイズよりも大きい場合、余った分に対しては割り当てが行われません。
- OBDRでサポートされているベンダー固有のパーティションは、タイプ0x12 (EISAを含む)とタイプ0xFEだけです。

ワンボタンディザスタリカバリの準備

ディザスタリカバリを成功させるには、このトピックに記載された手順を完了する前に、ディザスタリカバリ方法の一般的な準備手順に従ってください。ディザスタリカバリを迅速かつ効率的に実行するには、事前の準備作業が欠かせません。

> **重要：**
> 障害が発生する前にディザスタリカバリを準備します。

準備手順

ディザスタリカバリの一般的な準備を完了したら、以下の手順に従ってOBDRの準備をします。

1. DDSメディアまたはLTOメディア用として、メディアプールを作成します。メディア使用ポリシーは**[追加不可能]**、メディア割り当てポリシーは**[緩和]**(バックアップメディアはOBDRバックアップ時にフォーマットされるため)です。さらに、このメディアプールをOBDRデバイスのデフォルトのメディアプールに指定します。『*HPE Data Protectorヘルプ*』のキーワード「メディアプールの作成」で表示される内容を参照してください。このプールのメディアのみが、OBDRで使用できます。
2. OBDRを使用する復旧を可能にするシステム上で、OBDRバックアップをローカルに実行します。

   フルクライアントバックアップが暗号化されている場合は、ディザスタリカバリで使用できるように暗号キーをリムーバブルメディアに格納します。Cell Managerへの接続を確立できない場合このキーが必要になります。
3. ディザスタリカバリテスト計画を実施します。

ワンボタンディザスタリカバリ用のバックアップ仕様を作成する

利用者は、OBDRブートテープを準備するためにワンボタンディザスタリカバリ(OBDR)のバックアップ仕様を作成する必要があります。

前提条件

- OBDRデバイスを追加する前に、DDSまたはLTOメディア用のメディアプールを作成します。使用ポリシーは[追加不可能]、メディア割り当てポリシーは[緩和]です。このメディアプールは、OBDRデバイス用のデフォルトメディアプールとして選択する必要があります。

- デバイスは、OBDRによる復旧を可能にしたいシステムにローカルに接続する必要があります。
- OBDRによる復旧を可能にしたいシステムには、Data Protectorの自動ディザスタリカバリコンポーネントとユーザーインターフェイスコンポーネントをインストールしておく必要があります。
- このバックアップ仕様は、OBDRによる復旧を可能にしたいシステム上でローカルに作成する必要があります。

> **ヒント：**
> OBDRブートテープを準備するノードにすべてのボリュームを一時的に移動しておくと、MS Cluster内のすべての共有ディスクボリュームをOBDRで自動的に復元できるようになります。他のノードによってロックされる共有ディスクボリュームに関しては、段階1でディスクの構成に十分な情報を収集するのは事実上不可能です。

制限事項

- ワンボタンディザスタリカバリ(OBDR)は、Data Protector Cell Managerでは使用できません。

OBDR用のバックアップ仕様を作成する

手順

1. Data Protectorコンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで**[タスク]**をクリックし、次に**[ワンボタンディザスタリカバリウィザード]**をクリックします。
3. [結果エリア]で、OBDRバックアップのローカル実行の対象となるクライアントをドロップダウンリストから選択し、**[次へ]**をクリックします。
4. 必ずバックアップしなければならない重要なボリュームは既に選択されています。**[次へ]**をクリックします。

   > **重要：**
   > 重要なボリュームは自動的に選択されており、これらを選択解除することはできません。なお復旧手順を実行すると、システム上のすべてのパーティションがData Protectorにより削除されるため、そのほかにも保存が必要なパーティションがあれば、ここで選択しておいてください。

5. バックアップに使用するローカルなデバイスまたはドライブを選択します。ここでは1つのデバイスまたはドライブしか選択できません。**[次へ]**をクリックします。
6. バックアップオプションを選択します。使用可能なオプションの詳細については、『*HPE Data Protectorヘルプ*』のキーワード「バックアップオプション」で表示される内容を参照してください。
7. [バックアップサマリー]ページでバックアップ仕様の設定を確認し、**[次へ]**をクリックします。

   > **注：**
   > あらかじめ選択されているバックアップデバイスを変更したり、バックアップ仕様の実行順序を変更したりすることはできません。ここでは必須でないOBDRバックアップオブジェクトの削除と、一般的なオブジェクトプロパティの確認のみが可能です。
   >
   > また、バックアップオブジェクトの説明は変更も可能です。

8. バックアップウィザードの最終ページでは、バックアップ仕様の保存、バックアップの保存とスケジュール、対話型バックアップの開始、またはバックアップのプレビューを行うことができます。

バックアップ仕様を一度保存すると、編集が可能になります。バックアップ仕様を右クリックして、[プロパティ]を選択します。変更されたバックアップ仕様を、Data Protectorの標準バックアップ仕様またはOBDRバックアップ仕様として扱うことができます。変更されたバックアップ仕様をOBDRバックアップ仕様として保存すると、そのバックアップ仕様のOBDRに固有のオプションが上書きされなくなります。標準のバックアップ仕様として保存すると、OBDRに使用できなくなることがあります。

9. [バックアップ開始]をクリックして、バックアップを対話形式で実行します。[バックアップ開始]ダイアログボックスが表示されます。[OK]をクリックしてバックアップを開始します。

   バックアップが暗号化されている場合、実行後コマンドとして実行されるomnisrdupdateユーティリティによって暗号化IDが自動的にエクスポートされます。

一時DR OSのインストールと構成に必要な情報がすべて含まれているシステム用ブート可能イメージはテープの先頭に書き込まれ、これによりテープからのブートが可能となります。

> **重要：**
> ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行してブート可能なバックアップメディアを作成します。これは、IPアドレスやDNSサーバーの変更など、ネットワーク構成が変更された場合も同じです。

暗号化キーの準備

Cell Managerのリカバリまたはオフラインクライアントのリカバリに対しては、暗号化キーをリムーバブルメディアに保存して、ディザスタリカバリの際に使用できるようにする必要があります。Cell Managerのリカバリの場合は、障害が発生する前に、あらかじめリムーバブルメディアを準備してください。

暗号化キーは、DR OSイメージファイルの一部ではありません。ディザスタリカバリイメージの作成において、キーは自動的にCell Managerへ、ファイル*Data_Protector_program_data*\Config\Server\export\keys\DR-*ClientName*-keys.csv(Windowsシステム)または/var/opt/omni/server/export/keys/DR-*ClientName*-keys.csv(UNIXシステム)にエクスポートされます。*ClientName*はイメージが作成されているクライアント名となります。

ディザスタリカバリのために準備したバックアップごとに、正しい暗号化キーがあることを確認します。

OBDRを使用してLinuxシステムを復旧する

Linuxシステムのワンボタンディザスタリカバリ(OBDR)を成功させるには、事前にすべての準備手順を完了しておかなければなりません。

OBDR用にサポートされているオペレーティングシステムの詳細は、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。

前提条件

- 影響があったディスクと交換するための新しいハードディスクが必要です。
- 復旧するクライアントの重要なオブジェクトをすべて含む起動可能なOBDRバックアップメディアが必要です。OBDRバックアップは、クライアントでローカルに実行する必要があります。
- OBDRデバイスがターゲットシステムにローカルに接続されている必要があります。

