HP Data Protector A.06.11

障害復旧ガイド

製品番号: B6960-99124
初版: 2009年9月

ご注意

本書で取り扱っているコンピュータソフトウェアは秘密情報であり、その保有、使用、または複製には、Hewlett-Packard Companyから使用許諾を得る必要があります。米国政府の連邦調達規則であるFAR 12.211および12.212の規定に従って、コマーシャルコンピュータソフトウェア、コンピュータソフトウェアドキュメンテーションおよびコマーシャルアイテムのテクニカルデータ(Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items)は、ベンダが提供する標準使用許諾規定に基づいて米国政府に使用許諾が付与されます。

本書に記載されている内容は事前の通知なしに変更されることがあります。HP製品およびサービスに対する保証は、当該製品およびサービスに付属の明示的保証規定に記載されているものに限られます。ここでの記載で追加保証を意図するものは一切ありません。本書の内容につきましては万全を期しておりますが、本書の技術的あるいは校正上の誤り、省略に対しては責任を負いかねますのでご了承ください。

Intel®、Itanium®、Pentium®、Intel Inside®、およびIntel Insideロゴは、米国およびその他の国におけるIntel Corporationまたはその子会社の商標または登録商標です。

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

AdobeおよびAcrobatは、Adobe Systems Incorporatedの商標です。

Javaは、米国におけるSun Microsystems, Inc.の商標です。

Oracle®は、Oracle Corporation(Redwood City, California)の米国における登録商標です。

UNIX®は、The Open Groupの登録商標です。

Printed in the US

目次

図一覧

表一覧

出版履歴

次の版が発行されるまでの間に、間違いの訂正や製品マニュアルの変更を反映したアップデート版が発行されることもあります。アップデート版や新しい版を確実に入手するためには、対応する製品のサポートサービスにご登録ください。詳細については、HPの営業担当にお問い合わせください。

表 1 出版履歴

製品番号	ガイド版	製品
B6960-96004	2006 年 7 月	Data Protector リリース A.06.00
B6960-96038	2008年11月	Data Protector リリース A.06.10
B6960-99124	2009年9月	Data Protector リリース A.06.11

本書について

本書では、以下について説明します。

- 障害復旧のプランニングと準備
- 障害復旧手順のテスト
- 障害復旧の正しい実行方法

対象読者

このマニュアルは、障害復旧の計画、準備、テスト、および実行を担当するバックアップ管理者を対象としており、以下に関する知識があることを前提としています。

- Data Protector概念
- Data Protectorのバックアップおよび復元手順

ドキュメントセット

その他のドキュメントおよびオンラインヘルプでは、関連情報が提供されます。

ガイド

Data Protectorのガイドは、印刷された形式あるいはPDF形式で利用できます。PDFファイルは、Data Protectorのセットアップ時に、Windowsの場合はEnglish Documentation & Helpコンポーネントを、UNIXの場合はOB2-DOCSコンポーネントを、それぞれ選択してインストールします。インストールすると、このガイドはWindowsの場合はData_Protector_home¥docsディレクトリ、UNIXの場合は/opt/omni/doc/Cディレクトリに保存されます。

これらの資料は、HP Business Support CenterのWebサイトの[Manuals]ページから入手できます。

http://www.hp.com/support/manuals

[Storage]セクションの**[Storage Software]**をクリックし、ご使用の製品を選択してください。

- *HP Data Protector コンセプトガイド*

  このガイドでは、Data Protectorのコンセプトを解説するとともに、Data Protectorの動作原理を詳細に説明しています。手順を中心に説明しているオンラインヘルプとあわせてお読みください。

- *『HP Data Protector インストールおよびライセンスガイド』*

  このガイドでは、Data Protectorソフトウェアのインストール方法をオペレーティングシステムおよび環境のアーキテクチャごとに説明しています。また、Data Protectorのアップグレード方法や、環境に適したライセンスの取得方法についても説明しています。

- *『HP Data Protector トラブルシューティングガイド』*

  このガイドでは、Data Protectorの使用中に起こりうる問題に対するトラブルシューティングの方法について説明します。

- *『HP Data Protector ディザスタリカバリガイド』*

  このガイドでは、障害復旧のプランニング、準備、テスト、および実行の方法について説明します。

- *『HP Data Protector インテグレーションガイド』*

  このマニュアルでは、さまざまなデータベースやアプリケーションをバックアップおよび復元するための、Data Protectorの構成方法および使用法を説明します。このマニュアルは、バックアップ管理者やオペレータを対象としています。4種類のガイドがあります。

  - *『HP Data Protector Microsoft アプリケーション用インテグレーションガイド: SQL Server、SharePoint Portal Server、Exchange Server、および Volume Shadow Copy Service』*

    このガイドでは、Microsoft Exchange Server、Microsoft SQL Server、Volume Shadow Copy ServiceといったMicrosoftアプリケーションに対応するData Protectorの統合ソフトウェアについて説明します。

  - *『HP Data Protector インテグレーションガイド－Oracle、SAP』*

    このガイドでは、Oracle、SAP R3、SAP DB/MaxDBに対応するData Protectorの統合ソフトウェアについて説明します。

  - *『HP Data Protector integration guide for IBM applications: Informix, DB2, and Lotus Notes/Domino』*

    このガイドでは、Informix Server、IBM DB2、Lotus Notes/Domino Serverといった IBMアプリケーションに対応するData Protectorの統合ソフトウェアについて説明します。

  - *『HP Data Protector integration guide for VMware Virtual Infrastructure, Sybase, Network Node Manager, and Network Data Management Protocol Server』*

このガイドでは、VMware Virtual Infrastructure、Sybase、Network Node Manager、およびNetwork Data Management Protocol Serverに対応するData Protectorの統合ソフトウェアについて説明します。

- 『*HP Data Protector integration guide for HP Service Information Portal*』

  このガイドでは、HP Service Information Portalに対応するData Protector統合ソフトウェアのインストール、構成、使用方法について説明します。これはバックアップ管理者用です。ここでは、アプリケーションを使用してData Protectorサービスを管理する方法について説明しています。

- 『*HP Data Protector integration guide for HP Reporter*』

  このマニュアルでは、HP Reporter に対応するData Protector統合ソフトウェアのインストール、構成、使用方法について説明します。これはバックアップ管理者用です。Data Protectorのサービス管理にアプリケーションを使用する方法について説明します。

- 『*HP Data Protector integration guide for HP Operations Manager for UNIX*』

  このガイドでは、UNIX版のHP Operations ManagerとHP Service Navigatorを使用して、Data Protector環境の健全性と性能を監視および管理する方法について説明します。

- 『*HP Data Protector integration guide for HP Operations Manager for Windows*』

  このガイドでは、Windows版のHP Operations ManagerとHP Service Navigatorを使用して、Data Protector環境の健全性と性能を監視および管理する方法について説明します。

- 『*HP Data Protector integration guide for HP Performance Manager and HP Performance Agent*』

  このマニュアルでは、Windows版、HP-UX版、Solaris版、Linux版のHP Performance Manager(PM)およびHP Performance Agent(PA)を使用してData Protector環境の健全性と性能を監視および管理する方法について説明します。

- 『*HP Data Protector ゼロダウンタイムバックアップ コンセプトガイド*』

  このガイドでは、Data Protectorゼロダウンタイムバックアップとインスタントリカバリのコンセプトについて解説するとともに、ゼロダウンタイムバックアップ環境におけるData Protectorの動作原理を詳細に説明します。手順を中心に説明している『*HP Data Protector zero downtime backup administrator's guide*』および『*HP Data Protector zero downtime backup integration guide*』とあわせてお読みください。

- 『*HP Data Protector zero downtime backup administrator's guide*』

  このガイドでは、HP StorageWorks Virtual Array、HP StorageWorks Enterprise Virtual Array、EMC Symmetrix Remote Data FacilityおよびTimeFinder、HP StorageWorks Disk Array XPに対応するData Protector統合ソフトウェアのインストール、構成、使用方法について説明します。このマニュアルは、バックアップ管理者やオペレータを対

象としています。ファイルシステムやディスクイメージのゼロダウンタイムバックアップ、インスタントリカバリ、および復元についても説明します。

- 『*HP Data Protector zero downtime backup integration guide*』

  このガイドでは、Oracle、SAP R/3、Microsoft Exchange Server 2000/2003、およびMicrosoft SQL Server 2000データベースのゼロダウンタイムバックアップ、インスタントリカバリ、および標準復元を行うための、Data Protectorの構成方法および使用法について説明します。また、Microsoft Volume Shadow Copy Serviceを使用してバックアップ、および復元を実行するためのData Protectorの構成方法および使用方法についても説明します。

- *HP Data Protector MPE/iX system user guide*

  このマニュアルでは、MPE/iXクライアントの構成方法、およびMPE/iXデータのバックアップおよび復元方法を説明します。

- *HP Data Protector*『*Media Operations user guide*』

  このガイドでは、オフラインストレージメディアのトラッキングと管理について説明します。アプリケーションのインストールと構成、日常のメディア操作、およびレポート作成のタスクについて説明します。

- 『*HP Data Protector product announcements* ソフトウェアノートおよびリファレンス』

  このガイドでは、HP Data Protector A.06.11の新機能について説明しています。また、インストールの必要条件、必要なパッチ、および制限事項に関する情報に加えて、既知の問題と回避策についても提供します。

- 『*HP Data Protector product announcements* ソフトウェアノートおよびリファレンス *for integrations to HP Operations Manager, HP Reporter, HP Performance Manager, HP Performance Agent, and HP Service Information Portal*』

  このガイドは、記載されている統合ソフトウェアに対して同様の役割を果たします。

- 『*HP Data Protector Media Operations Product Announcements, Software Notes, and references*』

  このガイドは、Media Operationsに対して同様の役割を果たします。

- 『*HP Data Protector command line interface reference*』

  このガイドでは、Data Protectorコマンド行インタフェース、コマンドオプション、使用方法を、基本コマンド行の例とともに説明しています。

オンラインヘルプ

Data ProtectorはWindowsおよびUNIXの各プラットフォーム用にオンラインヘルプ(コンテキスト依存ヘルプ([F1]キー)および[ヘルプ]トピック)を備えています。

Data Protectorをインストールしていない場合でも、インストールDVD-ROMの最上位ディレクトリからオンラインヘルプにアクセスできます。

- ***Windowsの場合***: DP_help.zipを解凍し、DP_help.chm.を開きます。
- ***UNIXの場合***: 圧縮されたtarファイルDP_help.tar.gzをアンパックし、DP_help.htmでオンラインヘルプシステムにアクセスします。

ドキュメントマップ

略称

以下の表は、ドキュメントマップに使用されている略称の説明です。ガイドのタイトルには、すべて先頭に「"HP Data Protector"」が付きます。

略称	ガイド
CLI	コマンド行インタフェースリファレンス
Concepts	コンセプトガイド
DR	障害復旧ガイド
GS	スタートガイド
Help	オンラインヘルプ
IG-IBM	IBMアプリケーション用インテグレーションガイド - Informix、DB2、Lotus Notes/Domino
IG-MS	Microsoftアプリケーション用インテグレーションガイド - SQL Server, SharePoint Portal Server, Exchange Server, and Volume Shadow Copy Service
IG-O/S	インテグレーションガイド - Oracle、SAP
IG-OMU	インテグレーションガイド - HP Operations Manager、UNIX
IG-OMW	インテグレーションガイド - HP Operations Manager、Windows
IG-PM/PA	インテグレーションガイド - HP Performance Manager およびHP Performance Agent

略称	ガイド
IG-Report	インテグレーションガイド – HP Reporter
IG-SIP	インテグレーションガイド – HP Service Information Portal
IG-Var	インテグレーションガイド – VMware Virtual Infrastructure、Sybase、Network Node Manager、Network Data Management Protocol Server
Install	インストールおよびライセンスガイド
MO GS	Media Operations Getting Started Guide
MO RN	Media Operations product announcements, software notes, and references
MO UG	Media Operations User Guide
MPE/iX	MPE/iX System User Guide
PA	製品に関するお知らせ、ソフトウェア使用上の注意およびリファレンス
Trouble	トラブルシューティングガイド
ZDB Admin	ZDB Administrator's Guide
ZDB Concept	ZDB コンセプトガイド
ZDB IG	ZDB Integration Guide

対応表

以下の表は、各種情報がどのドキュメントに記載されているかを示したものです。黒く塗りつぶされたセルのドキュメントを最初に参照してください。

	Help	GS	Concepts	Install	Trouble	DR	PA	インテグレーションガイド MS	O/S	IBM	Var	SIP	Report	OMU	OMW	ZDB Concept	Admin	IG	MO GS	User	PA	MPE/iX	CLI
バックアップ	X	X	X					X	X	X	X					X	X	X				X	
CLI																							X
概念 / 手法	X		X					X	X	X	X	X		X	X	X	X	X				X	
障害復旧	X		X			X																	
インストール / アップグレード	X	X		X			X					X		X	X				X	X		X	
インスタントリカバリ	X		X													X	X	X					
ライセンス	X			X			X													X			
制限事項	X				X		X	X	X	X	X				X			X			X		
新機能	X						X																
プランニング方法	X		X									X				X							
手順 / 作業	X			X	X	X		X	X	X	X	X		X	X		X	X		X			
推奨事項			X				X									X					X		
必要条件				X			X	X	X	X	X				X				X	X	X		
復元	X	X	X					X	X	X	X						X	X				X	
サポート一覧							X																
サポートされる構成																X							
トラブルシューティング	X			X	X			X	X	X	X	X					X	X					

統合

以下の統合に関する詳細については、該当するガイドを参照してください。

統合	ガイド
HP Operations Manager for UNIX/for Windows	IG-OMU、IG-OMW
HP Performance Manager	IG-PM/PA
HP Performance Agent	IG-PM/PA

統合	ガイド
HP Reporter	IG-R
HP Service Information Portal	IG-SIP
HP StorageWorks Disk Array XP	すべてのZDB
HP StorageWorks Enterprise Virtual Array (EVA)	すべてのZDB
HP StorageWorks Virtual Array (VA)	すべてのZDB
IBM DB2 UDB	IG-IBM
Informix	IG-IBM
Lotus Notes/Domino	IG-IBM
Media Operations	MO User
MPE/iX system	MPE/iX
Microsoft Exchange Server	IG-MS, ZDB IG
Microsoft Exchange Single Mailbox	IG-MS
Microsoft SQL Server	IG-MS, ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	IG-MS, ZDB IG
NDMP Server	IG-Var
Network Node Manager (NNM)	IG-Var
Oracle	IG-O/S
Oracle ZDB	ZDB IG
SAP DB	IG-O/S
SAP R/3	IG-O/S, ZDB IG

統合	ガイド
Sybase	IG-Var
EMC Symmetrix	すべてのZDB
VMware	IG-Var

表記上の規則および記号

表 2 表記上の規則

規則	要素
青色のテキスト:表2(19ページ)	クロスリファレンスリンクおよび電子メールアドレス
青色の下線付きテキスト:http://www.hp.com	Webサイトアドレス
*斜体*テキスト	テキスト強調
等幅テキスト	• ファイルおよびディレクトリ名 • システム出力 • コード • コマンド、引数、および引数の値
等幅、*斜体*テキスト	• コード変数 • コマンド変数
等幅、太字テキスト	強調された等幅テキスト

△ **注意:**

指示に従わなかった場合、機器設備またはデータに対し、損害をもたらす可能性があることを示します。

重要:

詳細情報または特定の手順を示します。

注記:

補足情報を示します。

ヒント:

役に立つ情報やショートカットを示します。

Data Protectorグラフィカルユーザーインタフェース

Data Protectorでは、クロスプラットフォーム(WindowsとUNIX)のグラフィカルユーザーインタフェースを提供します。オリジナルのData ProtectorGUIまたはData ProtectorJava GUIを使用できます。Data Protectorグラフィカルユーザーインタフェースに関する詳細は、オンラインヘルプを参照してください。

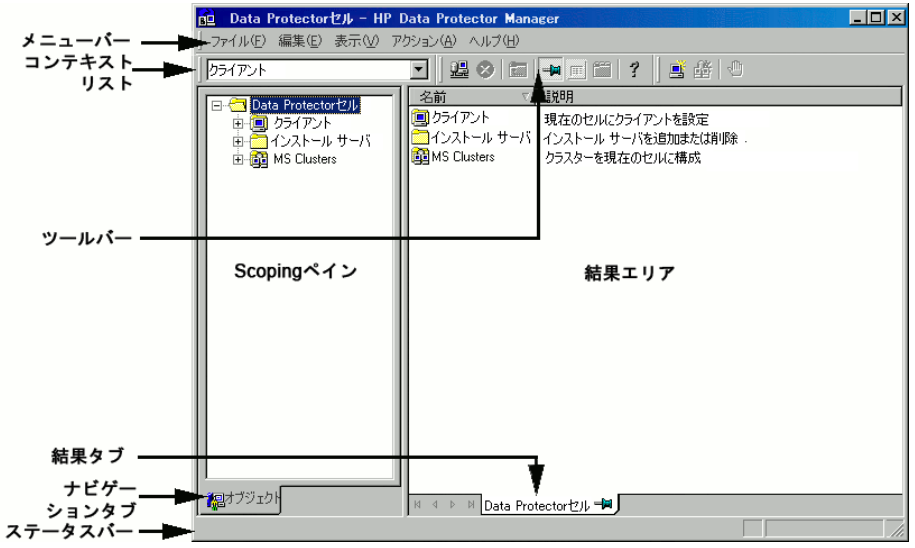


図 1 Data Protectorグラフィカルユーザーインタフェース

一般情報

Data Protectorの概要については、以下のWebサイトでご覧いただけます。http://www.hp.com/go/dataprotector.