手順

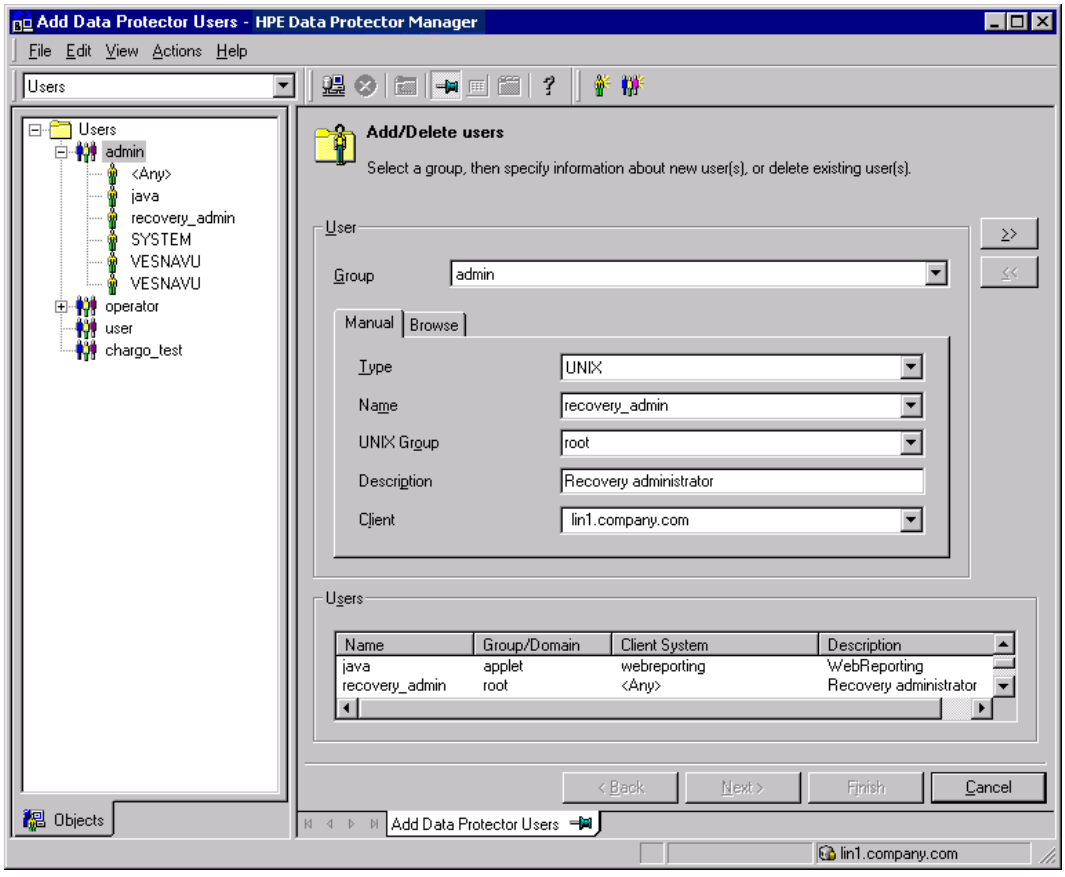
段階1

1. オフラインディザスタリカバリを行う場合を除き、ターゲットシステムのオペレーティングシステムに応じて、Cell Manager上のData Protector `admin`ユーザーグループに、以下のプロパティを持つData Protector `admin`アカウントを追加します。
   - 復元の開始
   - 別のクライアントへ復元
   - ルートユーザーとして復元

   > **注：**
   > ディザスタリカバリ手順を実行できるのは、ルートユーザーのみです。

   ユーザーの追加方法の詳細については、『HPE Data Protectorヘルプ』のキーワード「Data Protectorユーザーの追加」で表示される内容を参照してください。

   ユーザーアカウントの追加



2. イメージファイルとバックアップデータが格納されたテープをOBDRデバイスに挿入します。

3. ターゲットシステムをシャットダウンし、テープデバイスの電源を切ります。
4. ターゲットシステムの電源を入れます。ターゲットシステムが初期化されている間に、テープデバイス上の取り出しボタンを押してテープデバイスの電源を入れます。詳細については、デバイスのドキュメントを参照してください。
5. 先にDR OSがメモリにロードされてから、範囲メニューが表示されます。復旧の対象範囲を選択します。4つの異なる復旧対象範囲があり、2つの追加オプションがあります。
   - `Reboot`: ディザスタリカバリは実行されず、コンピューターが再起動されます。
   - `Default Recovery`: Data Protectorインストールファイルと構成ファイルが格納されている`/boot`ボリュームと/(ルート)ボリューム(`/opt`、`/etc`、および`/var`)を復旧します。他のすべてのディスクはパーティション作成やフォーマットが行われず、段階3に備えた状態になります。
   - `Minimal Recovery`: `/boot`//(ルート)ボリュームだけが復旧されます。
   - `Full Recovery`: 重要なボリュームだけでなく、すべてのボリュームが復元されます。
   - `Full with Shared Volumes`: ボリュームがすべて復旧されます。バックアップ時にロックされていた共有ボリュームもこれに含まれます。
   - `Run shell`: Linuxシェルを実行します。これは、詳細な構成や復旧タスクに使用できます。

段階2

6. ディザスタリカバリウィザードが表示されます。ディザスタリカバリオプションを変更するには、カウントダウン中に任意のキーを押してウィザードを停止した後、オプションを変更します。ディザスタリカバリを続行するには、[復元の実行]を選択します。
7. ディザスタリカバリバックアップが暗号化され、Cell Managerにアクセスできないクライアントを復元している場合、以下のプロンプトが表示されます。

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   [y]キーを押します。

   クライアントでキーストア(`DR-ClientName-keys.csv`)が使用できるようにします(たとえば、CD-ROM、フロッピーディスク、またはUSBフラッシュドライブを挿入します)。その後、キーストアファイルへのフルパスを入力します。キーストアファイルは、DR OSのデフォルトの場所にコピーされ、Disk Agentによって使用されます。以降は何の操作も必要なく、ディザスタリカバリが続行されます。
8. SRDファイル内の情報が最新でない場合(たとえば、障害後にバックアップデバイスを変更したなどの場合)、オフライン復旧を実行するには、この手順を続行する前にSRDファイルを編集します。
9. Data Protector選択した復旧対象範囲内で以前の記憶域構造が再確立され、重要なボリュームがすべて復元されます。

   Data Protectorは、最初にオンライン復旧を実行しようとします。Cell Managerまたはネットワークサービスが使用できない、あるいはファイアウォールによりCell Managerへのアクセスが拒否されるなどの理由でオンライン復旧が失敗すると、Data Protectorによってリモートオフライン復旧が試みられます。Media Agentホストが Cell Managerからの要求しか受け付けないなどの理由でリモートオフライン復元にも失敗すると、ローカルオフライン復元が実行されます。Data Protector
10. 手順1で作成したクライアントのローカルData ProtectorアカウントをCell ManagerのData Protector `admin`ユーザーグループから削除します(ディザスタリカバリ前にそのアカウントがCell Manager上に存在していた場合を除く)。