HPテクニカル サポート

この製品のテクニカルサポートについては、次のHPサポートのWebサイトに記載されています。

http://www.hp.com/support

HPにお問い合わせになる前に、次の情報を収集してください。

- 製品のモデル名とモデル番号
- テクニカル サポートの登録番号(該当する場合)
- 製品シリアル番号
- エラー メッセージ
- オペレーティング システムの種類とリビジョン レベル
- 質問の詳細

製品サービスへの登録

下記のSubscriber's Choice for BusinessのWebサイトに製品を登録することをお勧めします。

http://www.hp.com/go/e-updates

登録を済ませると、製品のアップグレード、ドライバの新しいバージョン、ファームウェアアップデートなどの製品リソースに関する通知を電子メールで受け取ることができます。

HP Webサイト

その他の情報については、次のHP Webサイトを参照してください。

- http://www.hp.com
- http://www.hp.com/go/software
- http://www.hp.com/support/manuals
- http://h20230.www2.hp.com/selfsolve/manuals
- http://www.hp.com/support/downloads

ご意見、ご感想

HPでは、お客様からのフィードバックを歓迎いたします。

製品ドキュメントについてのご意見、ご感想は、次のアドレスに電子メールでご送信ください。DP.DocFeedback@hp.com.ご送信いただいた内容は、HPに帰属します。

1 概要

概要

この章では、障害復旧プロセス全体の概要を示すとともに、『障害復旧ガイド』で使用されている基本用語について説明し、基本的な障害復旧の方法に関する概要を示します。

コンピュータ障害とは、人為的ミス、ハードウェアまたはソフトウェア障害、ウィルス、自然災害などにより、コンピュータシステムがブート不可能な状態になるイベントを指します。このような場合、システム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くなり、標準的な復元操作を行う前に環境の復旧が必要となります。このためには、ブートパーティションの再作成や再フォーマット、環境を定義するすべての構成情報を含めたオペレーティングシステムの再構築などを実行する必要があります。*最初にこの作業を完了しておかなければ、その他のユーザーデータを復旧できません。*

オリジナルシステムとは、システムでコンピュータ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、ブート不可能な状態になっているため、Data Protector の障害復旧は、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。

注記:

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障害復旧リに使用される、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クライアントを障害から復旧するときのフェーズ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。

障害復旧オペレーティングシステム(DR OS)とは、障害復旧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障害復旧を実行する前に、インストールおよび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元の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障害復旧処理に使用されるだけでなく、自身の構成データをオリジナルシステムの構成データと置き換えて、復元されたシステムの一部となります。

重要なボリュームとは、システムファイルおよびData Protectorファイルのブートに必要なボリュームです。オペレーティングシステムの種類に関係なく、以下のボリュームがクリティカルボリュームとなります。

- ブートボリューム
- システムボリューム
- Data Protectorの実行可能ファイルがインストールされているボリューム
- IDBがあるボリューム(Cell Managerのみ)

注記:

IDBが複数のボリューム上にある場合は、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になります。

Windows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。サービスは、CONFIGURATIONバックアップの一部としてバックアップされます。

CONFIGURATIONに含まれる一部の項目は、システム、ブート、Data Protector、IDBボリュームとは異なるボリュームにある場合があります。この場合、以下のボリュームもクリティカルボリュームの一部となります。

- ユーザープロファイルボリューム
- Windows Server 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上のアクティブディレクトリサービスボリューム
- Microsoft Cluster Server の定数ボリューム

オンライン復旧は、Cell Managerがアクセス可能な場合に行います。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およびSCSIライブラリデバイスのみが使用可能です。Cell Managerの復旧は常にオフラインで行うことに注意してください。

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、障害復旧プロセスは**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。

障害は常に重大な問題ですが、以下の要因により状況は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。
- 障害復旧を実行するために必要な手順に管理者が十分精通していない。
- 障害復旧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。

障害復旧は複雑な作業であり、事前に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。したがって、障害に備えたり、障害から回復するためには、十分に整備された段階的な復旧プロセスを完備しておくことが必要です。

障害復旧プロセス

障害復旧プロセスは4つのフェーズに分けられます。

- **フェーズ0** は、障害復旧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*プランニングと準備を実施しておく必要があります。
- まず**フェーズ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。
- フェーズ2では、オペレーティングシステムと、Data Protectorを含む環境を定義するすべての構成情報が(もとの通り)復元されます。(**フェーズ2**)。

- 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となります(**フェーズ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。

障害復旧の方法

この項では、基本的な障害復旧の方法に関する全般的な概要を示します。個々のオペレーティングシステムでサポートされる障害復旧の手法のリストについては、『*HP Data Protector product announcements ソフトウェアノートおよびリファレンス*』のサポート一覧か以下のWebサイトを参照してください。

http://www.hp.com/support/manuals

注記:

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、あらかじめ確認してください。

表3(26ページ)は、Data Protectorの障害復旧の方法に関する概要を示しています。

表 3 障害復旧の方法に関する概要

フェーズ0	フェーズ1	フェーズ2	フェーズ3
手動による障害復旧			
フルクライアントバックアップ、IDBバックアップ(Cell Managerのみ)。SRDファイルを更新します(Windows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。	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、オリジナルの記憶データ構造を再確立します。	drstart コマンドを実行して、クリティカルボリュームを自動復旧します。高度な復旧作業を実行するには、追加の手順が必要になります。	Data Protector 標準復元手順を使用して、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。
「Windowsシステムの半自動障害復旧」(41ページ)または「UNIX Cell Managerの手動による障害復旧」(125ページ)を参照してください。			

フェーズ0	フェーズ1	フェーズ2	フェーズ3
ディスクデリバリーによる障害復旧(DDDR)			
フルクライアントバックアップ、IDBバックアップ(Cell Managerのみ)。補助ディスクを作成します(UNIXのみ)。	***Windowsの場合:*** 交換ディスクをホストシステムに接続します。 ***UNIXの場合:***補助ディスクをターゲットシステムに接続します。 すべてのシステム: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。	***Windowsの場合:*** DDDRウィザードを使ってクリティカルボリュームを復元した後、交換ディスクをホストシステムから取り外してターゲットシステムに接続します。 ***UNIXの場合:***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。 すべてのシステム:システムをリブートします。 高度な復旧作業を実行するには、追加の手順が必要になります。	Data Protector 標準復元手順を使用して、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。
「Windowsクライアントのディスクデリバリーによる障害復旧 」(50ページ)または「UNIX Cell Managerの手動による障害復旧」(125ページ)を参照してください。			
拡張自動障害復旧(EADR)			
フルクライアントバックアップ、IDBバックアップ(Cell Managerのみ)。SRD を準備して更新します。DR CDを準備します。	DR CD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。 高度な復旧作業を実行するには、追加の手順が必要になります。	Data Protector 標準復元手順を使用して、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。
(「Windowsシステムの拡張自動障害復旧」(54ページ)を参照)。			
ワンボタン障害復旧(OBDR)			
ODBRウィザードによるフルクライアントバックアップ。SRD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 標準復元手順を使用して、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。

フェーズ0	フェーズ1	フェーズ2	フェーズ3
(「Windowsシステムのワンボタン障害復旧」(70ページ)を参照)。			
自動システム復旧(ASR)			
フルクライアントバックアップ。更新済みのSRDファイルとDPバイナリが書き込まれたASRフロッピーディスクを準備します。	Windowsインストールメディアからシステムをブートし、ASRモードに切り替えます。ASRフロッピーディスクを使用します。	クリティカルボリュームが復元されます。高度な復旧作業を実行するには、追加の手順が必要になります。	Data Protector 標準復元手順を使用して、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。
(「自動システム復旧」(84ページ)を参照)。			

次のフェーズに進む前に、以下の作業を完了する必要があります。

- *フェーズ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上のディスクデリバリーによる障害復旧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。

- *フェーズ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障害復旧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。

- *フェーズ2*:

  クリティカルボリュームが復元されます。高度な復旧作業を実行するには、追加の手順が必要になります。詳細は、「高度な復旧作業」(94ページ) を参照してください。

- *フェーズ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)。

手動による障害復旧の方法

手動による障害復旧は、基本的かつ柔軟性に優れた障害復旧の方法です。ターゲットシステムをオリジナルシステムの構成に復旧します。

最初に、DR OSをインストールして構成する必要があります。次に、Data Protectorを使ってデータを復元し(オペレーティングシステムファイルを含む)、現在のオペレーティングシステムファイルを、復元し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障害復旧

この方法は、WindowsクライアントおよびUNIXクライアント上でサポートされています。

Windowsクライアントの場合は、影響を受けたシステム上のディスク(またはディスクが物理的に損傷している場合は交換用のディスク)を、ホストシステムに一時的に接続します。復元後、新しいディスクを障害が発生したシステムに接続し、ブートします。

UNIXシステムの場合は、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エージェントがインストールされた補助ディスクを使用して、ディスクデリバリーによる障害復旧を実行します。

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。Windowsシステムでは、オペレーティングシステムの状態も自動的に復元されます。

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。

(「Windowsクライアントのディスクデリバリーによる障害復旧 」(50ページ)を参照)。

ワンボタン障害復旧(OBDR)

ワンボタン障害復旧(OBDR とは、WindowsクライアントとCell Manager用に自動化されたData Protector 復旧方法で、ユーザーが介在する手間は最小限に抑えられています。

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障害復旧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、障害復旧オペレーティングシステム(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バックアップ時と同じ状態に復元します。

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、新しいOBDRブートテープを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。

自動システム復旧(ASR)

自動システム復旧(ASR)はWindowsシステム上の自動システムで、障害発生時にディスクをオリジナルの状態に再構成(または、新しいディスクがオリジナルのものより大きい場合、パーティションをサイズ変更)します。この処理には、ディスクのパーティション化と論理ボリュームの構成(ファイル形式、ドライブ文字の割り当て、ボリュームマウントポイント、およびボリューム特性)が含まれます。このようにASRはData Protectorのdrstartコマンドにより、Data Protector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するアクティブなDR OSをインストールすることができます。

Data Protector は次に、ターゲットシステムを元のシステム構成に復旧し、最後にユーザーデータを復元します。

拡張自動障害復旧(EADR)

拡張自動障害復旧(EADR)では、Windowsクライアント用とCell Manager用の自動化されたData Protector復旧手法により、ユーザーの操作が最小限に抑えられます。

Windowsプラットフォーム用のEADR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。CONFIGURATION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、セル内のバックアップ対象の各クライアントごとに1つの大きな**DR OSイメージファイル**にパックされ、バックアップテープに(オプションでCell Managerにも)保存されます。

イメージファイルに加え、ディスクの適切なフォーマットとパーティション作成に必要なフェーズ1開始情報(**P1S**ファイルに保存)がCell Managerに保存されます。障害が発生した場合、EADRウィザードで、DR OSイメージをバックアップメディア(フルバックアップ時にCell Managerに保存されていない場合)から復元し、それを**障害復旧CD ISOイメージ**に変換します。CD ISOイメージは、CD書き込みツールでCDに保存して、ターゲットシステムのブートに使用します。

次にData Protectorは、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、最後にオリジナルシステムをバックアップ時と同じ状態に復旧します。

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 CD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。

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 を含むパーティション

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。

Data Protector統合ソフトウェアと障害復旧

障害復旧は、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、障害復旧を成功させるには、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。

障害復旧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. 障害復旧を実行します。
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。HP 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。

2 障害復旧のプランニングと準備

この章の内容

迅速かつ効率的に復元が実行できるよう、この章で説明する手順に従って、障害復旧に対する準備作業を行ってください。準備作業はどの障害復旧の方法でも大きな違いはありませんが、詳細な障害復旧プランの作成、整合性と関連性を兼ね備えたバックアップの実行、SRDファイルの更新(Windowsの場合)は、必ず行うようにしてください。

この章では、すべての障害復旧の方法に共通する一般的な準備手順を説明します。それぞれの障害復旧の方法について、個別に追加手順が必要です。追加手順については対応する項を参照してください。

計画

綿密な障害復旧プランの作成は、障害復旧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障害復旧を行うには、以下の手順で行います。

1. **プラン**

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

   - 復旧が必要なシステム、復旧の時間および度合いの決定。重要なシステムは、ネットワークが正しく機能するために必要なすべてのシステム(DNSサーバー、ドメインコントローラ、ゲートウェイなど)、Cell ManagerおよびMedia Agentクライアントです。
   - 復旧方法の決定 (必要な準備に影響します)。
   - 復旧に必要な情報の取得方法の決定。この情報には、IDBが含まれているメディア、更新されたSRDファイルの位置、Cell Managerバックアップメディアの位置とラベルなどがあります。
   - 復旧プロセスの指針となる、段階を追った詳細なチェックリストの作成。
   - 復旧が実際にうまくいくことを確認するテストプランの作成と実行。

2. **復旧の準備**

   使用する復旧方法により、準備には以下のような作業が含まれます。

   UNIXの場合:

   - 補助ディスクなどのツールの作成。補助ディスクには、最低限のオペレーティングシステム、ネットワーク機能、Data Protector Disk Agentをインストールします。
   - データ記憶構造などクライアント固有の準備データ収集を行う、実行前スクリプトの作成。

   Windowsの場合:

   - **システム復旧データ(SRD)**の更新と安全な場所への保存。セキュリティ上の理由から、SRDファイルへのアクセスは制限する必要があります。

   すべてのシステム:

   - 定期的で整合性のとれたバックアップの実行。

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い、影響を受けたシステムを復旧します。

整合性と関連性を兼ね備えたバックアップ

障害が発生した場合、ターゲットシステムを最新の有効なバックアップ時点の状態に戻さなければなりません。また、システムが最新の有効なバックアップ直前と同様に機能するようにする必要もあります。

注記:

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(HP-UXの実行レベル2におけるライセンスサーバーなど)。このような初期プロセスは、実行時にデータをメモリに読み込み、「ダーティフラグ」をファイルに書き込むこともあります。また、標準的な動作段階(標準実行レベル4)で行われたバックアップでは、適切なアプリケーションが正常に起動しません。この例で言えば、ライセンスサーバーがこのような疑似復旧後に起動された場合、ライセンスサーバーはデータが不整合であると認識し、サービスを予定どおりに実行できません。

Windows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。ログインアカウントを変更するか、関連するサービスを停止する必要があります。

バックアップ実行時にシステム上でどのプロセスが起動しているかによって異なりますが、アプリケーションに対するデータの整合性は維持されない可能性があります。したがって、復旧後、再起動や実行に関する問題が発生します。

整合性と関連性を兼ね備えたバックアップの作成

- 最も適切な方法として、関連するパーティションをオフラインに設定してバックアップする方法がありますが、通常はこの方法は実行できません。
- バックアップ時のシステム上の動作状況を調べます。バックアップ実行中に稼動できるのは、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のみです。
- UNIXの低水準アプリケーションやWindowsのバックグラウンドレベルアプリケーションに固有のサービスは実行できません。

整合性と関連性を兼ね備えたバックアップに何を含めるべきかは、使用する予定の障害復旧の方法や他のシステム仕様 (Microsoft Clusterの障害復旧など) に依存します。特定の障害復旧の方法に関連する項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、障害復旧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、障害復旧の手順が中断してしまいます。

Data Protector A.06.11では、Data Protector A.06.00 から暗号化モデルが変更されています。暗号化キーはCell Managerに保存されます。したがって障害復旧クライアントをCell Managerに接続して暗号化キーを取得するか、リムーバブルメディアの暗号化キーを使用する必要があります。暗号化の詳細については、オンラインヘルプの索引キーワード「暗号化」で表示される内容を参照してください。

2 つの障害復旧のシナリオが考えられます。

- Cell Manager への接続を確立可能な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ため、このようなシナリオには、追加の暗号化に関連する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障害復旧。プロンプトが表示されたら、暗号化キーを入力する必要があります。

  暗号化キーは、障害復旧ISOイメージの一部ではなく、キーファイルにエクスポートされます。このキーは、別のリムーバブルメディアに手動で保存する必要があります。障害復旧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、障害復旧は実行できなくなります。

システム復旧データ(SRD)の更新と編集

システム復旧データ(SRD)とは、Windowsターゲットシステムの構成と復元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、Windowsクライアント上でCONFIGURATIONバックアップを実行したときに生成され、以下の場所に保存されます。

- WindowsCell Managerの場合: Data_Protector_home¥Config¥server¥dr¥srd
- UNIX Cell Manager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ファイルの名前は、このファイルが作成されたコンピュータのホスト名と同じです(computer.company.comなど)。

CONFIGURATIONバックアップの後、SRDには、DR OSのインストールに必要なシステム情報だけが保存されます。障害復旧を実行するには、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クライアントでしか更新できません。更新されたSRDファイルの名前は、recovery.srdです。

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
- 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)

[SRDファイルの更新]ウィザードによる更新

[SRDファイルの更新]ウィザードを使ってSRDファイルを更新するには、以下の手順を行います。

1. [Data ProtectorManager]で[復元]コンテキストを選択し、**[タスク]**ナビゲーションタブをクリックします。
2. [タスク]ナビゲーションタブのScopingペインで、**[障害復旧]**を選択します。
3. 結果エリアで **[SRDファイルの更新]**オプションボタンを選択し、クライアントを選択した後、**[次へ]**をクリックします。

4. 各クリティカルオブジェクトごとにオブジェクトのバージョンを選択して、[次へ]をクリックします。
5. 更新したSRDファイルの保存先ディレクトリを入力して、[完了]をクリックします。

重要:

SRDファイルはCell Managerシステムに保存されるため、Cell Managerに障害が発生した場合は、このファイルにアクセスできなくなります。したがって、Cell Manager'のSRDファイルのコピーを別途作成しておくことが必要です。障害復旧に備えた準備の一環として、更新されたSRDファイルは、Cell Managerだけでなく、セキュリティが確保されている複数の保管先に置いてください。(「準備」(52ページ)を参照)。

omnisrdupdateによる更新

SRDファイルは、omnisrdupdateコマンドをスタンドアロンコマンドとして使用して更新することもできます。omnisrdupdateコマンドは*Data_Protector_home*¥binディレクトリにあります。

あるセッションに所属するバックアップオブジェクト情報が保存されている既存のSRDファイルを更新するには、omnisrdupdateでsession_IDを指定する必要があります。omnisrdupdateは、渡されたsession_IDの値に対応するバックアップオブジェクトの情報が格納されているSRDファイルを更新します。更新されたSRDファイルは、Cell Manager上に保存されます。

この手順は、(SRDファイルで指定されている)すべての重要なバックアップオブジェクトが、指定されたセッション内で実際にバックアップされた場合に限り、正常に実行されます。どのオブジェクトがSRD更新対象のクリティカルオブジェクトとされているかを調べるには、テキストエディタを使ってSRDファイルを開き、オブジェクトに関する部分(section objects)を参照します。この部分に、SRD更新対象のクリティカルオブジェクトがすべてリストされています。データベースは “/” で示されています。

SRDファイルのオブジェクトに関する部分は以下のようになります。

```
-section objects
-objcount 3
-object /C -objtype 6 -objpurpose 283
-endobject /C
-object / -objtype 3 -objpurpose 32
-endobject /
-object /CONFIGURATION -objtype 6 -objpurpose 4
-endobject /CONFIGURATION
-endsection objects
```

この場合、/C、/(データベース)、/CONFIGURATIONの3つの重要なオブジェクトがあります。

ヒント:

セッションIDを取得するには、omnidbコマンドを-sessionオプションを付けて実行します。最新のセッションIDを取得する場合は、コマンドプロンプトから「omnidb -session -latest」と入力してください。

更新済みのSRDファイルは、障害に備えて安全な場所に保存しておくことが必要です。更新済みSRDファイルの保存場所を指定するには、omnisrdupdateコマンドに-locationオプションを付けて実行します。-locationパラメータは複数指定できます(書き込み権限を持っているネットワーク共有を含む)。パラメータで指定した各保存場所に、更新済みSRDファイルのコピーが保存されます。(「準備」(52ページ)を参照)。

Cell Manager上のSRDファイルをどのホスト名で更新するかを指定するには、omnisrdupdateコマンドで-hostオプションを使用します。ホスト名を指定しなかった場合は、ローカルホストとみなされます。Cell Manager 上のSRDファイルは更新されません。

例

ホスト名がcomputer.company.comというクライアントの2002/05/02-5セッションに属するバックアップオブジェクト情報でSRDファイルを更新して、更新済みのSRDファイルのコピーをフロッピーディスクとホスト名がcomputer2というコンピュータのSRDfiles共有ディスクに保存するには、次のコマンドを実行してください。

```
omnisrdupdate -session 2002/05/02-5 -host computer.company.com -location a:-location ¥¥computer2¥SRDfiles
```

共有ディスクに対して書き込み権限があることを確認してください。

実行後スクリプトによる更新

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.exe」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が環境から自動的に取得されるので、ユーザーがセッションIDを指定する必要はありません。

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 *name*)の場合と同様に指定できます。

SRDファイルの編集

障害復旧を実行する時点で、SRDファイルに保存されているバックアップデバイスまたはメディアに関する情報が古くなっている場合もあります。その場合は、障害復旧を実行する前にSRDファイルを編集して、関連する情報を正しい情報に置き換えてください。(「編集後のSRDファイルを使用した復旧」(105ページ)を参照)。

重要:

セキュリティ上の理由から、SRDファイルへのアクセスは制限する必要があります。

3 Windows上での障害復旧

Windowsシステムの半自動障害復旧

この項では、Windowsシステム上での半自動障害復旧の準備と実行方法について説明します。サポート対象のオペレーティングシステムは、『*HP Data Protector product announcements 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。

概要

Windowsクライアントの障害復旧を半自動的に実行する手順の概要は、以下のとおりです。

1. **フェーズ0**
   a. 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)を実行します。
   b. SRDファイルを更新します。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。
2. **フェーズ1**
   a. 障害が発生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。(必要なパーティション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:**
> **手動障害復旧のフェーズ1は、自動展開ツールと組み合わせて使用できます。**

3. **フェーズ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、システムのクリティカル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の復旧作業か高度な復旧作業を行う場合は、特別な手順が必要となります。詳細については、「高度な復旧作業」(94ページ)を参照してください。

4. **フェーズ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標準復元手順を使用します。

要件

- パーティションのサイズは、障害が発生したディスクのパーティションサイズと同じかそれより大きくなければなりません。これにより、障害が発生したディスクに保存されていた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形式(FAT、NTFS)と、ボリュームの圧縮属性も一致していることが必要です。
- ターゲットシステムのハードウェア構成は、障害発生前の状態と同じでなければなりません。これには、SCSIのBIOS設定(セクタの再マッピング)も含まれます。
- ボリュームマウントポイントは自動では復元されません。このため、障害が発生する前にボリュームマウントポイントが作成されていた場合は、それらのマウントポイントを最初に再作成してから、障害復旧の手順を開始する必要があります。マウントポイントを再作成しないと、データの復元先が不正確になる可能性があります。

制限事項

- Internet Information Server (IIS)データベース、ターミナルサービスデータベース、Certificate Serverデータベースは、フェーズ2で自動的には復元されません。これらをターゲットシステムに復元するには、Data Protector 標準復元手順を実行してください。

準備

障害復旧が正しく実行されるよう準備するには、一般的な準備に関する手順と、特定の障害復旧の方法を使用するための要件に関連する手順を実行することが必要です。迅速かつ効率的に障害復旧を実行するには、事前の準備が必要です。Cell ManagerとMicrosoft Cluster Serverの障害復旧の準備にも十分な注意が必要です。

△ 注意:

障害が発生してから障害復旧の準備をしても遅すぎます。

この項で挙げられている手順を完了する前に、すべての障害復旧の方法に共通する一般的な準備手順として「計画」(33ページ)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、ブート可能なWindowsインストール用CD-ROMが必要です。ブート可能なCD-ROMがない場合は、フロッピーディスクからシステムを起動する標準手順を実行してください。
2. 復旧対象のシステムに適したドライバがあることを確認します。Windows のセットアップ中、ネットワーク、HBA、SCSIドライバなど、いくつかのドライバをインストールする必要があります。
3. 影響を受けたシステムを復旧するには、障害発生前のシステムに関する以下の情報が必要です(SRDファイルにも保存されています)。
   - 障害発生前にDHCPが使用されていなかった場合 – TCP/IPのプロパティ(IPアドレス、デフォルトゲートウェイ、サブネットマスク、DNS の順序)
   - クライアントのプロパティ(ホスト名)

4. 以下の条件が当てはまることを確認します。

   - 正常に実行されたクライアントのフルバックアップがあること。～を参照してください。

     オンラインヘルプの索引「バックアップ、Windows固有」および「バックアップ、構成」を参照してください。

   - 正常に実行されたバックアップセッションに含まれるバックアップオブジェクトに関する情報を使って更新されたSRDファイルが必要です。(「システム復旧データ(SRD)の更新と編集」(36ページ)を参照)。
   - Cell Managerを復旧する場合は、正常に実行されたCell ManagerのIDBバックアップが必要です。オンラインヘルプの索引IDBバックアップの構成方法および実行方法の詳細は、「IDB、構成」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)以下のものが含まれている必要があります。
     - すべてのノード
     - 管理仮想サーバー(管理者が定義)
     - Cell Manager仮想サーバーとIDB(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)

     詳細については、「Microsoft Cluster Serverの復元に固有の手順」(94ページ)を参照してください。
   - ブートパーティションのあるディスクには、Data Protector障害復旧ユーティリティのインストール(15MB)とアクティブDR OSインストールに必要な空きディスクスペースが必要です。また、元のシステムの復元に必要な空きディスクスペースも別途必要です。

5. 32ビットプラットフォームで実行するWindowsシステムについては、Data_Protector_program_data¥Depot¥DRSetupX86(Windows Server 2008の場合)、Data_Protector_home¥Depot¥DRSetupX86(その他のWindowsシステムの場合)、または¥i386¥tools¥DRSetupX86(Data Protectorインストール用メディアの場合)の内容を、3枚のフロッピーディスク(**drsetupディスケット**)にコピーします。AMD64/Intel EM64Tプラットフォームで実行するWindowsシステムについては、Data_Protector_program_data¥Depot¥DRSetupX64(Windows Server 2008の場合)、Data_Protector_home¥Depot¥DRSetupX64(その他のWindowsシステムの場合)、または¥i386¥tools¥DRSetupX64(Data Protectorインストール用メディアの場合)の内容を、4枚のフロッピーディスクにコピーします。Itaniumプラットフォームで実行するWindowsシステムについては、Data_Protector_program_data¥Depot¥DRSetupIA64(Windows Server 2008の場合)、Data_Protector_home¥Depot¥DRSetupIA64(その他のWindowsシステムの場合)、または¥i386¥tools¥DRSetupIA64(Data Protectorインストール用メディアの場合)の内容を、6枚のフロッピーディスクにコピーします。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。どのWindowsシステムの場合でも、1つのサイトにつき必要なdrsetupディスクは1セットだけです。ただし、1枚目のフロッピーディスク上に、影響を受けたクライアントの更新されたSRDファイルを必ずコピーしておいてください。SRDファイルが複数ある場合は、適切なバージョンを選ぶようにData Protectorが尋ねてきます。

6. ディスクパーティションを障害発生前の初期状態に再構成するため、各パーティションごとに以下の情報を記録しておきます(この情報は復旧プロセスで必要になります)。
   - 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、特定のパーティションのファイルシステムの種類が分かります。

表 4 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、障害復旧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。半自動障害復旧の準備に使用できる空のテンプレートについては、「Windowsでの手動による障害復旧準備用テンプレート」(145ページ) を参照してください。

表 5 半自動障害復旧準備用テンプレートの例

クライアントプロパティ	コンピュータ名	ANDES
	ホスト名	andes.company.com
ドライバ		hpn.sys、hpncin.dll
Windows Service Pack		Windows SP3

TCP/IPのプロパティ	IPアドレス	3.55.61.61
	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 の順序	11.17.3.108, 11.17.100.100
メディアラベル / バーコード番号		″andes – disaster recovery″ / [000577]
パーティション情報と順序	最初のディスクラベル	
	第1パーティションの長さ	31 MB
	第1ドライブの文字	
	第1ファイルシステム	EISA
	2番目のディスクラベル	BOOT
	第2パーティションの長さ	1419 MB
	第2ドライブの文字	C:
	第2ファイルシステム	NTFS/HPFS
	3番目のディスクラベル	
	第3パーティションの長さ	
	第3ドライブの文字	
	第3ファイルシステム	

復旧

以下の手順に従って、半自動障害復旧を使ってWindowsシステムを復旧します。高度な復旧作業(Cell ManagerまたはIISの復旧など)を行おうとしている場合は、「高度な復旧作業」(94ページ)も参照してください。

1. CD-ROMからWindowsシステムをインストールし、必要に応じてドライバを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にInternet Information Server(IIS)をインストールしないでください。詳細は、「Internet Information Server (IIS) の復元に固有の手順」(104ページ)を参照してください。

重要:

Windowsの無人セットアップを使用してWindowsがインストールされている場合、復旧時にWindowsのインストールに使用したスクリプトと同じものを使用して、$SystemRoot$フォルダと%SystemDrive%¥Documents and Settingsフォルダが同じ場所にインストールされるようにします。

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上にベンダー固有のパーティション(EISA Utility Partitionなど)があった場合は、SRDファイルから収集したEUP情報に基づいて、“ダミー”のFATパーティションを作成し(障害発生により失われた場合)、フォーマットします。EUPはあとから、“ダミー”パーティションによって保持され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すぐに、ブートパーティションを作成およびフォーマットしてください。詳細は、「準備」(52ページ)を参照してください。
   - 障害発生前のシステム上にEUPがなかった場合は、障害発生前の状態になるようブートパーティションを作成し(障害発生により失われた場合)、フォーマットします。詳細は、「準備」(52ページ)を参照してください。

   Windows を元の位置(つまり、障害発生前の元のシステムとドライブ文字およびディレクトリが同じ位置)にインストールします。この情報は、SRDファイルに保存されています。

注記:

インストール時には、障害発生前にWindowsドメインが置かれていた場所にシステムを追加せずに、ワークグループに追加してください。

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、影響を受けたクライアントのホスト名、そのIPアドレス、デフォルトゲートウェイ、サブネットマスク、DNSサーバーに関する情報を設定して、障害発生前と同じようにTCP/IPプロトコルを構成します。[このコンピュータのプライマリ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。

> **注記:**
>
> **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のAdministratorsグループ内に障害復旧用の一時的なアカウントを作成し、Cell Manager上でData ProtectorのAdminグループに追加します。オンラインヘルプの索引「追加、Data Protectorユーザー」を参照してください。

   障害発生前にシステム上に存在していなかったアカウントを使用する必要があります。この一時的な*Windows*アカウントは、この手順の後半で削除します。

5. ログオフした後、新規作成したアカウントを使用してシステムにログインします。
6. 障害発生後にバックアップデバイスを変更したなどの理由でSRDファイルの情報が最新のものでなく、オフライン復旧を実行しようとしている場合は、この手順を続行する前にSRDファイルを変更してください。(「編集後のSRDファイルを使用した復旧」(105ページ)を参照)。
7. Data_Protector_home¥Depot¥drsetup¥Disk1(Windows Cell Manager)または¥i386¥tools¥drsetup¥Disk1(Data Protectorインストール用メディア)のいずれかのディレクトリからdrstartコマンドを実行します。drsetupディスクが用意されている場合は(「準備」(42ページ)を参照)、drstartコマンドを実行することもできます。
8. drstartは、まず現在の作業ディレクトリ、フロッピーディスク、CD-ROMドライブをスキャンして、障害復旧用セットアップファイル(Dr1.cabとomnicab.ini)の位置を調べます。必要なファイルが見つかった場合、drstartユーティリティは障害復旧用ファイルを%SystemRoot%¥system32¥OB2DRディレクトリにインストールします。drstart.exeがファイルを見つけられない場合は、[DR Installation Source]テキストボックスにパスを入力するか、ブラウズしてファイルを選択します。

9. recovery.srdファイルがdr1.cabおよびomnicab.iniファイルと同じディレクトリに保存されている場合は、drstartによりrecovery.srdファイルが%SystemRoot%¥system32¥OB2DR¥binディレクトリにコピーされ、omnidrユーティリティが自動的に起動されます。そうでない場合は、SRDファイル(recovery.srd)の場所を[SRD Path]フィールドに入力するかブラウズして選択し、［次へ］をクリックします。

   フロッピーディスクにSRDファイルが複数ある場合は、適切なバージョンを選ぶようにData Protectorが尋ねてきます。

   omnidr が正常終了した後、システムを正しくブートするのに必要なすべてのクリティカルオブジェクトが復元されます。

10. ステップステップ 4 で追加した一時ユーザーアカウント*Data Protector*をCell Manager上のData ProtectorAdminグループから削除します(このアカウントが障害復旧前にもCell Manager上に存在していなかった場合)。

11. システムを再起動し、ログオンして、復元されたアプリケーションが実行されているか検証します。

12. Cell Manager の復旧、または高度な復旧作業(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、特別な手順が必要となります。詳細については、「Data Protector Cell Manager 固有の復元手順 」(101ページ)と「高度な復旧作業」(94ページ)を参照してください。

13. Data Protectorを使って、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DR OSは、以下の場合を除いて、最初のログイン後に削除されます。

- 障害復旧ウィザードが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の10秒間のポーズの間に、ユーザーがウィザードを中断して**[デバッグを使用](Use Debugs)**オプションを選択した場合。
- omnidrコマンドを、no_resetまたはdebugオプションを付けて手動で起動した場合。
- 障害復旧が失敗した場合。

Windowsクライアントのディスクデリバリーによる障害復旧

ディスクデリバリーによるデ障害復旧を実行するには、現在稼働中のData Protectorクライアント(Data Protector障害復旧ホスト)を使って、新しいディスクをこのクライアントに接続した状態で作成します。管理者は、ディスクのフォーマットおよびパーティションの構成が正しく行われるよう、障害発生前に十分なデータを収集する必要があります。ただし、Data ProtectorによりCONFIGURATIONバックアップの対象として関連情報が自動的に保存されます。

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 を含むパーティション

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。

サポート対象のオペレーティングシステムは、『*HP Data Protector product announcements 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。

ヒント:

この方法は、ホットスワップハードディスクドライブとともに使用すると非常に便利です。システムの電源を切らずに稼動させたまま、ハードディスクドライブをシステムから外して、新しいハードディスクドライブを接続できるためです。

概要

Windowsクライアントの障害復旧にディスクデリバリーを使用する手順の概要は、以下のとおりです。

1. **フェーズ0**
   a. 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)を実行します。
   b. 各パーティションに関して必要な情報を収集します。
2. **フェーズ1**
   a. ホストシステムに交換ディスクを接続します。
   b. 交換ディスク上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ます。Windowsマウントポイントの詳細については、オンラインヘルプの索引「TBD」を参照してください。
3. **フェーズ2**
   a. Data Protector ディスクデリバリーウィザードを使用して、オリジナルシステムのクリティカルディスクを交換ディスクに復元します。
   b. ホストシステムをシャットダウンした後、交換ディスクを取り外してターゲットシステムに接続します。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. 交換したディスクからターゲットシステムを再起動します。
4. **フェーズ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標準復元手順を使用します。