段階3

11. Cell Managerを復旧する場合、または拡張復旧タスク(SRDファイルの編集など)を行う場合は、特別な手順が必要になります。
12. Data Protectorの標準復元手順でユーザーデータとアプリケーションデータを復元します。

第5章: ディザスタリカバリのトラブルシューティング

この章では、ディザスタリカバリの実行中に発生する可能性がある問題について説明します。問題の発生時には、まず、ある特定のディザスタリカバリの方法に関連する問題かどうかを検討した後、ディザスタリカバリ全般の問題かどうかを検討してください。エラーメッセージの確認方法については、ディザスタリカバリのトラブルシューティング、上を参照してください。

Data Protectorのトラブルシューティング全般については、『HPE Data Protectorトラブルシューティングガイド』を参照してください。

開始する前に

- 最新のData Protectorパッチがインストールされていることを確認してください。確認方法については、『HPE Data Protectorヘルプ』のキーワード「パッチ」で表示される内容を参照してください。
- Data Protectorの全般的な制限事項、既知の問題、および対処方法については、『HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照してください。
- 対応するバージョン、プラットフォーム、その他の情報の最新一覧については、https://softwaresupport.hpe.com/manualsを参照してください。

自動ディザスタリカバリのトラブルシューティング

AUTODR.logファイル

自動ディザスタリカバリには、EADRとOBDRの2つの障害復旧方法があります。これらの方法に関連するメッセージは、デフォルトのData Protector一時ファイルディレクトリ内のAUTODR.logファイルに記録されます。エラーが発生した場合は、このファイルを調べてください。

AUTODR.logには、主に開発およびサポート用のさまざまなメッセージが記録されます。実際に関係があり、エラーが発生したことを示しているメッセージは、そのうちの一部だけです。通常、これらのエラーメッセージはログファイルの末尾に記録され、tracebackが追加されます。

AUTODR.logファイルのメッセージには4つのレベルがあります。それらのレベルは、Data Protector GUIのバックアップセッションの最後に報告されるメッセージのレポートレベルには対応していません。

- Critical error: 深刻なエラーで、オブジェクトのバックアップは続行不可能であり、中止されます。
- Error: エラーが発生しましたが、重大なエラーであるかどうかはさまざまな要因によって異なります。

  たとえば、AUTODR.logに、あるドライバーがDR OSに含まれていないことが記録されていたとします。復旧したシステムが復旧後に動作しないのは、ドライバーが見つからないことが原因である可能性があります。また、一部の重要でないサービスがオペレーティングシステムのブート後に稼動されていないことが原因である可能性もあります。エラーの重大性は、どのドライバーがバックアップされていないのかによって異なります。
- Warning およびInfo。これらはエラーメッセージではなく、通常は何らかの障害を意味するものではありません。

AUTODR.logファイルに記録される最も一般的なメッセージは、次の2種類です。

- unsupported location: DR OSに含まれるサービスまたはドライバーに必要なファイルが*%SystemRoot%*ディレクトリに存在しないことをData Protectorが示します。

  多くの場合、そのようなドライバーはウィルス対策ソフトウェアやリモートコントロールソフトウェアによって使用されます(pcAnywhereなど)。見つからないファイルを必要とするサービスまたはドライバーがブート後に起動しないことを示している可能性があるため、このメッセージは重要です。ディザスタリカバリが成功するかどうかは、影響を受けるサービスまたはドライバーによって異なります。この問題に対して考えられる解決方法は、不足しているファイルを*%SystemRoot%*ディレクトリにコピーし、Windowsレジストリ内のそのパスを変更することです。Windowsレジストリを不正に編集すると、システムが深刻なダメージを受ける可能性があることに注意してください。

ディザスタリカバリセッションのデバッグ

ディザスタリカバリセッションの際のデバッグ設定とデバッグログの場所は、以下のようにディザスタリカバリ段階によって異なります。

- DR OSの準備中は、デバッグログはX:\$DRM$\log(Windows Vista以降のリリースの場合)、c:\$DRM$\log(Windows XP、Windows Server 2003の場合)、または/opt/omni/bin/drim/log/Phase1.log(Linuxシステムの場合)に自動的に保存されます。
- データ復元手順の際は、ディザスタリカバリウィザードで手動でデバッグオプションを選択して、デバッグを有効にする必要があります。

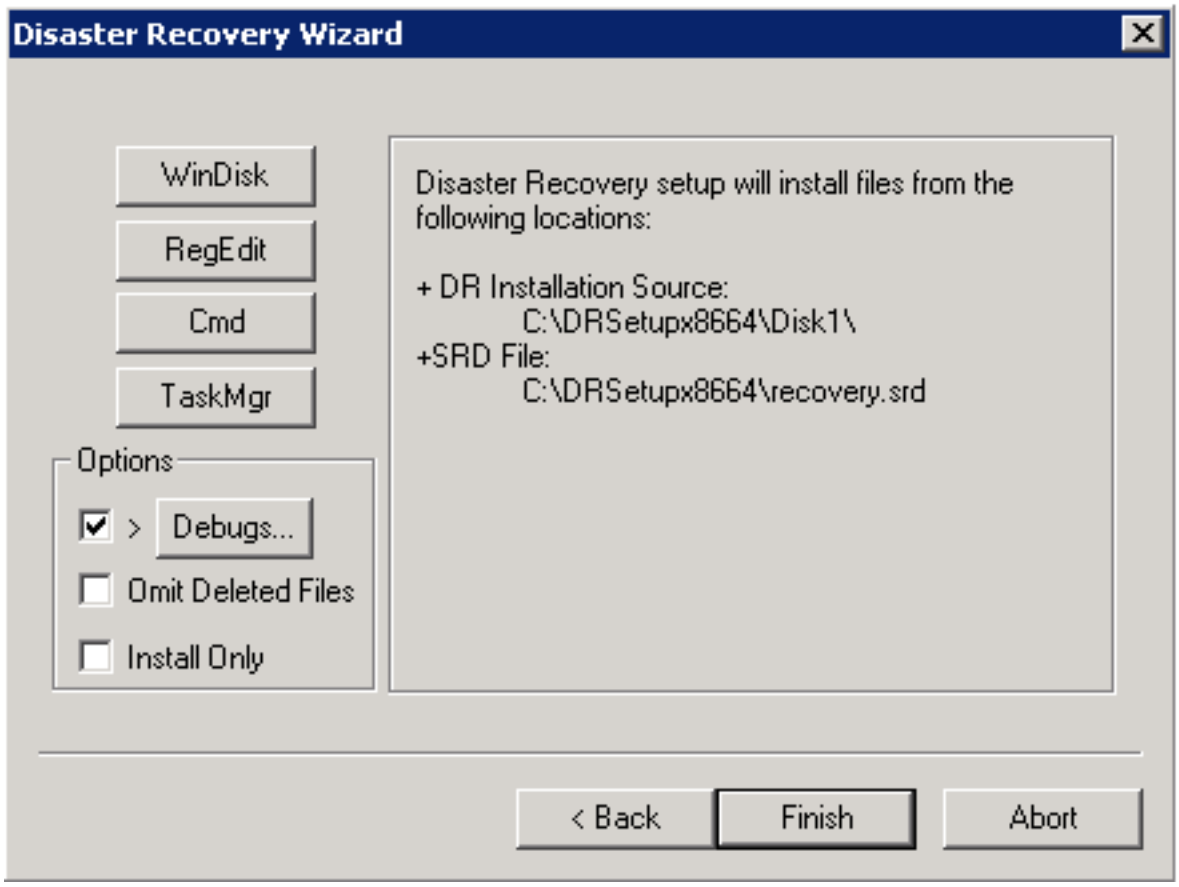
Windows

デバッグログの作成を有効にするには:

1. ディザスタリカバリウィザードで、カウントダウン中に任意のキーを押してウィザードを停止します。

   [デバッグ]ボタンの左のチェックボックスを選択します。

   ディザスタリカバリセッション中のデバッグを有効にする

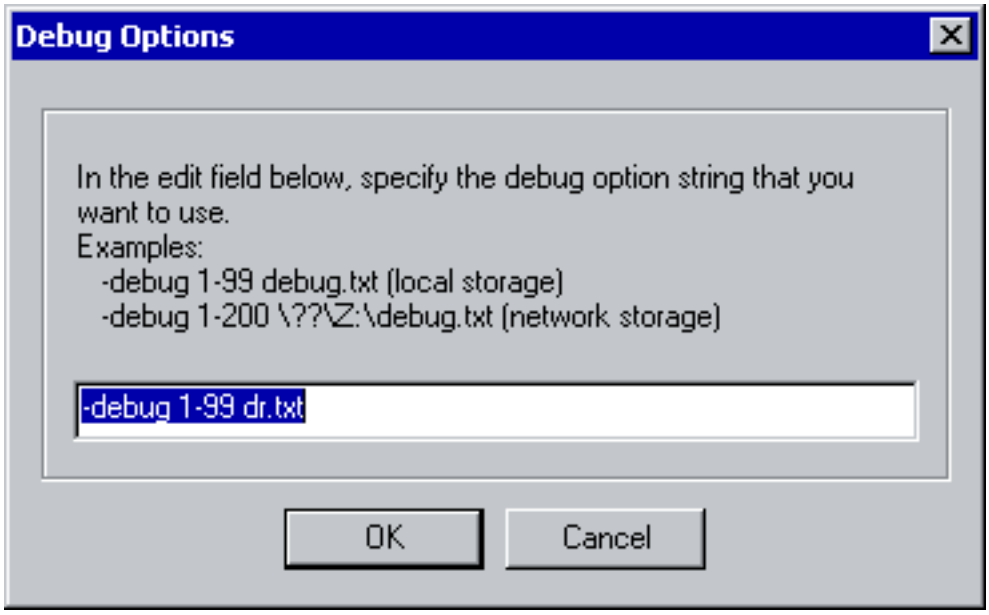


2. デバッグを保存する場所などのデバッグオプションを指定するには、**[デバッグ...]**をクリックします。デフォルトでは、*%SystemRoot%*\system32\OB2DR\tmpディレクトリにデバッグが保存されます。

> **注：**
> Windows Vista以降のリリースの場合、*%SystemRoot%*\system32\OB2DR\tmpディレクトリはRAMディスク上にあります。RAMディスクのサイズは通常、64 MB未満に制限されています。RAMディスクの使用量が制限に到達すると、Data Protectorは予期しない動作を始める可能性があります。したがって、ディザスタリカバリセッションによる大量のデバッグの発生が予想されるときは、デバッグを保存する場所を変更する必要があります。

[デバッグオプション]ウィンドウが表示されます。

デバッグログの保存場所の変更



3. デバッグログを保存する場所を入力します。ドライブの前には\\?は必要ありません。例：\\?\Z:\debug.txt。ネットワーク共有にデバッグを保存することを選択した場合、net useコマンドを使用してデバッグログが書き込まれる共有をマウントします。例：net use X: "\\client\debug_output_folder /user:username password".

Linuxシステム

デバッグログの作成を有効にするには:

1. ディザスタリカバリウィザードで、**[デバッグの使用]**を選択します。
2. デバッグオプション画面で、デフォルトオプションの使用またはデフォルトオプションの変更を選択します。

```
Select one of following options:
1) Use Default Debug Option "-debug 1-200 dr.txt"
2) Specify Different Debug Option
3) Disable Debug option
Command [1-3]:
```

> **注：**
> Linuxシステムでは、デバッグログが保存されるディレクトリはRAMディスク上にあります。RAMディスクのサイズは通常制限されています。RAMディスクの使用量が制限に到達すると、Data Protectorは予期しない動作を始める可能性があります。したがって、ディザスタリカバリセッションによる大量のデバッグの発生が予想されるときは、デバッグを保存する場所を変更する必要があります。場所を変更するには、**[別のデバッグオプションを指定する]**を選択します。

3. デバッグパラメーターを入力できる新しい画面が表示されます。

```
Examples:
-debug 1-200 debug.txt (local storage)
```

```
-debug 1-200 //servername/sharename/debug.txt (windows share)
-debug 1-200 servername:/sharename/debug.txt (nfs share)
Specify the debug option string that you want to use:
```

デバッグファイルをWindows共有ディスクまたはNFS共有フォルダーに保存することを選択できます。

ディザスタリカバリ中のomnircオプションの設定

omnircオプションに関する一般情報は、『*HPE Data Protectorトラブルシューティングガイド*』を参照してください。

WindowsシステムまたはLinuxシステム上で、ディザスタリカバリの実行中にomnircオプションを設定する必要がある場合には、以下の手順を実行してください。

Windowsシステム

1. 「ディザスタリカバリ」ウィザードが表示されたら、カウントダウン中に任意のキーを押してウィザードを停止します。
2. **[Cmd]**をクリックして、コマンドプロンプトを開始します。
3. 次のコマンドを実行します。

   ```
   echo variable > %SystemRoot%\system32\OB2DR\omnirc
   ```

   変数には、omnircファイルに書き込むomnircオプションを正確に指定します。

   例：

   ```
   echo OB2RECONNECT_RETRY=1000 > %SystemRoot%\system32\OB2DR\omnirc
   ```

   このコマンドでは、ディザスタリカバリオペレーティングシステム内にomnircファイルを作成し、OB2RECONNECT_RETRYオプションに1000秒を設定しています。
4. コマンドプロンプトを閉じ、「ディザスタリカバリ」ウィザード内の**[次へ]**をクリックして、ディザスタリカバリを続行します。

Linuxシステム

1. ディザスタリカバリウィザードで、**[Alt] [F3]**を押して別のコンソールに切り替えます。
2. コンソールで、次のコマンドを実行します。

   ```
   echo variable > /opt/omni/.omnirc
   ```

   *variable*には、.omnircファイルに書き込むomnircオプションを正確に指定します。

   例：

   ```
   echo OB2RECONNECT_RETRY=1000 > /opt/omni/.omnirc
   ```

   このコマンドでは、ディザスタリカバリオペレーティングシステム内に.omnircファイルを作成し、OB2RECONNECT_RETRYオプションに1000秒を設定しています。
3. **exit**と入力してシェルを終了し、ディザスタリカバリウィザードでディザスタリカバリを続行します。

Windows上でのdrm.cfgファイル

Data Protectorのディザスタリカバリの構成は、広範なシステム構成を対象とするよう設定されています。しかし、場合によっては、これらの設定が最適ではないことや、システム上の問題をトラブルシューティングするために設定の一部を変更しなければならないことがあります。

drm.cfgファイルには、変更が可能で、ディザスタリカバリの処理に影響を与えるパラメーターが、その影響の説明と一緒に記述されています。ファイルは、EADRおよびOBDRに使用できます。

これらのパラメーターを変更するには、以下の手順に従ってください。

1. 一時ファイルのdrm.cfg.tmplをdrm.cfgにコピーします。このテンプレートは、インストールまたはアップグレードの際に*Data_Protector_home*\bin\drim\configに作成されます。パラメーターはすべてデフォルト値に設定されています。
2. drm.cfgファイルを編集します。パラメーターに目的の値を設定します。ファイルの指示に従ってください。

EADRまたはOBDRの自動収集を無効にする

フルクライアントバックアップを実行すると、特定のバックアップ方法に必要なデータの収集中にCONFIGURATIONバックアップに失敗します。これは、Data Protectorがデフォルトではすべての自動ディザスタリカバリ方法のデータを収集するため、この方法がディザスタリカバリに使用されない場合も当てはまります。たとえば、ブートディスクがLDMディスクの場合に、Data ProtectorがEADRのデータを収集しているときにこの状況が発生することがあります。

失敗したディザスタリカバリ方法のデータの自動収集を無効にします。これにより、Data Protectorが、他の方法に必要なデータを収集できるようになります。

OB2_TURNOFF_COLLECTINGオプションを次のいずれかの値に設定します。

値	説明
0	デフォルト設定、すべての自動方法(EADRとOBDR)でのデータ収集がオンになります。
1	EADR/OBDRデータの収集をオフにします。
2	EADR/OBDRデータは引き続き収集されます。
3	すべての方法の収集をオフにします。

共通の問題(すべての方法)

ディザスタリカバリの実行中に、次のような問題が発生することがあります。

メディアコピーまたはオブジェクトコピーからディザスタリカバリを実行できない。

問題
メディアコピーまたはオブジェクトコピーからディザスタリカバリを実行できない。 Data Protectorは、デフォルトでは元のメディアセットを使用して、ディザスタリカバリを実行します。そのため、ディザスタリカバリウィザードにはコピーオブジェクトバージョンが表示されません。
対処方法
• オブジェクトコピー: オリジナルメディアセット内のすべてのメディアをIDBからエクスポートした後、SRDファイルを再生成します。その後、Data Protectorのディザスタリカバリウィザードでは、最初に使用可能なオリジナルメディアセットのコピーが表示されます。 • メディアコピー: SRDファイル内のオリジナルメディアのメディアIDをメディアコピーのメディアIDに書き換えます。その後、Data Protectorのディザスタリカバリウィザードでは、最初に使用可能なオリジナルメディアセットのコピーが表示されます。

ディザスタリカバリが完了した後にログオンできない

問題
ディザスタリカバリ後にシステムにログオンしようとしたときに発生する問題。 次のメッセージが返されることがあります。 `The system cannot log you on to this domain, because the system’s computer account in its primary domain is missing or the password on that account is incorrect.` このようなメッセージが返される場合は、以下のいずれかの理由が考えられます。 • ディザスタリカバリに必要なすべての情報を収集した後で、Windowsを再インストールし、このシステムを問題のドメインに追加した場合。 • ディザスタリカバリに必要なすべての情報を収集した後で、問題のドメインからシステムをいったん取り出し、後から同一または別のドメインに追加した場合。 このような場合、Windowsは、ディザスタリカバリ時に復元される情報とは互換性のない新しいシステム保護情報を生成します。
対処方法
1. 管理者としてローカルな形でシステムにログオンします。 2. [コントロールパネル]で**[ネットワーク]**をクリックし、**[ネットワークID]**タブを使用して、現在のドメインから一時ワークグループにシステムを移動します。 3. 先ほどのドメインにシステムを再び追加します。この操作にはドメイン管理者のパスワードが必要です。**[OK]**をクリックします。

4. システムを再起動します。

この新しい状態を反映させるために、必要なすべてのディザスタリカバリ準備手順を再実行します。

ネットワーク設定不適切なためディザスタリカバリが失敗する

問題
Data Protectorが不適当なネットワーク構成のクライアントを復旧するため、ディザスタリカバリセッションが失敗します。 クライアントネットワークの構成に使用されるデフォルトの設定は、クライアントのオペレーティングシステムに依存します。 **Windows XP、Windows Server 2003の場合：** SRDファイルに明記された、元のネットワーク構成(バックアップ時点のネットワーク構成)。 **Windows Vista以降のリリースの場合：** DHCP設定により定義されたネットワーク構成。
対処方法
デフォルト以外のネットワーク構成への切り替え 1. ディザスタリカバリセッションを開始します。 2. Data Protectorが表示されたら次を実行します。 **Windows XP、Windows Server 2003の場合：** ネットワークをDHCPに切り替えるには、この後10秒以内にF8を押します。 **Windows Vista以降のリリースの場合：** バックアップ時点のネットワーク設定に切り替えるには、この後10秒以内にF8を押します。 **[F8]**キーを押します。

BTRFSタイプのファイルシステムのサポートが制限される

問題
BTRFSタイプのファイルシステムのサポートが制限されます。 マウントされたbtrfsサブボリュームに子サブボリュームがある場合、バックアップ中に子サブボリュームからのデータがスキップされます。子サブボリュームは空のフォルダーとしてバックアップされます。
対処方法
1. 各サブボリュームを新しいマウントポイントとしてマウントします。 2. バックアップ仕様で新しいマウントポイントを構成します。

ディザスタリカバリ中にエラーメッセージが表示される

問題
ディザスタリカバリ中に次のエラーメッセージが表示されます。 `Failed to perform post-DR operations`
対処方法

ディザスタリカバリの処理を完了するには、omniccコマンドを手動で実行します。
• オンライン復旧の場合: Cell Manager上で次のコマンドを実行します。
`omnicc -secure_comm –configure_peer <hostname_of_client_being_recovered> -overwrite`
• オフライン復旧の場合: Media Agent上で次のコマンドを実行します。
`omnicc -secure_comm -remove_peer <hostname_of_client_being_recovered>`

半自動ディザスタリカバリのトラブルシューティング

半自動ディザスタリカバリの実行中に、次のような問題が発生することがあります。

「ファイルがコピーできない」

問題
Drstartレポート: "Can not copy *filename*." このエラーメッセージは、*drstart*ユーティリティが指定ファイルをコピーできないことを意味します。その原因の1つとして、ファイルがシステムによってロックされていることが考えられます。たとえば、*drstart*が*omniinet.exe*をコピーできない場合、その原因として、すでにInetサービスが実行されていることが考えられます。これは通常では考えられない状況で、クリーンインストールの後にこのような現象が生じることはありません。
対処方法
残りのファイルのコピーを続行するかどうかを確認するダイアログボックスが表示されます。**[はい]**をクリックすると、drstartはロックされているファイルをスキップし、ほかのファイルのコピーを続行します。ファイルがシステムによりロックされている場合には、ディザスタリカバリに必要なプロセスがすでに実行中でありそのファイルはコピーする必要がないため、これで問題は解決されます。 **[中止]**をクリックしてdrstartユーティリティを終了することもできます。