要件

- パーティションのサイズは、障害が発生したディスクのパーティションサイズと同じかそれより大きくなければなりません。これにより、障害が発生したディスクに保存されていた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形式(FAT、NTFS)が一致していることが必要です。
- ディスクが作成されたシステムおよびディスクが使用されているシステムでは、同じセクタのマッピング/アドレッシングを使用する必要があります(有効化/無効化されたSCSI BIOS、EIDE: 両方のシステムとも同じアドレッシングモード(LBA、ECHS、CHS)を使用する必要があります)。

制限事項

- ディスクデリバリーによる障害復旧は、Microsoft Cluster Serverではサポートされていません。
- RAIDはサポートされていません。これには、ソフトウェアRAID(フォールトトレラントボリュームおよびダイナミックディスク)も含まれます。
- Internet Information Server(IIS)データベース、ターミナルサービスデータベース、Certificate Serverデータベースは、フェーズ2で自動的には復元されません。これらをターゲットシステムに復元するには、Data Protector 標準復元手順を実行してください。

準備

障害復旧の準備としていくつかの手順を実行します。この項で挙げられている手順を完了する前に、すべての障害復旧の方法に共通する一般的な準備手順として「計画」(33ページ)も参照してください。

重要:

障害復旧の準備は、障害が発生する*前*に行っておく必要があります。

障害から迅速かつ効率的に復旧するには、以下が必要です。

- 最新かつ有効な、復旧対象のクライアントのフルバックアップ
- 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
- Data Protectorホストシステムは、影響を受けたクライアントとオペレーティングシステムが同じで、新しいディスクの接続に必要なハードウェアI/Oパスも一致している必要があります。

ディスクパーティションを障害発生前の初期状態に再構成するため、各パーティションごとに以下の情報を記録しておきます(この情報は復旧プロセスで必要になります)。

- 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

表5(46ページ) に、ディスクデリバリーによる障害復旧の準備の例を示します。障害復旧の準備に使用できる空のテンプレートについては、「Windowsでの手動による障害復旧準備用テンプレート」(145ページ)を参照してください。

復旧

この項では、ディスクデリバリーによる障害復旧を使ってWindowsクライアントを復旧する手順を説明します。「高度な復旧作業」(94ページ)も参照してください。

Windows上でのディスクデリバリーによる障害復旧では、Data Protector障害復旧ホスト(DRホスト)を使用して、影響を受けたディスクの最新の有効なフルバックアップをクライアントに接続されている新しいハードディスクに復元します。次に、障害が発生したシステム上の影響を受けたディスクを新しいハードディスクと交換します。

実際のディスクデリバリーによる障害復旧は以下の手順で構成されています。

1. DR ホストに新しいディスクを接続します。
2. DRホストを再起動して、新しいディスクを認識させます。
3. 障害復旧ホストのData ProtectorGUIを使って、[復元]コンテキストに切り替え、[タスク]タブをクリックします。Scopingペインで**[障害復旧]**を選択して、ドロップダウンリストからクライアントを選択し、結果エリアで**[ディスクのデリバリーによる障害復旧]**を選択します。
4. 各クリティカルオブジェクトごとに、復元対象のオブジェクトバージョンを選択して、**[次へ]**をクリックします。
5. パーティションをまだ作成していない場合は、ディスクアドミニストレータを使って新しいディスクのパーティションを作成します。このとき、ディスクデリバリーによる障害復旧の準備作業の一環として収集したパーティション情報を使用します。

6. パーティションを作成する際には、フルバックアップが実行される前と同じ順序でパーティションを割り当てる必要があります。これにより、復元後のドライブ文字の再割り当てが円滑に行われるので、boot.iniファイルに設定されているシステムパーティションへのパスが不適切になることによって起こるシステム再起動時の障害を防止できます。

重要:

Windows のマウントポイントにドライブ文字を割り当てます。この場合、各マウントポイントごとにドライブ文字を割り当てることができるよう、十分な未使用のドライブ文字が必要となります。

7. 元のドライブ文字を右クリックして、必要なドライブ文字の割り当てをすべて行います。ホストシステムと元のシステムのドライブ文字が異なる可能性があるために、この作業が必要となります。
8. [**完了**]を選択します。
9. 新しいディスクをDRホストから取り外して、ターゲットシステムに接続します。
10. ターゲットシステムの電源を入れます。
11. 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標準復元手順を使用します。これでクライアントの復旧は完了です。

ディスクデリバリーは、マルチブートシステムのディスクのうち1つで障害が発生したときに、ユーザーが少なくとも1つの構成をブートできる場合にも、有効な手段になります。

注記:

Data Protectorはボリューム圧縮フラグを復元しません。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されて復元されますが、新規ファイルを圧縮ファイルとして作成したい場合は、手動でボリューム圧縮フラグをセットする必要があります。

Windowsシステムの拡張自動障害復旧

Data Protectorには、WindowsCell Manager用やクライアント用に拡張された障害復旧の手順が用意されています。サポート対象のオペレーティングシステムは、『*HP Data Protector product announcements 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。

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。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、セル内のバックアップ対象の各クライアントごとに1つの大きな**DR OSイメージファイル**にパックされ、バックアップテープに(オプションでCell Managerにも)保存されます。

イメージファイルに加え、ディスクの適切なフォーマットとパーティション作成に必要な**フェーズ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。障害が発生した場合、拡張自動障害復旧ウィザードで、DR OSイメージをバックアップメディア(フルバックアップ時にCell Managerに保存されていない場合)から復元し、それを **障害復旧CD ISOイメージ**に変換します。CD ISOイメージは、CD書き込みツールでCDに保存して、ターゲットシステムのブートに使用します。

次にData Protectorは、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、最後にオリジナルシステムをバックアップ時と同じ状態に復旧します。

重要:

バックアップメディア、DRイメージ、SRDファイル、障害復旧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

Windowsクライアントに対して拡張自動障害復旧を行う手順の概要は、以下のとおりです。

1. **フェーズ0**
   a. フルクライアントバックアップを実行します。
   b. 拡張自動障害復旧ウィザードを使用して、影響を受けたシステムのDR OSイメージファイルからDR CD ISOイメージを作成し、CDに書き込みます。DR OSイメージがフルバックアップ中にCell Managerに保存されなかった場合、拡張自動障害復旧ウィザードでは、バックアップメディアからイメージが復元されます。

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て新しいDR CDを作成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、ネットワークが変更された場合も同じです。

c. 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、暗号化キーをリムーバブルメディアに保存して、障害復旧の際に使用できるようにします。Cell Managerの復旧時、またはCell Managerへの接続を確立できない場合には、このキーが必要になります。

2. フェーズ1
   a. 障害が発生したハードウェアを交換します。
   b. 障害復旧CD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。
3. フェーズ2
   a. クリティカルボリューム(ブートパーティション、オペレーティングシステム、およびData Protectorが格納されているパーティション) は自動的に復元されます。
4. フェーズ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、障害復旧CDを準備します。

Cell Managerの復旧の場合は、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クライアントの拡張自動障害復旧に関する制限事項、準備、および、復旧方法を説明します。「高度な復旧作業」(94ページ)も参照してください。

要件

障害復旧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。

- Data Protector 自動障害復旧コンポーネントが、この方法で復旧したいクライアントと、DR CD ISOイメージを作成するシステムにインストールされている必要があります。『*HP Data Protector インストールおよびライセンスガイド*』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は、障害発生前の状態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に交換用ディスクが接続されていること。
- 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。オリジナルパーティショ

ンで[ドライブを圧縮してディスク領域を空ける]オプションを有効に設定していた場合は、少なくとも400MBの領域が必要になります。

- 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パーティションに少なくとも200MB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。
- ブートに必要なドライバは、すべて%SystemRoot%フォルダにインストールされている必要があります。インストールされていない場合は、kb.cfgファイルで指定されている必要があります。(「kb.cfgファイルの編集」(105ページ)を参照)。
- ネットワーク機能が付いたセーフモード、またはディレクトリサービス復元モード(ドメインコントローラのみ)でシステムをブートする場合は、ネットワークが使用可能でなければなりません。ただし、システムのバックアップは通常のブートプロセスの後に実行する必要があります。
- システムのBIOSは、El-Torito標準で定義されているブート可能CDをサポートしている必要があります。また、INT13h機能のXXhにより、LBAアドレッシングを使用しているハードディスクドライブへの読み書きが可能である必要があります。BIOSのオプションは、システムのユーザーマニュアル、またはブート前にシステム設定を調査することでチェックできます。
- オフライン復元を計画している場合は、クライアントバックアップ時のデバイスへの書き込みにはデフォルトのブロックサイズ64KBを使用してください。障害復旧を実行する際にWindowsで使用できるブロックサイズはこのデフォルトのサイズだけです。デフォルトのブロックサイズ64KBが設定されているかどうかを確かめるには、[プロパティ]ボックスの**[拡張...]**を選択します。図2(58ページ)を参照してください。

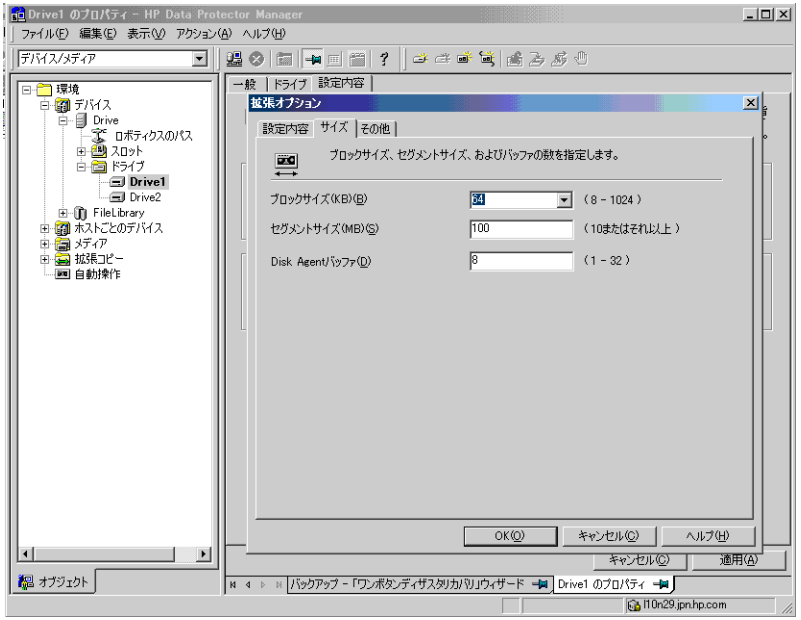


図 2 デフォルトのブロックサイズの確認

- 障害復旧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。.
- クラスター環境では、各クラスターノードのバスアドレス一覧が同じであれば、クラスターノードは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。
  - 同等のクラスターノードのマザーボードハードウェア
  - 両方のノードで同じOSのバージョン(サービスパックおよびアップデート)
  - バスコントローラの数とタイプが同一
  - バスコントローラが同じPCIマザーボードのスロットに挿入されている。
- Windows XP の場合は、オペレーティングシステムがバックアップの時点で起動されておらず、起動期間が終了すると、障害復旧は失敗します。
- Windows VistaまたはWindows Server 2008システム用のISO CD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Windows Automated Installation Kit(WAIK) 1.1がインストールされている必要があります。WAIKの古いバージョンはサポートされていません。
- Windows Vista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

- ダイナミックディスクはサポートされていません(Windows NTからのミラーセットのアップグレードも含む)。
- 新しいディスクのサイズは、影響を受けたディスクのサイズ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。
- 拡張自動障害復旧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、0x12タイプ(EISAを含む)と0xFEタイプのみです。
- 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 (IIS)、ターミナルサービスデータベース、Certificate Serverデータベースは、フェーズ2で自動的には復元されません。これらをターゲットシステムに復元するには、Data Protector標準復元手順を実行してください。
- 障害復旧のISOイメージは、Data ProtectorがFAT/FAT32パーティションにインストールされているシステムには作成できません。障害復旧のイメージを作成するには、Data ProtectorがNTFSボリュームにインストールされているクライアントがセル内に少なくとも1つ必要です。

準備

この項で挙げられている手順を完了する前に、すべての障害復旧の方法に共通する一般的な準備手順として「計画」(33ページ)も参照してください。「高度な復旧作業」(94ページ)も参照してください。

重要:

障害復旧の準備は、障害が発生する*前*に行っておく必要があります。

前提条件

- フルクライアントバックアップを実行します(CONFIGURATIONも含む)。

  オンラインヘルプの索引「バックアップ、Windows固有」および「バックアップ、構成」を参照してください。
- ***Microsoft Cluster Serverの場合***: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)以下のものが含まれている必要があります。
  - すべてのノード

- 管理仮想サーバー(管理者が定義)
- Cell Manager仮想サーバーとIDB(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)

詳細については、「Microsoft Cluster Serverの復元に固有の手順」(94ページ) を参照してください。

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。詳細は、「「EADR 用に全ノードのP1Sファイルをマージ」(98ページ)」を参照してください。

DR IOSイメージファイル

一時 DR OSのインストールと構成に必要なデータ(DRイメージ)は、フルクライアントバックアアップ時に1つの大きなファイルにパックされ、バックアップメディア、さらにオプションでCell Managerにも保存されます。Cell Managerにも、バックアップ仕様にあるクライアントすべての障害復旧イメージを保存したい場合は、以下の手順を実行してください。

1. コンテキストリストで[**バックアップ**]を選択します。
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ます。詳細は、オンラインヘルプの索引「作成、バックアップ仕様」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. **[WinFSオプション]**をクリックし、**[障害復旧イメージ全体をディスクにコピー]**を選択します。
7. Windows VistaまたはWindows Server 2008システム上にあるデータをバックアップする場合、**[NTFSハードリンクを検出]**と[Shadow Copyを使用]も選択し、**[フォールバックを許可]**をクリアします。

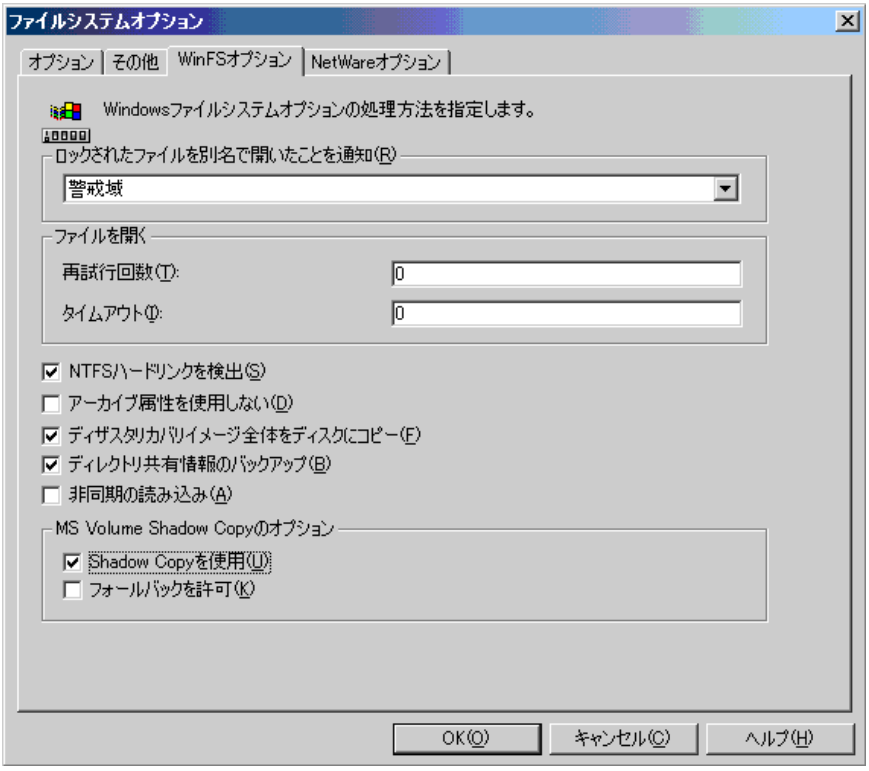


図 3 [WinFSオプション]タブ

バックアップ仕様内の特定クライアントのDRイメージ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**]を選択します。
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ます。詳細は、オンラインヘルプの索引「作成、バックアップ仕様」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. Cell ManagerにDRイメージファイルを保存したいクライアントを選択して、[**プロパティ**]をクリックします。
6. [**WinFSオプション**]をクリックし、[**障害復旧イメージ全体をディスクにコピー**]を選択します。

7. Windows VistaまたはWindows Server 2008システム上にあるデータをバックアップする場合、[**NTFSハードリンクを検出**]と[**Shadow Copyを使用**]も選択し、[**フォールバックを許可**]をクリアします。

障害復旧CDをCell Manager上で作成する場合、障害復旧イメージ全体をCell Managerに保存するのが便利です。そうすればDRイメージはハードディスクから読み込まれ、バックアップメディアから読み込む場合よりもはるかに速く作業が進みます。DRイメージファイルはデフォルトで、Cell ManagerのData_Protector_program_data¥Config¥Server¥dr¥p1sディレクトリ(Windows Server 2008の場合)、Data_Protector_home¥Config¥Server¥dr¥p1s(その他のWindowsシステムの場合)、または/etc/opt/omni/server/dr/p1sディレクトリ(UNIXシステムの場合)に*client name*.imgという名前で保存されます。デフォルトのディレクトリを変更するには、グローバルオプションファイルで新たなグローバル変数EADRImagePath = *valid_path*(EADRImagePath = /home/imagesまたはEADRImagePath = C:¥tempなど)を指定します。詳細は、オンラインヘルプの索引「グローバルオプションファイル、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か(Windowsの場合)、他のボリュームへのリンクを作成(UNIXの場合)できます。

kb.cfgファイル

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(および他の必要ファイル)を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。