拡張自動ディザスタリカバリとワンボタンディザスタリカバリのトラブルシューティング

拡張自動ディザスタリカバリ方法またはワンボタンディザスタリカバリ方法を使用したディザスタリカバリの実行中に、以下のような問題が発生することがあります。

システムに接続されたD2Dゲートウェイが復旧されるときに、Linux上でのEADRオンライン復元が失敗する

デタッチされたSAN-LVMボリュームを含むRHEL EADRが機能しない、ページ 138

自動ディザスタリカバリ情報が収集できない

問題
EADRまたはOBDRを実行中に、次のエラーが出力される場合があります。「`Automatic DR information could not be collected. Aborting the collecting of system recovery data`」
対処方法

このエラーの原因は、`autodr.log`(場所は、デフォルトのData Protector一時ファイルディレクトリ)に格納されています。
1. すべての記憶デバイスが正しく構成されているかどうか、確認してください。デバイスマネージャーにデバイスが「不明なデバイス」として報告される場合は、適切なデバイスドライバーをインストールしてからEADR/OBDRを実行し直す必要があります。正しく構成されていない記憶デバイスがシステムに接続されている場合も、`autodr.log`に同様のエントリが表示されることがあります。
`DRIM_WIN_ERROR 13 SetupDiGetDeviceRegistryProperty`
2. 十分なレジストリの空き領域が必要です。レジストリの最大サイズを現在のレジストリサイズの2倍以上に設定することをお勧めします。レジストリの空き領域が不足していると、以下のようなエントリが`autodr.log`に書き込まれます。
`ERROR registry 'Exception while saving registry' .... WindowsError: [Errno 1450] Insufficient system resources exist to complete the requested service.`
3. 必ず自動マウント機能を有効にします。自動マウント機能によって、すべてのボリュームが(マウントポイントなしで)オンラインになります。自動マウントが無効であると、ドライブ文字を指定していないボリュームすべてがブートプロセス中にオフラインになります。これにより、システム予約パーティションがドライブ文字にアクセスできなくなり、ディザスタリカバリ手順が失敗することがあります。
自動マウント機能を無効にする必要がある場合は、必ずシステム予約パーティションをマウントしておいてください。
問題が再発する場合は、(少なくとも手動によるディザスタリカバリは可能になるように)Data Protector自動ディザスタリカバリコンポーネントをアンインストールし、技術サポートに連絡してください。

重大でないエラーが検出された

問題

EADRまたはOBDRを実行中に、次のエラーが出力される場合があります。「Some non-critical errors were detected during the collecting of Automatic DR data. Review the Automatic DR log file.

対処方法

自動ディザスタリカバリモジュールの実行中に「重要でないエラー」が検出された場合は、バックアップをディザスタリカバリに使用する妨げとなる可能性が非常に低いエラーが検出されたことを意味します。重要でないエラーの原因は、autodr.log(場所は、デフォルトのData Protector一時ファイルディレクトリ)に格納されています。例：

*%SystemRoot%*フォルダーにないサービスやドライバー(ウィルススキャナーなど)が検出されました。Autodr.logには、同様のエラーメッセージが含まれます。

```
ERROR safeboot 'unsupported location' 'intercheck support 06' 2
u'\\??\\D:\\Program Files\\Sophos SWEEP for NT\\icntst06.sys'.
```

これはディザスタリカバリの成否に影響する問題ではないので、このエラーメッセージは無視してかまいません。

デバイスが計画されたゲートウェイを持つStoreOnce/DDBoostデバイスから作成された場合に復元セッションが失敗する

問題

計画されたゲートウェイを持つStoreOnce/DD Boostデバイスからデバイスを構成し、ディザスタリカバリ用に同じクライアントを構成すると、復元セッションが終了してCell Manager上に次の警告メッセージが表示されます。

```
[Major] From: RSM@<hostname> "" Time: 6/14/2016 2:48:49 PM

[61:3003] Lost connection to B2D gateway named "DeviceName" on host <hostname>

Ipc subsystem reports: "unknown"

[Warning] From: RSM@<hostname> "" Time: 6/14/2016 2:48:49 PM

Device <DeviceName> is disabled and will not be used.
```

このエラーは、クライアントB2Dゲートウェイとの接続が失われたために発生します。

対処方法

復元セッションの終了時に表示される警告メッセージは無視してください。拡張自動ディザスタリカバリは正常に終了し、クライアント復旧コンソール上に結果が表示されます。

復元中にネットワークが使用できなくなった

問題
この問題は、ケーブルやスイッチの破損など、さまざまな原因によって発生します。ネットワーク障害の別の原因としては、DNSサーバーが、バックアップ時にそのように構成されたために、復旧中にオフラインになっていることが考えられます。DR OSの構成がバックアップ時と同じため、ネットワークは使用不可能になります。
対処方法
1. スイッチやケーブルなどに問題がないことを確認します。 2. バックアップ時の構成によりDNSサーバーが復元中にオフラインになる場合は、以下のいずれかの方法で対処します。 • オフライン復旧を実行して、復旧後にDNS設定を変更する。 • 段階2の開始前にレジストリを編集する。この場合、レジストリの変更内容が反映されるように、段階2に入る前にシステムを再ブートする必要があります。段階2が完了したら、設定を修正してから段階3を開始する必要があります。 **注意：** レジストリを不適切に編集すると、ディザスタリカバリが失敗する原因になります。

システムに接続されたD2Dゲートウェイが復旧されるときに、Linux上でのEADRオンライン復元が失敗する

問題
EADRオンライン復元でD2Dデバイスを使用すると、RMAが失敗して次のエラーメッセージが表示されます。 `[61:1005] Got unexpected close from RMA on clientsystem.domain.org if the gateway is configured on the same EADR system`
対処方法
復旧対象のDRシステムに割り当てられているゲートウェイを削除して、新しいゲートウェイを追加します。ゲートウェイを再構成する方法の詳細については、『*HPE Deduplication guide*』を参照してください。

ネットワークドライバーがないために、ネットワークが使用できない

問題

Windows VistaまたはWindows Server 2008システムの場合、搭載されているネットワークカードがDR OSでサポートされていないため、障害復旧の際にネットワークが使用できなくなっています。
対処方法
見つからないドライバーをDR OSイメージに挿入してください。

Cell Managerとクライアントが異なるドメインに存在するときにEADRとOBDRオンライン復旧が失敗する

問題
この問題は、ネットワーク構成が正しくないために発生する可能性があります。
対処方法
1. Cell Managerとクライアントシステムの両方の`host`ファイルを更新します。これらのファイルには、Cell Managerとクライアントのホスト名とIPアドレスを格納する必要があります。 2. Cell Managerとクライアント間の`ping`要求が正しい値を返すかどうかをチェックします。問題があれば、ネットワーク管理者に問い合わせてください。 3. `omnicheck -dns`コマンドを使用して、Cell Managerとクライアント間のDNS解決が正しいかどうかをチェックします。詳細については、`omnicheck`のmanページまたは『*HPE Data Protector Command Line Interface Reference*』を参照してください。問題があれば、ネットワーク管理者に問い合わせてください。

自動ログオンが正常動作しない

問題
自動ログオンが失敗する
対処方法
管理者アカウントでパスワードを省略してログオンしてみてください。

EADR中にコンピューターが応答を停止する

問題
ディザスタリカバリCDに問題があると、コンピューターがハングすることがあります。
対処方法
• CDが読み取り可能かどうかをチェックします。 • CD-RWを何度も再使用することは避けてください。

Microsoft Cluster ServerのEADR用のCD ISOイメージを作成できない

問題
CD ISOイメージを作成するには、クォーラムディスクをバックアップする必要があります。
対処方法
クォーラムディスクをバックアップします。

Microsoft Cluster Serverクライアントでの CD ISOイメージの作成が失敗する

問題
Microsoft Cluster Server環境では、ISOイメージをクラスタークライアントに作成することはできません。ファイルシステムの復元は、期待どおりに機能します。 この問題が発生するのは、Data Protectorが、ドメイン名(物理的なクライアントのIPに解決される)ではなくクラスターIP(仮想的なIP)の使用を試みることが原因です。
対処方法
ネットワークサービスの接続順序を、`Local Area Connection`が先頭になるように変更します。

ウィルス対策ソフトウェアをメディア作成ホスト上にインストールしたときにISOイメージの作成が失敗する

問題
WAIK/ADKを使用してISOイメージを作成して、ウィルス対策ソフトウェアをメディア作成ホスト上にインストールすると、ISOイメージ作成が失敗して次のエラーメッセージが表示されます。 GUI内： ISOイメージファイルの作成に失敗しました。Data Protectorの一時ディレクトリに格納されている`autodr`ログをチェックしてください。 `autodr.log`ファイル内： パッケージの追加操作が失敗してアクセス拒否(5)エラーが表示されます。
対処方法
ISOイメージ作成プロセスが完了するまで、メディア作成ホスト上のウィルス対策ソフトウェアを一時的に無効にします。

ドライブベースの暗号化を使用した場合に、omniisoによるISOイメージの作成が失敗する

問題

バックアップセッションからISOイメージを作成する場合に、バックアップ仕様で**[ドライブベースの暗号化]**が無効にされていると、ISOイメージの作成が失敗して次のエラーメッセージが表示されます。

```
[Major] From: omniiso@computer.company.com "omniiso" Time: <DateTime>

Error updating SRD file objects [error: -1]. Aborting.
```

次の場合、エラーメッセージが表示されます。

- バックアップ仕様で後続するバックアップの**[ドライブベースの暗号化]**が有効にされていた場合。
- セッション内のあて先ドライブが同じで、そこからISOイメージが作成され、後続するバックアップが別のメディアに移動された場合。

この問題はキーストアが最初のメディアに作成されていないために発生します。後続のバックアップによってドライブに暗号化のマークが付けられていたため、omniisoは最初のメディアの暗号化キーをエクスポートしようとして失敗します。

対処方法

- 暗号化されていないバックアップを、ドライブベースの暗号化を無効にした別のドライブに移動して、再度`omniiso`を実行します。
- **"ドライブベースの暗号化"**を有効または無効にして同じあて先ドライブに対してバックアップを実行しないようにします。

段階1で、ボリュームが再マウントされない

問題

ディスクコントローラーおよびその構成によって、一部のシステムでは、別のボリュームのマウントポイントに関連付けられているドライブ文字が割り当てられていないボリュームは、障害回復の段階1で、適正に再マウントできない場合があります。これは、マウントポイントを含むボリュームが再作成または再フォーマットされた場合に発生する場合があり(DR OSを含むシステムボリュームなど)、オペレーティングシステムが「セーフモード」で起動され、元のマウントポイントのターゲットボリュームにあるファイルシステムが検出されなくなります。その結果、ディザスタリカバリモジュールは、このボリュームを認識しなくなり、`drecovery.ini`にないとレポートします。そのボリュームのコンテンツは、認識はされませんが、完全な状態で残ります。

対処方法

- ドライブ文字を使用してボリュームをマウントし、`chkdsk /v /f`コマンドを使用して検証するか、システムが完全に復元された後で元のマウントポイントを再作成します。
- 手動で直接MiniOSにシステムを再起動します(リカバリCDから再起動しないようにします)。前にアンマウントされていたボリュームが自動的にドライブ文字にマウントされます。

ディザスタリカバリが失敗または中止された後、起動記述子が残る

問題
Intel Itaniumシステムで、ディザスタリカバリセッションが失敗または中止されると、起動記述子(DRM Temporary OSという名前)がEFI環境に残る場合があります。これにより、ディザスタリカバリプロセスを再開始すると予期しない動作が生じる可能性があります。
対処方法
範囲選択メニューから**[起動記述子の削除]**を使用して起動記述子を削除します。起動記述子が削除されると、範囲を選択してディザスタリカバリを続行できます。

Intel Itaniumシステムで間違ったブートディスクが選択されるか、またはブートディスクが選択されない

問題
Intel Itaniumシステムでは、間違ったブートディスクが選択されます(またはブートディスクがまったく選択されません)。
対処方法
1. 範囲選択メニューから**[手動ディスク選択]**を選択します。新しいメニューに、使用可能なすべてのディスクが表示されます。 2. 正しいブートディスクを決定します。元のディスクの情報を参照するには**o**を押し、選択したディスクの詳細を参照するには**d**を押します。 3. カーソルキーを使用してリストからディスクを選択肢、**b**を押します。**c**を押すと、選択内容を削除できます。 ブートディスクがシステムディスクと同じでない場合(デフォルトではどちらのディスクも同じです)、システムディスクも選択する必要があります。 **[戻る]**を選択します。 4. リカバリの範囲を選択すると、ディザスタリカバリが続行します。

ディザスタリカバリが失敗し、「十分なスペースがありません」というメッセージが表示される

問題
Windows Server 2008 R2ドメインコントローラーのディザスタリカバリは、失敗すると以下と同様のエラーを表示します。

```
[Major] From: VRDA@computer.company.com "Dev1" [/CONFIGURATION]" Time:
07.12.2012 15:33:58 X:\windows\System32\OB2DR\tmp\config\
ActiveDirectoryService\D$\ Windows\NTDS\ntds.dit Cannot write:
([112] There is not enough space on the disk. ) => not restored.
```

対処方法

1. クライアントバックアップのバックアップ仕様を変更します。ソースページでCCONFIGURATIONオブジェクトを展開し、ActiveDirectoryService項目およびSYSVOL項目のチェックボックスをオフにします。

   > **注：**
   > 変更後も、Active DirectoryおよびSYSVOLはシステムボリューム(C:/)バックアップの一部としてバックアップされます。デフォルトでは、これらはC:/Windows/NTDSとC:/Windows/SYSVOLにそれぞれあります。

2. ディザスタリカバリの手順を繰り返します。

Windows 8.1クライアントのディザスタリカバリが失敗し、「書き込めません: ([13]データが無効です。)=>復元されません。」メッセージが表示されます

問題

Windows 8.1クライアントのディザスタリカバリが失敗し、以下のようなエラーが表示されます。

```
[Major] From: VRDA@computer.company.com "hostname"
[mountpoint]" Time:
<timestamp> <filename> Cannot write: ([13] The data is invalid. ) => not
restored.
```

対処方法

ディザスタリカバリCDからクライアントシステムをブートし、Windows 8.1クライアントのパーティションをフォーマットしてディザスタリカバリを続行します。

復旧イメージ作成で、Windowsクラスター上での不足ボリュームのレポートに失敗する

問題

システム上に存在しないボリュームが原因でDR復旧イメージ作成ウィザードが失敗しますが、Disk Witness Quorum構成では、クラスターデータベースが破損していないこと(クラスターフォルダーはクォーラムディスク上にある)およびイベントログがクォーラムに関係していることが確認されます。