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が正常にブートしない、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ります。詳細については、「kb.cfgファイルの編集」(105ページ)を参照してください。

暗号化キーの準備

Cell Manager の復旧またはオフラインクライアントの復旧に対しては、暗号化キーをリムーバブルメディアに保存して、障害復旧の際に使用できるようにする必要があります。Cell Managerの復旧に対しては、事前に (障害が発生する前に)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。このキーは、障害復旧イメージの作成時に、Cell Managerに自動的にエクスポートされます。エクスポート先のファ

イルは、Data_Protector_program_data¥Config¥Server¥export¥keys¥DR-ClientName-keys.csv(Windows Server 2008の場合)、Data_Protector_home¥Config¥Server¥export¥keys¥ DR-ClientName-keys.csv(その他のWindowsシステムの場合)、または/var/opt/omni/server/export/keys/DR-ClientName-keys.csv(UNIXシステムの場合)です。ここで、ClientNameはイメージを作成するクライアントの名前です。

障害復旧の準備のための各バックアップについて、正しい暗号化キーがあることを確認してください。

フェーズ1開始ファイル(P1S)

フルバックアップ中は、DRイメージファイル以外に、フェーズ1開始ファイル(P1S)が作成されます。このファイルは、バックアップメディアおよびCell ManagerのData_Protector_home¥Config¥Server¥dr¥p1sディレクトリ(Windowsシステムの場合)または/etc/opt/omni/server/dr/p1sディレクトリ(UNIXシステムの場合)に保存されます。ファイル名はホスト名と同じです(たとえばcomputer.company.com)。これはUnicode UTF-8でエンコードされたファイルで、システムにインストールされているすべてのディスクのフォーマット/パーティション作成方法に関する情報が含まれています。これに対して更新済みのSRDファイルには、システム情報、およびバックアップオブジェクトと対応するメディアに関するデータのみが含まれています。

障害が発生した場合、障害復旧インストールの際にEADRウィザードを使用して、DRイメージ、SRDファイル、P1Sファイルを**障害復旧CD ISOイメージ**としてマージできます。このイメージはISO9660フォーマットをサポートしているCD書き込みツールでCDに保存できます。この**障害復旧CD**は、自動障害復旧を実行する際に使用します。

重要:

Cell Manager用の障害復旧CDを事前に用意しておく必要があります。

Microsoft Clusterのノード用の障害復旧CDを作成する場合には、特別な手順が必要になります。(「Microsoft Cluster Serverの復元に固有の手順」(94ページ)を参照)。

重要:

セキュリティ上の理由から、バックアップメディア、DRイメージ、SRDファイル、障害復旧CDへのアクセスを制限しておくことをお勧めします。

DR ISOイメージの作成

DR ISOイメージを作成するには、以下の手順を実行します。

1. コンテキストリストで[**復元**]を選択します。
2. [**タスク**]ナビゲーションタブをクリックし、[障害復旧]を選択します。
3. ドロップダウンリストから、DR ISOイメージを準備するクライアントを選択します。
4. [**拡張自動障害復旧**]、[**次へ**]の順にクリックします。
5. 各クリティカルオブジェクトごとに、適切なオブジェクトバージョンを選択して、[**次へ**]をクリックします。
6. Cell ManagerにDRイメージファイルが保存されている場合は保存ディレクトリを指定するか、ブラウズします。それ以外の場合は、[Restore image file from a backup]をクリックします。[**次へ**]をクリックします。
7. DR ISOイメージ(recovery.iso)の保存先のディレクトリを選択します。

   Windows VistaおよびWindows Server 2008システム:

   WAIKオプションの指定:

   - Windows自動インストールキット(WAIK)ディレクトリ

     場所を入力すると、その場所がData Protectorに保存され、DR ISOイメージが次回作成されるときに、デフォルト選択としてGUIで使用されます。ディレクトリが指定されていない場合、Data ProtectorはデフォルトのWAIKパスを使用します。

   - DR ISOイメージに挿入するドライバ

     このオプションを使用して、見つからないドライバをDR OSに追加することができます。[Add]または[Remove]をクリックして、ドライバを手動で追加または削除します。.Windows VistaまたはWindows Server 2008クライアントリカバリセットの一部であるドライバを挿入するには、[Inject]をクリックします。リカバリセットの*%Drivers%*の部分のドライバが、DR OSイメージに自動的に挿入されます。

   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、Windows Preinstallation Environment(WinPE)固有のドライバを挿入する必要があります。

8. [**完了**]をクリックしてウィザードを終了し、DR ISOイメージを作成します。

9. 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、DR ISOイメージをCDに書き込みます。

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 CD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。

復旧

影響を受けたシステムで障害復旧を正しく実行するには、以下が必要です。

- 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
- 復旧対象のクライアントの正常なフルバックアップ
- Data Protector 障害復旧CD

Windowsクライアントの拡張自動障害復旧を実行する手順を以下に示します。

1. オフライン障害復旧を行う場合以外は、ターゲットシステムのオペレーティングシステムによって、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アカウントを追加します。

   Windows VistaおよびWindows Server 2008システム:

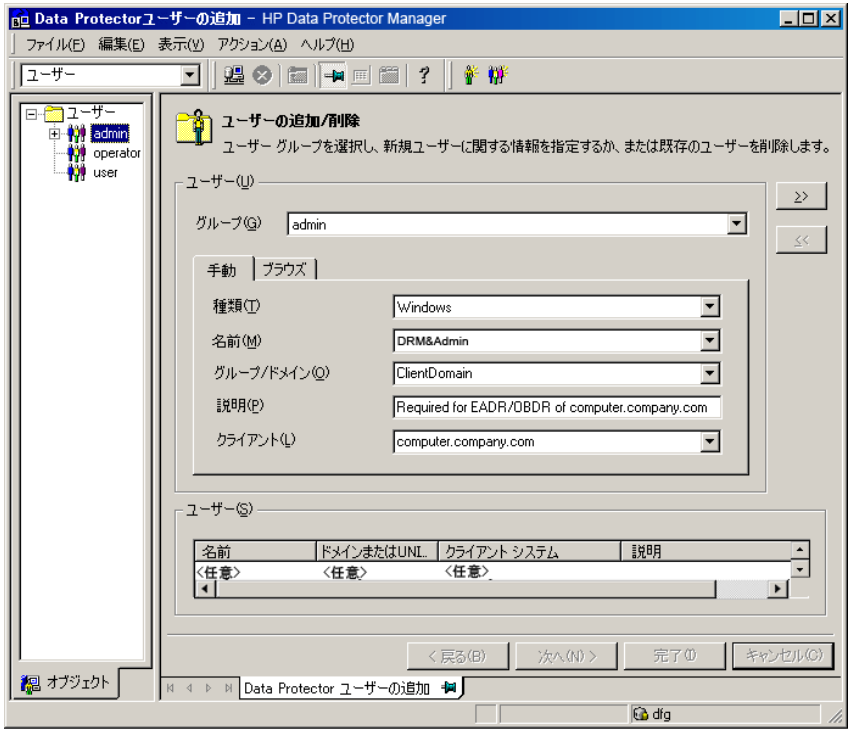
   - 種類: Windows
   - 名前:SYSTEM
   - グループ/ドメイン: NT AUTHORITY
   - クライアント: 復旧するシステムの一時ホスト名

     一時ホスト名は、Windowsプレインストール環境(WinPE)によってシステムに割り当てられます。一時ホスト名を検索するには、WinPEのコマンドプロンプト画面でhostnameコマンドを実行します。

   他のWindowsシステムの場合:

   - 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)

   ユーザーの追加の詳細については、オンラインヘルプの索引「Data Protectorユーザーの追加」を参照してください。



2. 元のシステムの障害復旧CDからクライアントシステムをブートします。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フラッシュドライブなど)が接続されていないことを確認してください。
3. 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.

4. Windows VistaおよびWindows Server 2008では、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。その他のWindowsシステムの場合は、ブートプロセスの最初に範囲選択メニューが表示されます。

   復旧範囲を選択して、Enterキーを押します。復旧範囲は5種類あります。

   - **[再起動]**:障害復旧は実行されず、システムが再起動されます。
   - **[デフォルト復旧]**:クリティカルボリュームが復旧されます。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、フェーズ3に備えた状態になります。
   - **[最小復旧]**:システムディスクとブートディスクのみが復旧されます(EADRとOBDRのみで使用可能)。
   - **[Full Recovery]**:重要なものだけでなく、すべてのボリュームが復旧されます。
   - **[共有ボリュームを含む完全復旧]**:Microsoft Cluster Server (MSCS)の場合にのみ選択できるオプションです。このオプションは、MSCS内のすべてのノードが障害の影響を受けているときに、最初のノードでEADRを実行する場合に使用します。復元セット内のすべてのボリューム(バックアップ時にバックアップ対象のノードによりロックされていたクラスター共有ボリュームを含む)が復元されます。

     1つでも稼動中のノードがあってMSCSが実行されている場合、共有ボリュームは復元されません。これは、稼動中のノードにより共有ボリュームがロックされるためです。この場合は[デフォルト復旧]を選択してください。

   プラットフォームやオペレーティングシステムによっては、使用可能なオプションが他にもあります。そのいくつかのオプションは、障害復旧が完全には終了しなかった場合や、追加手順が必要な場合に使用します。

   - **[Restore BCD]**:Windows VistaおよびWindows Server 2008システムでのみ使用可能です。選択されている場合、Data Protectorは、障害復旧セッション中にあらかじめBoot Configuration Data (BCD)ストアも復元して、Data Protectorの復元セッションでBCDストアを復元します。このオプションは、デフォルトで選択されています。
   - [Restore DAT]:Windows VistaおよびWindows Server 2008システムでのみ使用可能です。選択されている場合、Data Protectorは、障害復旧セッション中にあらかじめMicrosoft VSSライターのデータも復元して、Data Protectorの復元セッションでライターデータを復元します。このオプションは、デフォルトで選択されています。
   - [Remove Boot Descriptor]:Intel Itaniumシステムでのみ使用可能です。障害復旧のプロセスによって残された起動記述子をすべて削除します。「Intel Itanium固有の問題」(142ページ)を参照してください。
   - [Manual disk selection]: Intel Itaniumシステムでのみ使用可能です。ディスクの設定が大幅に変更された場合は、障害復旧モジュールがブートディスクを見つけることができません。このオプションを使用して正しいブートディスクを選択します。「Intel Itanium固有の問題」(142ページ)を参照してください。

Windows VistaおよびWindows Server 2008システム:

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、メニューが表示されて、暗号化されたドライバのロックを解除できます。「WindowsのBitLockerドライブ暗号化でロックされたボリュームのロック解除」(109ページ) を参照してください。

5. 復旧範囲を選択すると、Data Protectorは、ハードディスクに対して直接DR OSのセットアップを設定します。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およびWindows Server 2008システムの場合は、この手順が省略され、再起動は行われません。

   "To start recovery of the machine HOSTNAME press F12(マシンHOSTNAMEの復旧を開始するには、F12キーを押してください。)"というプロンプトの表示で10秒間待つと、システムはCDではなくハードディスクから起動します。

   障害復旧ウィザードが表示されます。障害復旧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。**[完了]**をクリックして、障害復旧を続行します。

6. 障害復旧のバックアップがData Protectorによって暗号化されているときに、Cell Managerを復旧またはCell Managerがアクセスできないクライアントを復旧しようとすると、次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]キーを押してください。

   キーストア(DR-ClientName-keys.csv)が(キーが保存されたメディアを挿入することにより)クライアントで使用可能であることを確認し、キーストアファイルのフルパスを入力します。キーストアファイルが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、障害復旧が続行されます。

7. 障害発生後にバックアップデバイスを変更したなどの理由でSRDファイルの情報が最新のものでなく、オフライン復旧を実行しようとしている場合は、この手順を続行する前にSRDファイルを変更してください。詳細については、「編集後のSRDファイルを使用した復旧」(105ページ)を参照してください。

8. Data Protectorは次に、選択された復旧範囲内で障害発生前の記憶データ構造を再構築し、すべてのクリティカルボリュームを復元します。一時DR OSは、以下の場合を除いて、最初のログイン後に削除されます。

   - **[最小復旧]**が選択された場合。
   - 障害復旧ウィザードが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の10秒間のポーズの間に、ユーザーがウィザードを中断して**[デバッグ]**オプションを選択した場合。
   - omnidrコマンドを、no_resetまたはdebugオプションを付けて手動で起動した場合。
   - 障害復旧が失敗した場合。

   Windows VistaおよびWindows Server 2008システムの場合は、一時DR OSが残されることはありません。

9. ステップステップ 1で追加したクライアントのローカル管理者アカウントが、障害復旧前にCell Manager上に存在していなかった場合は、Cell Manager上のData ProtectorAdminユーザーグループから削除します。

10. Cell Manager の復旧、または高度な復旧作業(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、特別な手順が必要となります。詳細については、「Data Protector Cell Manager 固有の復元手順 」(101ページ)と「高度な復旧作業」(94ページ)を参照してください。

11. Data Protector標準復元手順を使用して、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。

注記:

Data Protectorはボリューム圧縮フラグを復元しません。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されて復元されますが、新規ファイルを圧縮ファイルとして作成したい場合は、手動でボリューム圧縮フラグをセットする必要があります。

Windowsシステムのワンボタン障害復旧

ワンボタン障害復旧(OBDR) とは、WindowsクライアントとCell Manager用の自動化されたData Protectorの復旧方法で、ユーザーが介在する手間は最小限に抑えられています。サポート対象のオペレーティングシステムは、『*HP Data Protector product announcements 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 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障害復旧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、障害復旧オペレーティングシステム(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バックアップ時と同じ状態に復元します。

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。

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 を含むパーティション

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

Windowsクライアントに対してワンボタン障害復旧を行う手順の概要は、以下のとおりです。

1. **フェーズ0**
   a. OBDRバックアップが必要です(Data Protectorワンボタン障害復旧ウィザードを使用してバックアップ仕様を作成します)。
   b. 暗号化されたバックアップを使用している場合は、暗号化キーをリムーバブルメディアに保存して、障害復旧の際に使用できるようにします。Cell Managerの復旧時、またはCell Managerへの接続を確立できない場合には、このキーが必要になります。
2. **フェーズ1**

   復旧用テープからブートし、復旧範囲を選択します。
3. **フェーズ2**

   クリティカルボリューム(ブートパーティション、オペレーティングシステム、およびData Protectorが格納されているパーティション)はデフォルトで復元されます。

4. **フェーズ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ブートテープ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障害復旧に関する必要条件、制限事項、準備、および、復旧について説明します。「高度な復旧作業」(94ページ)も参照してください。

要件

- Data Protector 自動障害復旧コンポーネントとユーザーインターフェースコンポーネントが、この方法で復旧するシステムにインストールされている必要があります。(『*HP Data Protector インストールおよびライセンスガイド*』を参照)。
- OBDRを実行できるシステム構成にしておく必要があります。システムのBIOSは、El-Torito標準で定義されているブート可能CDをサポートしている必要があります。また、INT13h機能のXXhにより、LBAアドレッシングを使用しているハードディスクドライブへの読み書きが可能である必要があります。OBDRデバイスがCD-ROMをエミュレートする場合には、同じ標準に準拠していなければなりません。BIOSのオプションは、システムのユーザーマニュアル、またはブート前にシステム設定を調査することでチェックできます。

  サポートされているシステム、デバイスおよびメディアに関する詳細は、以下のWebページにあるHP StorageWorksのテープとハードウェアの互換性一覧表を参照してください。

  http://www.hp.com/support/manuals 『*HP Data Protector product announcements ソフトウェアノートおよびリファレンス*』も参照してください。
- ターゲットシステムのハードウェア構成は、障害発生前の状態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に交換用ディスクが接続されていること。
- 最小限のオペレーティングシステム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。オリジナルパーティションで[ドライブを圧縮してディスク領域を空ける]オプションを有効に設定していた場合は、少なくとも400MBの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200MB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。

- ブートに必要なドライバは、すべて%SystemRoot%フォルダにインストールされている必要があります。
- ネットワーク機能が付いたセーフモード、またはディレクトリサービス復元モード(ドメインコントローラのみ)でシステムをブートする場合は、ネットワークが使用可能でなければなりません。ただし、システムのバックアップは通常のブートプロセスの後に実行する必要があります。
- 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。障害復旧には、このようなプールのメディアしか使用できません。
- オフライン復元を計画している場合は、クライアントバックアップ時のデバイスへの書き込みにはデフォルトのブロックサイズ64KBを使用してください。障害復旧を実行する際にWindowsで使用できるブロックサイズはこのデフォルトのサイズだけです。デフォルトのブロックサイズ64KBが設定されているかどうかを確かめるには、[プロパティ]ボックスの**[拡張...]**を選択します。図4(73ページ)を参照してください。