対処方法
この問題を解決するには、クォーラムを再作成し、構成データのバックアップを再度実行します。

クライアントバックアップ中に警戒域のエラーまたは警告が表示される

問題

クライアントバックアップ中に次の警戒域のエラーが報告される場合があります。
`Cannot perform stat(): ([2] No such file or directory)`
`File is shorter than it was when it was opened`
このような警告およびエラーは、Data Protectorの一時ディレクトリ内のファイルが変更されたことにより表示される可能性があります。たとえば、`/CONFIGURATION`マウントポイントと/ (ルート)マウントポイントを同時にバックアップすると、発生する可能性があります。

対処方法
バックアップ仕様から`/opt/omni/bin/drim/tmp`と`/opt/omni/bin/drim/log`ディレクトリを除外します。 8.10以降のバージョンで作成されたバックアップ仕様では、これらのファイルは自動的に除外されます。

Cell ManagerとRMAホストが応答しない

問題

RHELオペレーティングシステム内のLinux仮想マシンのディザスタリカバリが失敗して次のエラーメッセージが表示されます。
`Cell Manager is not responding. Attempting offline restore.`
`RMA host is not responding.`
ディザスタリカバリに使用した仮想マシンのNICとMACアドレスが、元の仮想マシンと異なるため、このようなエラーが発生する場合があります。仮想マシンにIPアドレスが割り当てられなくなり、オンライン復旧が失敗します。

対処方法
この場合、以下の手順を実行します。 • **Alt+F2**を押して別のコマンドシェルを開きます。 • `/etc/sysconfig/network`に移動します。 • インターフェイスファイルを修正して、現在のインターフェイスとMACアドレスを一致させます。 • ネットワークサービスを再開します。 • 必要に応じて、ネットワーク接続用のホストファイルを編集します。

- Cell Managerとメディア(バックアップ)ホストがクライアントに到達できることを確認します。
- **Alt+F1**を押してメインコマンドシェルウィンドウに戻り、復旧オプションを選択します。

EADRオフライン復元が、D2DおよびDDBoostデバイスで失敗する

問題
設定したユーザー名とパスワードでディスク間デバイスを使用すると、オフラインEADRが失敗します。
対処方法
一時的にユーザー名とパスワードを削除して復元を実行します。

デタッチされたSAN-LVMボリュームを含むRHEL EADRが機能しない

問題
Linuxシステムで、EADR復旧後に**[デフォルトの復旧]**または**[最小復旧]**方法を使用した場合は、復旧されたシステムをブートできない可能性があります。以下のエラーメッセージがブート中に表示されます。 **<volume_name>を開こうしているときに、スーパーブロックで不正なマジックナンバーが検出されました**
対処方法
EADRの復旧後、復旧されたシステムをブートする前に、OS保守、ルートパスワード、mount -o remount、rw / (読み取り/書き込みモードで「/」マウントポイントを再マウント)を入力して、/etc/fstabを編集する必要があります。 デフォルトの復旧オプションを選択した場合は、そのオプションをコメントアウトするか、/boot、/、/opt、/etc、および/varを除くすべてのマウントポイントをfstabから削除します。 最小復旧オプションを選択した場合は、そのオプションをコメントアウトするか、/bootを除くすべてのマウントポイントをfstabから削除します。

Internet Information Serverのディザスタリカバリのトラブルシューティング

Internet Information Server (IIS)のディザスタリカバリの問題は、通常はサービスが実行されていないかサービスがインストールされていないために発生します。

IISに必要なサービスが自動的に開始されない

問題
IISの復旧後には、IISに必要なサービス(SMTPやNNTPなど)は自動では開始されません。
対処方法
1. これらのサービスは手動で開始してください。 2. 手動でも起動できない場合は、IIS Admin Serviceを停止して、*%SystemRoot%*\system32\inetsrv\MetaBase.binファイルを復元します(**[上書き]**オプションを使用)。 **注：** *%SystemRoot%*\system32\inetsrvディレクトリは、IISサービスのデフォルトの保存場所です。このサービスをほかの場所にインストールした場合は、その場所をMetaBase.binファイルの復元先として指定してください。 3. IIS管理サービスとIISに必要なすべてのサービスを開始します。

付録A: 準備作業の例

HP-UX 11.x上での抹消リンクの移動例

```
# The system will go from "run-level" 4 to "run-level 1"

# retaining the (rpcd), inetd, networking, swagentd services up. The state is called
"minimum activity" for backup purposes (need networking).

# IMPORTANT: ensure the links are present in /sbin/rc1.d before

# moving and they do have this exact name. You have to rename them for the rc0.d
directory. Put them BELOW the lowest (original "/sbin/rc0.d/Kxx") "K...-link" in rc0.d

# Move K430dce K500inetd K660net K900swagentd into ../rc0.d BELOW the lowest kill
link!!!

echo "may need to be modified for this system"

exit 1

#

cd /sbin/rc1.d

mv K430dce ../rc0.d/K109dce

mv K500inetd ../rc0.d/K110inetd

mv K660net ../rc0.d/K116net

mv K900swagentd ../rc0.d/K120swagentd
```

ディザスタリカバリ準備の一覧表の例(Windows用)

クライアントプロパティ	コンピューター名	ANAPURNA
	ホスト名	anapurna.company.com
ドライバー		tatpi.sys, aic78xx.sys
Windows Service Pack		Windows Vista
IPv4用のTCP/IPプロパティ	IPアドレス	10.17.2.61
	デフォルトゲートウェイ	10.17.250.250
	サブネットマスク	255.255.0.0
	DNS順序	10.17.3.108, 10.17.100.100

IPv6用のTCP/IPプロパティ	IPアドレス	td10:1234:5678:abba::6:1600
	サブネットプレフィックスの長さ	64
	デフォルトゲートウェイ	td10:1234:5678:abba::6:1603
	優先度の高いDNSサーバー	td10:1234:5678:abba::6:1603
	代替DNSサーバー	td10:1234:5678:abba::6:1604
メディアラベル/バーコード番号		"anapurna - disaster recovery" / [000577]
パーティション情報/順序	最初のディスクラベル	
	最初のパーティションの長さ	31MB
	最初のドライブ文字	
	最初のファイルシステム	EISA
	2番目のディスクラベル	BOOT
	2番目のパーティションの長さ	1419MB
	2番目のドライブ文字	C:
	2番目のファイルシステム	NTFS/HPFS
	3番目のディスクラベル	
	3番目のパーティションの長さ	
	3番目のドライブ文字	
	3番目のファイルシステム	

フィードバックを送信

このドキュメントに関するご意見は、ドキュメンテーションチームまで電子メールでお送りください。お使いのシステムに電子メールクライアントが設定されている場合は、上のリンクをクリックすると、電子メールウィンドウが開き、件名行に次の情報が入力されます。

ディザスタリカバリガイド (HPE Data Protector 10.00)に関するフィードバック

本文にご意見、ご感想を記入の上、**[送信]**をクリックしてください。

電子メールクライアントが利用できない場合は、上記の情報をコピーしてWebメールクライアントの新規メッセージに貼り付け、AutonomyTPFeedback@hpe.com宛にお送りください。

お客様からのご意見、ご感想をお待ちしています。