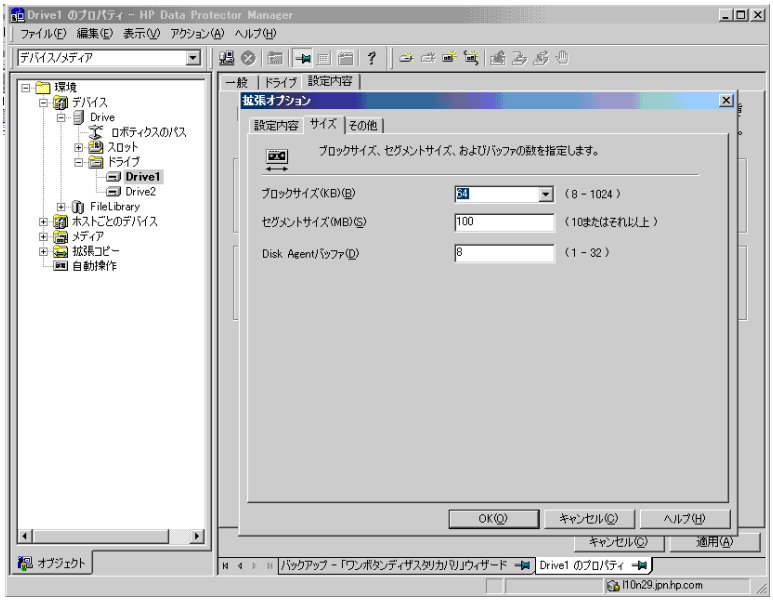


図 4 デフォルトのブロックサイズの確認

- バックアップするシステムがWindows VistaまたはWindows Server 2008システムの場合、Windows Automated Installation Kit (WAIK) 1.1をインストールする必要があります。WAIKの古いバージョンはサポートされていません。
- Windows Vista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

- 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 (IIS)データベース、ターミナルサービスデータベース、Certificate Server データベースは、フェーズ2で自動的には復元されません。これらをターゲットシステムに復元するには、Data Protector 標準復元手順を実行してください。
- ワンボタン障害復旧のバックアップセッションは、同じOBDRデバイス上では1度に1つのクライアントまたはCell Managerに対してしか実行できません。バックアップセッションは、ローカルに接続された1台のOBDR対応デバイス上で行う必要があります。
- ダイナミックディスクはサポートされていません(Windows NTからのミラーセットのアップグレードも含む)。
- 新しいディスクのサイズは、影響を受けたディスクのサイズ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。
- 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、0x12タイプ(EISAを含む)と0xFEタイプのみです。
- 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のみサポートされています。
- Windows VistaおよびWindows Server 2008システムの場合は、LDMディスクはサポートされていません。
- 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。

準備

この項で挙げられている手順を完了する前に、すべての障害復旧の方法に共通する一般的な準備手順として「計画」(33ページ)も参照してください。「高度な復旧作業」(94ページ)も参照してください。

重要:

障害復旧の準備は、障害が発生する*前*に行っておく必要があります。

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](テープ上のバックアップであることを確実にするため)、メディア割り当てポリシーは[緩和](テープはOBDRバックアップ時にフォーマットされるため)です。また、このメディアプールを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。オ

ンラインヘルプの索引「メディアプールの作成」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。

Microsoft Cluster Server の場合: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)以下のものが含まれている必要があります。

- すべてのノード
- 管理仮想サーバー(管理者が定義)
- Cell Manager仮想サーバーとIDB(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)

詳細については、「Microsoft Cluster Serverの復元に固有の手順」(94ページ) を参照してください。

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りロックされている共有ディスクボリュームのディスクをフェーズ1で構成するために必要な情報を収集するのは不可能です。

OBDRバックアップ

OBDRを使用して復旧を実行するシステム上でインストールされたGUIからローカルにOBDRバックアップを実行するには、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]**を選択します。
2. Scopingペインで**[タスク]**ナビゲーションタブをクリックし、**[ワンボタン障害復旧ウィザード]**を選択します。
3. **[次へ]**をクリックします。
4. クリティカルオブジェクトはすでにすべて選択された状態になっていて(Cell ManagerOBDRバックアップの場合はIDBも含む)、選択を解除することはできません。復旧手順の中で、Data Protectorはシステムからパーティションをすべて削除してしまうため、他のパーティションを復旧後も使用する場合、手動で選択します。**[次へ]**をクリックします。
5. バックアップに使用するローカル接続のOBDRドライブを選択して**[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、オンラインヘルプの索引「バックアップオプション」を参照してください。

Windows VistaおよびWindows Server 2008システム:

WAIKオプションの指定:

- Windows自動インストールキット(WAIK)ディレクトリ

  場所を入力すると、その場所がData Protectorに保存され、DR ISOイメージが次回作成されるときに、デフォルト選択としてGUIで使用されます。ディレクトリが指定されていない場合、Data ProtectorはデフォルトのWAIKパスを使用します。

- DR ISOイメージに挿入するドライバ

  このオプションを使用して、見つからないドライバをDR OSに追加することができます。[**Add**]または[**Remove**]をクリックして、ドライバを手動で追加または削除します。.Windows VistaまたはWindows Server 2008クライアントリカバリセットの一部であるドライバを挿入するには、[**リカバリセットからドライバを自動的に挿入**]を選択します。リカバリセットの%Drivers%部分のドライバが自動的にDR OSイメージに挿入されます。ただし、そのドライバは[ドライバを挿入]テキストボックスには表示されません。

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は、DR OS内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、Windows Preinstallation Environment(WinPE)固有のドライバを挿入する必要があります。

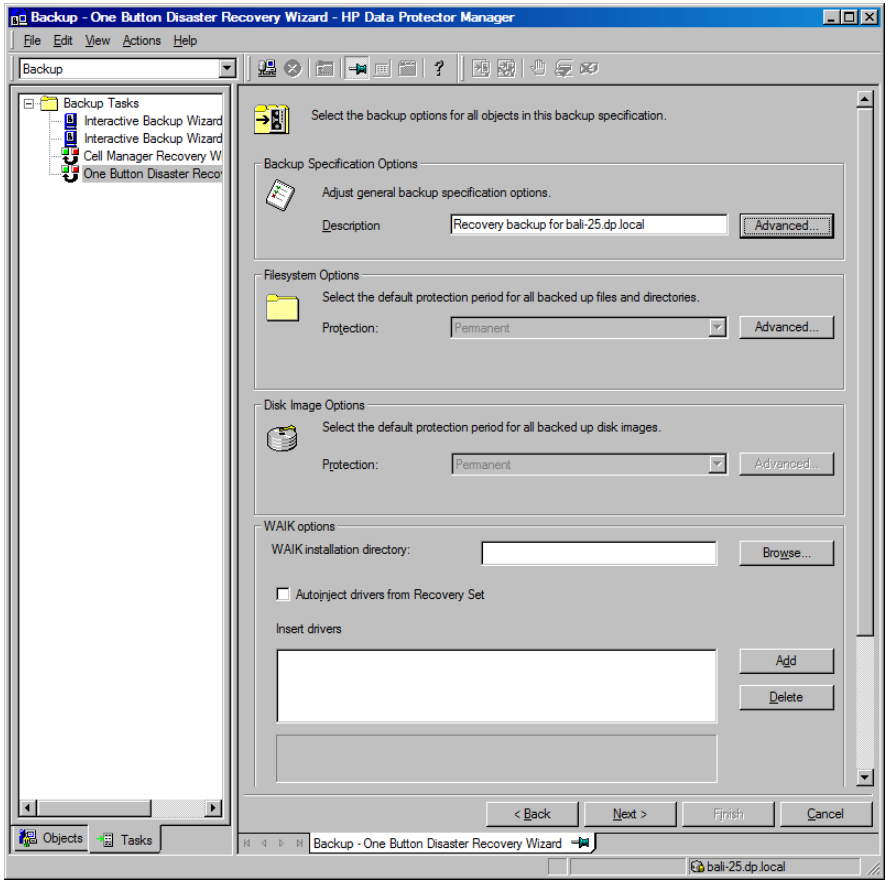


図 5 Windows VistaおよびWindows Server 2008クライアントバックアップオプション

7. [**次へ**]をクリックして、[スケジューラ]ページを表示します。ここでは、バックアップの実行スケジュールを設定できます。オンラインヘルプの索引「特定の日時に対するバックアップのスケジュール設定」を参照してください。

8. **[次へ]**をクリックして、[バックアップオブジェクトのサマリー]ページを表示します。このページには、バックアップオプションが表示されます。

注記:

[サマリー]ページでは、それまでに選択したバックアップデバイスやバックアップ仕様の順序を変更することができません(順序を入れ替える機能はありません)。OBDRに必要ではないバックアップオブジェクトのみ削除可能であり、一般的なオブジェクトのプロパティのみ表示できます。

ただし、バックアップオブジェクトの説明は変更できます。

9. [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、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保存して、後でスケジュールを設定したり仕様を変更できるようにしておくことをお勧めします。

   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。修正したバックアップ仕様は、ワンボタン障害復旧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。標準バックアップ仕様として保存した場合は、OBDR には使用できません。

10. **[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。

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。

kb.cfgファイル

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(および他の必要ファイル)を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。

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が正常にブートしない、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ります。詳細については、「kb.cfgファイルの編集」(105ページ)を参照してください。

△ **注意:**

バックアップメディアへのアクセスは、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。

暗号化キーの準備

Cell Manager の復旧またはオフラインクライアントの復旧に対しては、暗号化キーをリムーバブルメディアに保存して、障害復旧の際に使用できるようにする必要があります。Cell Managerの復旧に対しては、事前に (障害が発生する前に)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。このキーは、障害復旧イメージの作成時に、Cell Managerに自動的にエクスポートされます。エクスポート先のファイルは、Data_Protector_program_data¥Config¥Server¥export¥keys¥DR-ClientName-keys.csv(Windows Server 2008の場合)、Data_Protector_home¥Config¥Server¥export¥keys¥ DR-ClientName-keys.csv(その他のWindowsシステムの場合)、または/var/opt/omni/server/export/keys/DR-ClientName-keys.csv(UNIXシステムの場合)です。ここで、ClientNameはイメージを作成するクライアントの名前です。

障害復旧の準備のための各バックアップについて、正しい暗号化キーがあることを確認してください。

復旧

影響を受けたシステム上で障害復旧を正しく実行するには、以下が必要です。

- 影響を受けたディスクと交換する新しいハードディスク(必要な場合)。
- 復旧対象クライアントのクリティカルオブジェクトがすべて含まれたブート可能なバックアップメディア。
- ターゲットシステムにローカル接続されたOBDRデバイス。

Windowsシステムのワンボタン障害復旧の詳細な手順を以下に示します。

1. オフライン障害復旧を行う場合以外は、ターゲットシステムのオペレーティングシステムによって、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アカウントを追加します。

   Windows VistaおよびWindows Server 2008システム:

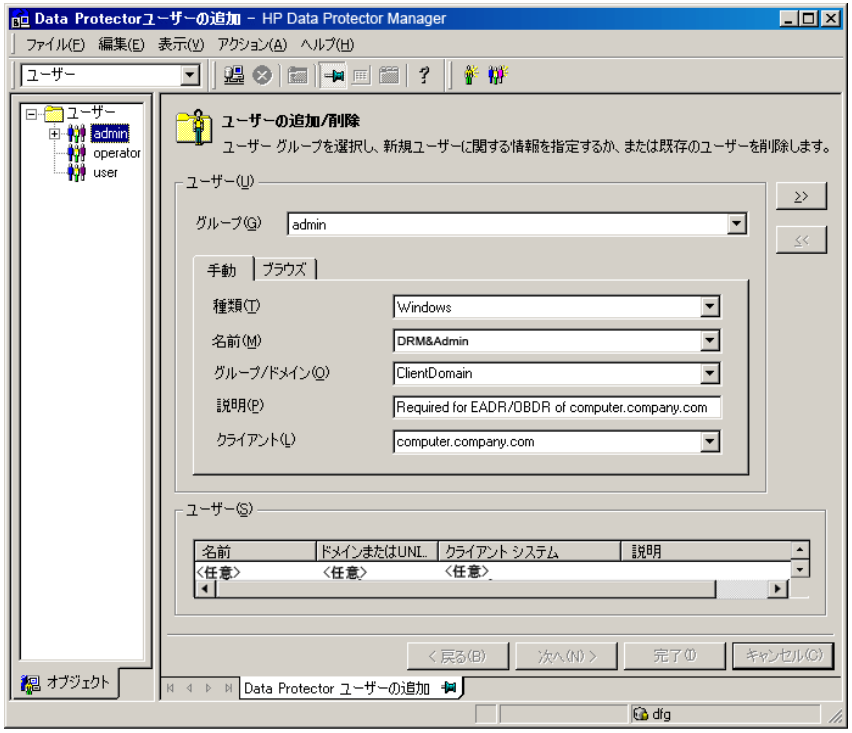
   - 種類:Windows
   - 名前:SYSTEM
   - グループ/ドメイン:NT AUTHORITY
   - クライアント:復旧するシステムの一時ホスト名

     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。一時ホスト名を検索するには、WinPEのコマンドプロンプト画面でhostnameコマンドを実行します。

   その他のWindowsシステムの場合:

   - 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)

   ユーザーの追加の詳細については、オンラインヘルプの索引「Data Protectorユーザーの追加」を参照してください。



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フラッシュドライブなど)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、初期化中にテープデバイスの取出しボタンを押して、テープデバイスの電源を入れます。詳細は、デバイス付属のドキュメントを参照してください。

5. Windows VistaおよびWindows Server 2008では、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。その他のWindowsシステムの場合は、ブートプロセスの最初に範囲選択メニューが表示されます。

   復旧範囲を選択して、Enterキーを押します。復旧範囲は5種類あります。

   - [再起動]:障害復旧は実行されず、システムが再起動されます。
   - [デフォルト復旧]:クリティカルボリュームが復旧されます。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空のまま残され、フェーズ3に備えた状態になります。
   - [最小復旧]:システムディスクとブートディスクのみが復旧されます(EADRとOBDRのみで使用可能)。
   - [Full Recovery]:重要なものだけでなく、すべてのボリュームが復旧されます。
   - [共有ボリュームを含む完全復旧]: Microsoft Cluster Server (MSCS)の場合にのみ選択できるオプションです。このオプションは、MSCS内のすべてのノードで障害の影響を受けているときに、最初のノードのワンボタン障害復旧を実行する場合に使用します。復元セット内のすべてのボリューム(バックアップ時にバックアップ対象のノードによりロックされていたクラスター共有ボリュームを含む)が復元されます。

   ヒント:

   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。バックアップ時に他のノードによりロックされている共有ディスクボリュームのディスクをフェーズ1で構成するために必要な情報を収集するのは不可能なことです。

   1つでも稼動中のノードがあってMSCSサービスが実行されている場合、共有ボリュームは復元されません。稼動中のノードが共有ボリュームをロックしているためです。この場合は[デフォルト復旧]を使用してください。

プラットフォームやオペレーティングシステムによっては、使用可能なオプションが他にもあります。そのいくつかのオプションは、障害復旧が完全には終了しなかった場合や、追加手順が必要な場合に使用します。

- [Restore BCD]:Windows VistaおよびWindows Server 2008システムでのみ使用可能です。選択されている場合、Data Protectorは、障害復旧セッション中にあらかじめBoot Configuration Data (BCD)ストアも復元して、Data Protectorの復元セッションでBCDストアを復元します。このオプションは、デフォルトで選択されています。
- [Restore DAT]:Windows VistaおよびWindows Server 2008システムでのみ使用可能です。選択されている場合、Data Protectorは、障害復旧セッション中にあ

らかじめMicrosoft VSSライターのデータも復元して、Data Protectorの復元セッションでライターデータを復元します。このオプションは、デフォルトで選択されています。

- [Remove Boot Descriptor]:Intel Itaniumシステムでのみ使用可能です。障害復旧のプロセスによって残された起動記述子をすべて削除します。「Intel Itanium固有の問題」(142ページ)を参照してください。
- [Manual disk selection]: Intel Itaniumシステムでのみ使用可能です。ディスクの設定が大幅に変更された場合、障害復旧モジュールがブートディスクを見つけられないことがあります。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。「Intel Itanium固有の問題」(142ページ)を参照してください。

Windows VistaおよびWindows Server 2008システム:

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、メニューが表示されて、暗号化されたドライバのロックを解除できます。「WindowsのBitLockerドライブ暗号化でロックされたボリュームのロック解除」(109ページ) を参照してください。

6. 復旧範囲を選択すると、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。Windows VistaおよびWindows Server 2008システムの場合は、DR OSはインストールされず、再起動は行われません。

   障害復旧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。[完了] をクリックして、障害復旧を続行します。

7. 障害復旧のバックアップが暗号化されているときに、Cell Managerを復旧またはCell Managerがアクセスできないクライアントを復旧しようとすると、次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]キーを押してください。

   キーストア(DR-ClientName-keys.csv)がクライアントで使用可能であることを(たとえば、CD-ROM、フロッピーディスク、USBフラッシュドライブを挿入することで)確認し、キーストアファイルのフルパスを入力します。キーストアファイルが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、障害復旧が続行されます。

8. 障害発生後にバックアップデバイスを変更したなどの理由でSRDファイルの情報が最新のものでなく、オフライン復旧を実行しようとしている場合は、この手順を続行する前にSRDファイルを変更してください。詳細については、「編集後のSRDファイルを使用した復旧」(105ページ)を参照してください。

9. 次にData Protectorは、従来の記憶データ構造を再構築し、すべてのクリティカルボリュームを復元します。

   一時DR OSは、以下の場合を除いて、最初のログイン時に削除されます。

   - [最小復旧]が選択された場合。
   - 障害復旧ウィザードが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の10秒間のポーズの間に、ユーザーがウィザードを中断して[Debugs]オプションを選択した場合。
   - omnidrコマンドを、-no_resetまたは-debugオプションを付けて手動で起動した場合。
   - 障害復旧が失敗した場合。

   Windows VistaおよびWindows Server 2008システムの場合は、一時DR OSが残されることはありません。

10. ステップステップ 1で追加したクライアントのローカル管理者アカウントが、障害復旧前にCell Manager上に存在していなかった場合は、Cell Manager上のData ProtectorAdminユーザーグループから削除します。

11. Cell Manager の復旧、または高度な復旧作業(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、特別な手順が必要となります。詳細については、「Data Protector Cell Manager 固有の復元手順 」(101ページ)と「高度な復旧作業」(94ページ)を参照してください。

12. Data Protector 標準復元手順を使用して、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。

注記:

Data Protectorはボリューム圧縮フラグを復元しません。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されて復元されますが、新しく作成するファイルも圧縮ファイルとして作成したい場合は、手動でボリューム圧縮フラグをセットする必要があります。

自動システム復旧

自動システム復旧(ASR)はWindowsシステム上の自動システムで、障害発生時にディスクをオリジナルの状態に再構成(または、新しいディスクがオリジナルのものより大きい場合、パーティションをサイズ変更)します。この処理には、ディスクのパーティション化と論理ボリュームの構成(ファイル形式、ドライブ文字の割り当て、ボリュームマウントポイント、およびボリューム特性)が含まれます。このようにASRはData Protector drstartコマンドによ

り、Data Protector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するアクティブなDR OSをインストールすることができます。

Data Protector は次に、ターゲットシステムを元のシステム構成に復旧し、最後にユーザーデータを復元します。

サポート対象のオペレーティングシステムは、『*HP Data Protector product announcements 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。

重要:

ハードウェアやソフトウェア、または構成が変更された場合や、ASRディスクをアップデートする場合には、その都度クライアントのフル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。

重要:

Cell Manager用のASRセットは、前もって作成しておく必要があります。これは、障害後にはASRアーカイブファイルを取得できないためです。他のシステム用のASRセットは障害発生時にCell Managerを使用して作成できます。

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 を含むパーティション

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

Windowsクライアントに対して自動システム復旧(ASR)を行う手順の概要は、以下のとおりです。

1. **フェーズ0**
   a. フルクライアントバックアップを実行します。
   b. Data Protector バイナリをコピーしたASRフロッピーディスクを作成し、構成を変更するたびに1枚目のフロッピーディスクを更新します。
   c. 暗号化されたバックアップを使用している場合は、暗号化キーをリムーバブルメディアに保存して、障害復旧の際に使用できるようにします。Cell Manager の

復旧時、または Cell Manager への接続を確立できない場合には、このキーが必要になります。

2. **フェーズ1**
   a. Windowsインストールメディアからブートし、**F2**キーを押してASRモードに切り替えます。
   b. ASRセットの1枚目のフロッピーディスク(更新されたフロッピーディスク)を用意します。
   c. 再起動後に、DRのインストールおよびSRDファイルの場所に関する情報を指定します(a:¥)。
   d. プロンプトが表示されたらフロッピーディスクを交換します。
3. **フェーズ2**
   a. すべてのクリティカルオブジェクトが自動的に復元されます。システムを再起動し、Windowsインストールメディアと ASRフロッピーディスクを取り出します。
4. **フェーズ3**
   a. Data Protector 標準復元手順を使用して、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。

ASRは、障害への準備作業(の一部)を実行するとともに、ブートパーティションを再作成する目的で使用されます。Data Protectorには、集中管理、高パフォーマンスバックアップ、高可用性サポート、復元、監視、レポート、通知など、その他の必要な機能がすべて用意されています。

以下の項で、Windowsシステム上での自動システム復旧に関する必要条件、制限事項、準備、および、復旧について説明します。「高度な復旧作業」(94ページ)も参照してください。

要件

- Data Protector自動システム復旧コンポーネントが、ASRで復旧するシステム上にインストールされている必要があります。『*HP Data Protector インストールおよびライセンスガイド*』を参照してください。
- ファイアウォールを使用している場合は、ポート1071と1073が開放されている必要があります。ASRは変数OB2PORTRANGEとOB2PORTRANGESPECをサポートしていません。

ハードウェア構成

- ターゲットシステムのハードウェア構成は、元の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。ただし、ハードディスクドライブ、ビデオカード、ネットワークインターフェースカードは除きます。ネットワークカードまたはビデオカードを交換した場合は、それらを手動で構成する必要があります。

- フロッピーディスクのディスクドライブがインストールされていること。
- フロッピードライブとCD-ROMドライブが、IDEまたはSCSIコントローラに接続されている必要があります。USBやPCMCIAデバイスなどの外部デバイスはサポートされていません。

  ただし、USBのフラッシュドライブを使用したASRはHP Integrityサーバー(IA-64プラットフォーム)上でサポートされています。詳細は、http://docs.hp.com/en/windows.html上のホワイトペーパー『*Recovering Windows Server 2003 on HP Integrity servers*』を参照してください。

ハードディスクドライブ

- ターゲットシステムと元のシステムの間で、重要なボリュームを持つ物理ディスクの数が一致していること。
- 同じバスの同じホストバスアダプタに交換用ディスクが接続されていること。
- ターゲットシステムの各交換ディスクの記憶容量は、元のシステムの対応するディスクの記憶容量以上である必要があります。さらに、交換ディスクのジオメトリも交換前のディスクと同じである必要があります。
- ターゲットシステム上のどのディスクも、セクターあたりのバイト数が512バイトであること。
- ASRで使用されるすべてのディスクがシステムからアクセスできる必要があります(ハードウェアRAIDが構成されている、SCSIディスクが適切にターミネートされている、など)。
- オフライン復元を計画している場合は、クライアントバックアップ時のデバイスへの書き込みにはデフォルトのブロックサイズ64KBを使用してください。障害復旧を実行する際にWindowsで使用できるブロックサイズはこのデフォルトのサイズだけです。デフォルトのブロックサイズ64KBが設定されているかどうかを確かめるには、[プロパティ]ボックスの**[拡張...]**を選択します。図6を参照してください。

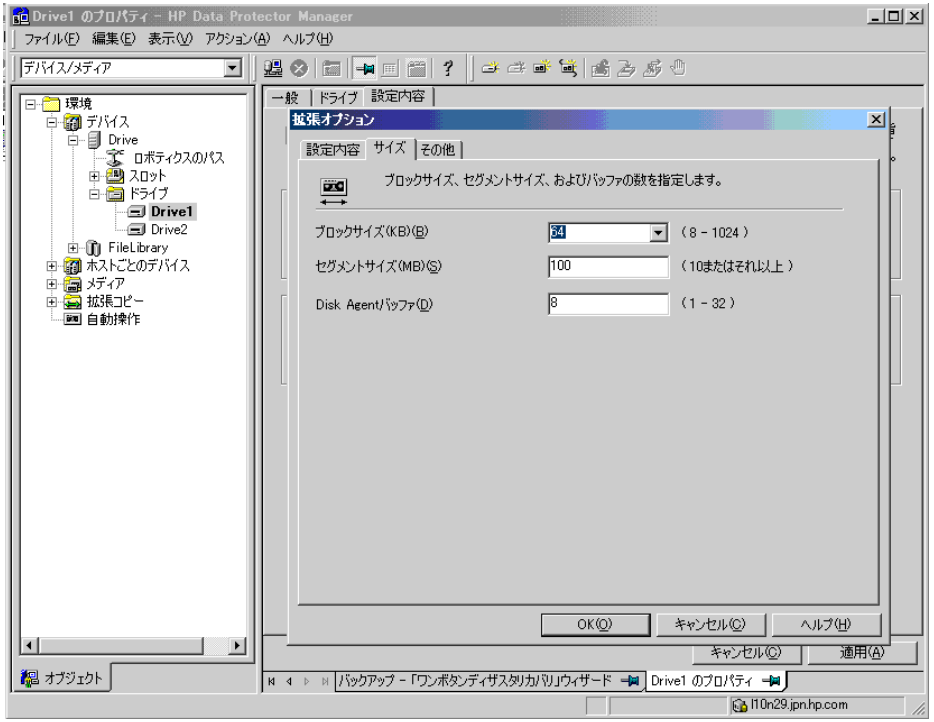


図 6 デフォルトのブロックサイズの確認

制限事項

- Windows XP Home EditionはASRをサポートしていません。
- 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。
- Internet Information Server (IIS)データベース、ターミナルサービスデータベース、Certificate Serverデータベースは、フェーズ2で自動的には復元されません。これらをターゲットシステムに復元するには、Data Protector 標準復元手順を実行してください。
- ベンダー固有のパーティションに格納されていたデータは、ASRでは自動的に復元されません。ASR 時にパーティションは再作成されますが、データはベンダー固有の手順で復元する必要があります。ただし、EISAユーティリティパーティションに格納されていたデータは、Data Protector 標準復元手順で復元できます。
- サポートされているローカルバックアップデバイスは、Windowsのインストール中にインストール可能なデバイス(追加のドライバが必要とならないデバイス)だけです。

準備

この項で挙げられている手順を完了する前に、すべての障害復旧の方法に共通する一般的な準備手順として「計画」(33ページ)も参照してください。さらに、障害復旧の準備に関して「高度な復旧作業」(94ページ)を参照してください。

重要:

障害復旧の準備は、障害が発生する*前*に行っておく必要があります。

前提条件

- 自動システム復旧を正常に行うためには、フルクライアントバックアップ(CONFIGURATIONも含む)が必要です。オンラインヘルプの索引「バックアップ、Windows固有」および「バックアップ、構成」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)以下のものが含まれている必要があります。

  - すべてのノード
  - 管理仮想サーバー(管理者が定義)
  - Cell Manager 仮想サーバーとIDB(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)

  詳細については、「Microsoft Cluster Serverの復元に固有の手順」(94ページ) を参照してください。

フルクライアントバックアップを実行したら、ASRセットを用意する必要があります。ASRセットは、3枚(32ビットシステムの場合)、4枚(AMD64/Intel EM64Tシステムの場合)、または6枚(Itaniumシステムの場合)のフロッピーディスクに格納されたファイルの集まりで、交換ディスクの適切な再構成(ディスクのパーティションと論理ボリュームの構成)を実行するときと、元のシステム構成およびフルクライアントバックアップでバックアップされたユーザーデータの自動復旧を実行するときに必要になります。これらのファイルは、バックアップメディア上に保存されますが、ASRアーカイブファイルとしてCell Manager上のData_Protector_program_data¥Config¥server¥dr¥asrディレクトリ(Windows Server 2008の場合)、Data_Protector_home¥Config¥server¥dr¥asrディレクトリ(その他のWindowsシステムの場合)、または/etc/opt/omni/server/dr/asr/ ディレクトリ(UNIXシステムの場合)にも保存されます。障害が発生すると、ASRアーカイブファイルが3枚(32ビットシステムの場合)、4枚(AMD64/Intel EM64Tシステムの場合)、または6枚(Itaniumシステムの場合)のフロッピーディスクに展開されます。これらのフロッピーディスクは、ASRの実行時に必要となります。

注記:

Cell Manager用のASRセットは、前もって作成しておく必要があります。これは、障害後にはASRアーカイブファイルを取得できないためです。

ASRセットを作成するには、以下の手順を実行します。

1. フルクライアントバックアップを実行します。
2. 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ます。
3. [HP Data Protector Manager]で[復元]コンテキストを選択します。
4. Scopingペインで[**タスク**]ナビゲーションタブをクリックし、[**障害復旧**]を選択します。
5. 結果エリアのドロップダウンリストから、ASRセットを作成するクライアントを選択します。
6. [**自動システムリカバリセットの作成**]をクリックし、[**次へ**]をクリックします。

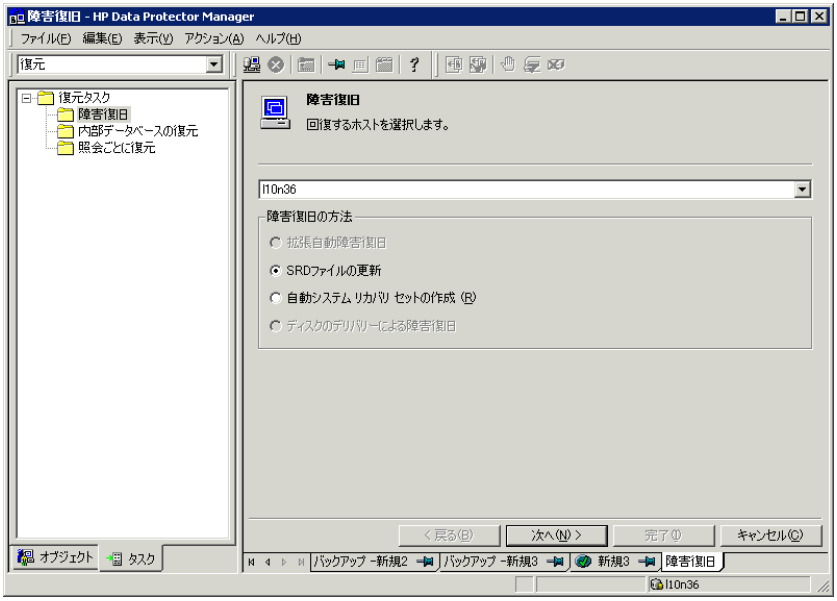


図 7 ASRセットの作成

Data ProtectorがCell ManagerからASRアーカイブファイルを取得します。Cell Managerに保存されていない場合は、障害復旧ウィザードによりバックアップメディアから復旧するようメッセージが表示されます。

7. 各クリティカルオブジェクトごとに、適切なオブジェクトバージョンを選択して、[**次へ**]をクリックします。
8. フルクライアントバックアップ時に作成されたASRアーカイブファイルが、Cell Managerからダウンロードされます。取得されたASRアーカイブファイルの保存先を選択し、[**DRインストールをコピー**]チェックボックスをオンにして、DRインストールファイルを同じ場所にコピーします。ASRを実行するにはこれらのファイルをフロッピーディスク(ASRセット)に保存する必要があるため、フロッピーディスクドライブを保存先に指定することをお勧めします。

   Data Protectorは、3枚(32ビットシステムの場合)、4枚(AMD64/Intel EM64Tシステムの場合)、または6枚(Itaniumシステムの場合)のフロッピーディスクを作成します。Cell Manager用のASRセットは事前に作成しておく必要がありますが、他のシステム用のASRディスクは障害発生時に Cell Manager を使用して作成できます。

ASRセットの作成後、ハードウェアやソフトウェア、構成の変更があった場合には、その都度1枚目のディスクのみをアップデート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。ASRセットの1枚目のディスクをアップデートするには、最初からすべての手順を再度実行しますが、[DRインストールをコピー]チェックボックスをオンにする必要はありません。このオプションを選択すると、アップデートには不要なDRインストールファイルが(選択した保存先に)コピーされます。

重要:

ASRフロッピーディスクへのアクセスは、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。

ローカルデバイス

ローカル接続されたデバイスをASR用に使用する場合は、そのデバイスがサポートされているか確認してください。以下の手順で確認します。

1. コマンドプロンプトからdevbra -devを実行します(ディレクトリは*Data_Protector_home*¥bin)。
2. scsitabファイル(ディレクトリは*Data_Protector_home*)の名前を変更して、コマンドプロンプトからdevbra -dev を実行します。
3. devbra -devコマンドの2つの出力を比較します。2つのファイルが同じであれば、ASRでそのデバイスを使用することができます。そうでない場合は、scsitabファイルをASRディスクの1枚目にコピーします。scsitabファイルをコピーする必要があるのは、最初にASRセットを作成する時のみです。ASRセットのアップデートだけを行う場

合には、コピーする必要はありません。オンラインヘルプの索引「新しいデバイスのサポート」を参照してください。

4. scsitabファイル名前を元に戻します。

復旧

影響を受けたシステムの障害復旧を正常に実行するには、以下のものが必要です。

- 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
- 復旧対象のクライアントの正常なフルバックアップ
- アップデート済みのASRセット
- Windowsインストールメディア

ASRを実行する手順を以下に示します。

1. Windowsのインストールメディアからシステムをブートします。
2. OSのセットアップ時に**F2**キーを押して、ASRモードに入ります。
3. ASRセットの1枚目のフロッピーディスク(更新されたフロッピーディスク)を用意します。
4. 再起動後に障害復旧ウィザードが起動され、[DRのインストール元]と[SRDファイルのパス]の入力が求められます。DRインストールファイルとSRDファイルは、両方ともASRセットの1枚目のディスクにあります(a:¥)。

   ASR の設定を変更するには、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、オプションを選択します。**[完了]**をクリックして、障害復旧を続行します。

   障害発生後にバックアップデバイスを変更したなどの理由でASRディスク上のSRDファイルの情報が最新のものでなく、オフライン復旧を実行しようとしている場合は、この手順を続行する前にSRDファイルを変更してください。(「編集後のSRDファイルを使用した復旧」(105ページ)を参照)。

注記:

オリジナルのOSメディアに適切なドライバが用意されていないと、ASRを実行できません。[ハードウェアの追加]ウィザードを使用して、ネットワークをインストールすることができます。このウィザードは以下のコマンドで起動できます。%SystemRoot%¥system32¥rundll32 shell32.dll,Control_RunDLL hdwwiz.cpl

5. オフライン障害復旧を行う場合以外は、Cell Manager上のData ProtectorのAdminユーザーグループにクライアントのローカルシステムアカウントを追加します。オンラインヘルプの索引「ユーザー、Data Protector"」を参照してください。

   図8 (93ページ) に示されている情報を入力します。

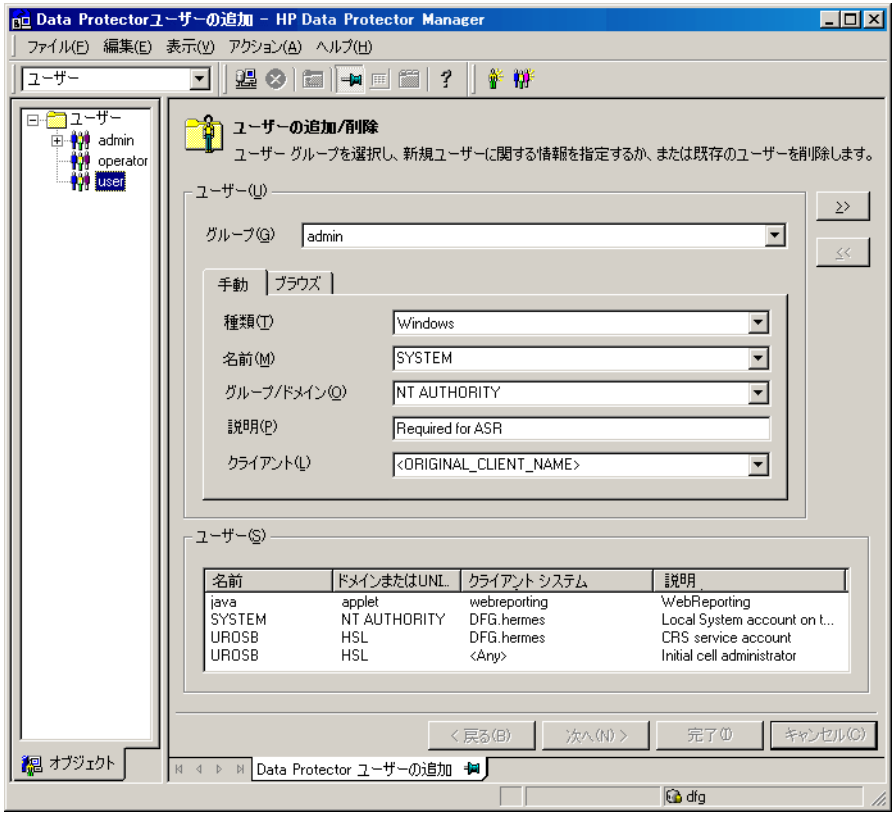


図 8 ASRのユーザー名

6. プロンプトが表示されたらフロッピーディスクを交換します。
7. プロンプトが表示されたらシステムを再起動し、Windowsインストールメディアと ASRディスクを取り出します。

8. 障害復旧のバックアップがData Protector によって暗号化されているときに、Cell Managerを復旧またはCell Managerがアクセスできないクライアントを復旧しようとすると、次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]キーを押してください。キーストア(DR-ClientName-keys.csv)が(キーが保存されたメディアを挿入することにより)クライアントで使用可能であることを確認し、キーストアファイルのフルパスを入力します。キーストアファイルが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。

9. ステップステップ 5(93ページ)で追加したクライアントのローカルシステムアカウントが、障害復旧前にCell Manager上に存在していなかった場合は、Cell Manager上のData ProtectorAdminユーザーグループから削除します。

10. Data Protector 標準復元手順を使用して、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。

高度な復旧作業

この項では、Microsoft Cluster ServerやInternet Information Serverの復元など、高度な復旧作業を行う場合に必要な手順について説明します。

Microsoft Cluster Serverの復元に固有の手順

この項では、Microsoft Cluster Server (MSCS)の障害復旧を行う場合に必要な手順について説明します。概念と一般的情報については、『*HP Data Protector コンセプトガイド*』のクラスター化関連の項を参照してください。また、オンラインヘルプの索引キーワード「クラスター」で表示される内容を参照してください。

ご使用のクラスター環境に適した障害復旧の方法を選択し、障害復旧プランに取り入れます。どの方法を使用するかを決定する前に、それぞれの障害復旧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。

考えられる状況

MSCS の障害復旧では、考えられる状況が2つあります。

- 最低1台のノードが稼動している場合
- クラスター内のすべてのノードに障害が発生した場合

重要:

MSCSの復旧は、「ディスクデリバリーによる障害復旧」以外の方法で行えます。使用する障害復旧の方法に関する固有の制限や必要条件は、MSCSの障害復旧にも当てはまります。サポート対象のオペレーティングシステムは、『*HP Data Protector product announcements 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、障害復旧の必要条件(整合性のある最新のバックアップ、更新済みのSRDファイル、不良ハードウェアの交換など)がすべて満たされていなければなりません。

MSCS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)以下のものが含まれている必要があります。

- すべてのノード
- 管理仮想サーバー (管理者が定義)
- Cell Manager仮想サーバーとIDB (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)

二次ノードの障害復旧

これはMSCSの障害復旧についての基本的な状況です。障害復旧に関する他の必要条件に加えて、以下の条件も満たされている必要があります。

- 最低1台のクラスターノードが正常に機能していること
- 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資源がオンラインであること(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であること)
- 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障害復旧はData Protectorクライアントの障害復旧と同じです。二次ノードの復元に使用する特定の障害復旧の方法の手順に従ってください。

注記:

ローカルディスクのみが復元されます。復旧作業中でも共有ディスクはすべてオンラインであり、稼動中のノードにより所有/ロックされているためです。

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。

MSCSデータベースの復元は、すべてのノードの復旧が完了し、それらがクラスターに参加したあとに実行できます。そうすることによって、すべてのノードが共同作用することを確実にします。MSCSデータベースは、WindowsのCONFIGURATIONに含まれています。オンラインヘルプの索引「構成オブジェクトの復元」を参照してください。

一次ノードの障害復旧

この場合、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は実行されていません。

障害復旧に関する他の必要条件に加えて、以下の条件も満たされている必要があります。

- 一次ノードはクォーラムディスクへの書き込みが可能である必要があります(クォーラムディスクはロックされていてはいけません)。
- Cell Manager を復旧する場合、一次ノードはすべてのIDBボリュームへの書き込みが可能である必要があります。
- すべての物理ディスク資源がオンラインになるまで、他のノードはすべてシャットダウンしておく必要があります。

この場合、一次ノードの復元の際にはクォーラムディスクを最初に復元します。Cell Managerがクラスターにインストールされている場合には、IDBの復元も必要です。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。一次ノードの復元が完了したら、残りの全ノードの復元が可能となります。

注記:

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います。共有クラスターディスクを交換した場合、障害復旧のフェーズ1でこのディスク署名が変わることになります。その結果、クラスターサービスは交換されたディスクを有効なクラスター資源として認識せず、その資源に依存するクラスターグループは正常に動作しません。詳細は、「Windows でのハードディスク署名の復元」(99ページ)を参照してください。

一次ノードの復元は、以下の手順で行います。

1. クォーラムディスクを含めて、プライマリノードの障害復旧を実行します。
   - 半自動障害復旧の場合: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(-full_clusオプション)によって自動的に復元されます。
   - 拡張自動障害復旧およびワンボタン障害復旧の場合:復旧範囲を尋ねられたときに、[**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
   - 自動システム復旧の場合: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は、自動的に復元されます。

   ヒント:

   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。他のノードによりロックされている共有ディスクボリュームのディスクをフェーズ1で構成するために必要な情報を収集するのは不可能です。

2. システムを再起動します。
3. クラスター データベースを復元します。MSCSデータベースは、Windows の CONFIGURATION に含まれています。オンラインヘルプの索引「構成オブジェクトの復元」を参照してください。

注記:

MSCSデータベースを復元するには、MSCSサービスが実行中である必要があります。したがって、障害復旧のフェーズ2では自動的に復元されません。しかし、クラスターデータベースはフェーズ2の最後にData Protector標準復元手順で復元できます。

4. Cell Manager を復元している場合は、IDBの整合性を取ります。(「IDB の整合性をとる (すべての方法)」(101ページ)を参照)。

5. 定数ボリュームとIDBボリュームが復元されます。他のすべてのボリュームは影響を受けず、破損していなければ復元された一次ノードにより所有されます。

   他のボリュームが破損していた場合は、以下を行う必要があります。

   a. クラスターサービスとクラスターディスクドライバを使用不可にします(MSDN Q176970に記述されているとおりに行う必要があります)。

   b. システムを再起動します。

   c. 従来の記憶データ構造を再構築します。

   d. クラスターサービスとクラスターディスクドライバを使用可能にします。

   e. システムを再起動します。

   f. 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。

6. 残りのノードを復元します。(「二次ノードの障害復旧」(95ページ)を参照)。

EADR 用に全ノードのP1Sファイルをマージ

EADRを行うには、バックアップ実行後に特別な手順が必要です。バックアップ時に他のノードによりロックされている共有ディスクボリュームのディスクをフェーズ1で構成するために必要な情報を収集するのは不可能です。すべての共有ディスクボリュームを復元するにはこの情報が必要です。クラスター内の全ノードのP1Sファイルに共有クラスターボリューム情報を含めるには、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実行後、クラスター内の全ノードのP1Sファイルに含まれる共有クラスターボリューム情報をマージします。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。
- すべての共有クラスターボリュームを一時的にバックアップ対象のノードに移動します。こうすれば、すべての共有クラスターボリュームに関する必要情報が収集されます。この場合、一次ノードにできるのはこのノードだけです。

全ノードのP1Sファイルをマージするには、以下のようにData_Protector_home¥bin¥drim¥binから mmerge.cmdコマンドを実行します。

```
mmerge p1sA_path ... p1sX_path
```

ここで、p1sAはMSCS内の最初のノードのP1Sファイルへのフルパスであり、p1sX は最後のノードのP1Sファイルへのフルパスです。マージ後のP1Sファイルは元のP1Sファイルと同じディレクトリに保存され、ファイル名には.merged が追加されます (例: computer.company.com.merged)。元のファイルの他のディレクトリに移動した後、マージ後のP1Sファイルの名前を元の名前に変更します(.merged拡張子を削除する)。

UNIXCell Managerのみ: mmerge.cmdコマンドは、Data Protector自動障害復旧モジュールがインストールされた Windowsシステムでのみ動作します。UNIX Cell Managerを使用している場合は、P1Sファイルを自動障害復旧モジュールがインストールされたWindows

クライアントにコピーして、ファイルをマージします。マージ後のP1Sファイルの名前を元の名前に変更し、Cell Managerにコピーします。

例

MSCS用のP1Sファイルの2つのノードでのマージ例: mmerge Data_Protector_home¥Config¥server¥dr¥p1s¥node1.company.com Data_Protector_home¥Config¥server¥dr¥p1s¥node2.company.com.パス名に空白が含まれている場合には、Windowsではパス名を引用符で囲む必要があります。マージ後のファイルは、node1.company.com.mergedとnode2.company.com.merged です。これらのファイルの名前を元の名前(node1.company.comとnode2.company.com)に戻します。この場合、最初に元のP1Sファイルの名前を変更する必要があります。

Windows でのハードディスク署名の復元

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います。共有クラスターディスクを交換した場合、障害復旧のフェーズ1でこのディスク署名が変わることになります。その結果、クラスターサービスは交換されたディスクを有効なクラスター資源として認識せず、その資源に依存するクラスターグループは正常に動作しません。最低1台のノードが稼動中でその資源を所有している限り、共有クラスター資源は運用可能であるため、これはアクティブなノードを復元する場合のみ当てはまります。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。クリティカルディスク以外のディスクを交換した場合は、そのハードディスク署名を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。これを交換した場合は元のディスク署名を復元する必要があり、そうしないとクラスターサービスは開始しません。

フェーズ2において、MSDSデータベースはシステムボリュームの¥TEMP¥ClusterDatabaseに復元されます。システムを再起動しても、クラスターサービスは実行されません。これは、フェーズ1でハードディスク署名が変わったために、クォーラムリソースが識別されないためです。この問題は、(*Data_Protector_home*¥binlnsにある)clubarユーティリティを実行して、元のハードディスク署名を復元することで解決できます。clubarが正常終了すると、クラスターサービスが自動的に開始されます。

例

コマンドプロンプトで、clubar r c:¥temp¥ClusterDatabase force q:と入力し、c:¥temp¥ClusterDatabaseから、MSCSデータベースを復元します。

clubar の使用法と構文の詳細は、*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上のData Protector共有ディスクがクォーラムディスクと異なる場合は、これも復元する必要があります。Data Protector共有ディスクと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 2000リソースキットに含まれているdumpcfgユーティリティを使用します。dumpcfgの使用法の詳細は、dumpcfg /?を実行するか、Windows 2000リソースキットのマニュアルを参照してください。Windows 2000におけるハードディスク署名に関する問題については、MSDN Q280425を参照してください。

元のハードディスク署名はSRDファイルから取得できます。SRDファイル内の署名には、番号の後にvolumeというキーワードが付いています。

例

```
-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
```

-volume の後の数字がハードディスク署名です。この例では、SRDファイルに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)に関する情報が保存されています。クォーラムディスクの署名は、バックアップ時にアクティブだったノードのSRDファイルにだけ保存されています。これは、アクティブなノードがクォーラムディスクをロックしており、他のノードはクォーラムディスクにアクセスできないためです。したがって、常にクラスター全体のバックアップを取ることをお勧めします。これは、フェーズ1で共有ディスクボリュームのディスクを構成するのに十分な情報を得るにはすべてのSRDファイルを揃える必要があり、これにはクラスター内の全ノードのSRDファイルが必要なためです。SRDファイルに保存されているハードディスク署名は10進数で表示されていることに注意してください。これに対して、dumpcfgコマンドでは16進数を指定する必要があります。

マジョリティノードセットクラスターでの自動システム復旧

マジョリティノードセット(MNS)クラスターで自動システム復旧(ASR)を実行するには、次の手順を実行してください。

1. MNS クラスターを設定し、そのクラスターにData Protectorクライアントをインストールします。

   MNSクラスターにCell Managerはインストールできないことに注意してください(サポートされていません)。

2. ファイルシステムのバックアップ、構成のバックアップ、IDBのバックアップを実行します。

3. ASRディスク セットを作成します。

   ASRの準備方法、ASRセットを作成するための準備、ASRを使用する復旧の手順については、オンラインヘルプの索引キーワード「自動システム復旧」で表示される内容を参照してください。

4. ノードで障害復旧を実行します。

   障害復旧準備方法など、詳細な手順については、オンラインヘルプの索引キーワード「障害復旧」で表示される内容を参照してください。

ノードが復旧し、クラスターに参加できるようになります。

Data Protector Cell Manager 固有の復元手順

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 (すべての方法)

この項に記載の手順は、一般的な障害復旧手順の実行後のみ使用します。

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データベース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 ProtectorGUI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、オンラインヘルプの索引「メディアのリサイクル」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。このような場合は、Data Protectorプロセスを中止して、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。

   Windows VistaおよびWindows Server 2008:

   ```
   Data_Protector_home¥bin¥omnisv -stop
   del Data_Protector_program_data¥tmp¥*.*
   Data_Protector_home¥bin¥omnisv -start
   ```

   他のWindowsシステムの場合:

   ```
   Data_Protector_home¥bin¥omnisv -stop
   del Data_Protector_home¥tmp¥*.*
   Data_Protector_home¥bin¥omnisv -start
   ```

2. 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 ProtectorGUIを使ってエクスポートします。メディアのエクスポートの詳細については、オンラインヘルプの索引「エクスポート、メディア」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 ProtectorGUIを使ってインポートします。メディアのインポートの詳細については、オンラインヘルプの索引「インポート、メディア」を参照してください。

拡張自動障害復旧に固有の手順

拡張自動障害復旧を使用して、WindowsCell Managerを復元する場合には、フェーズ0で2つの特別な手順が必要です。

- Cell Manager用の障害復旧CDを事前に用意しておく必要があります。

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 CD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。

- 障害復旧の準備作業の一環として、Cell Managerの更新済みのSRDファイルを、Cell Manager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」(42ページ)を参照)。
- 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、障害復旧は実行できなくなります。

  「準備」(42ページ) を参照してください。

重要:

バックアップメディア、DRイメージ、SRDファイル、暗号化キーの保存されたリムーバブルメディア、障害復旧CDへのアクセスを制限しておくことをお勧めします。

ワンボタン障害復旧に固有の手順

Cell Managerが障害の影響を受けている場合はIDBが使用できないため、OBDRのブート可能メディアの位置を知っておく必要があります。

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OBDRバックアップを実行して新しいブート可能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。

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、障害復旧は実行できなくなります。

「準備」(42ページ) を参照してください。

重要:

バックアップメディアと暗号化キーが保存されたリムーバブルメディアへのアクセスを制限することをお勧めします。

自動システム復旧に固有の手順

自動システム復旧(ASR)を使用してWindows Cell Managerを復旧する場合には、フェーズ0で別途手順が必要です。

- Cell Manager用のASRディスクを事前に用意しておく必要があります。

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ASRディスクを更新します。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。

重要:

バックアップメディアとASRディスクへのアクセスを制限することをお勧めします。

Internet Information Server (IIS) の復元に固有の手順

Internet Information Server (IIS)は、障害復旧ではサポートされていません。IISの半自動障害復旧を行うには、(通常の半自動障害復旧の手順に加えて)以下の手順を実行してください。

1. 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でください。
2. IIS Admin Serviceが実行されている場合は、それを停止またはアンインストールします。
3. drstartコマンドを実行します。
4. IISデータベースがプレーン ファイルとして、デフォルトのIISディレクトリ(%SystemRoot%¥system32¥inetsrv)に復元されます(ファイル名はDisasterRecovery)。
5. ブートが正常に終了したら、Data Protector標準復元手順、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。この処理は長時間かかることに注意してください。

トラブルシューティング

1. IISに依存するサービス(SMTP、NNTPなど)のいずれかが自動的に起動されない場合は、手動での起動を試みてください。
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overwriteオプションを使用して復元してください。

注記:

%SystemRoot%¥system32¥inetsrvはIISサービスのデフォルトのディレクトリです。IISサービスを別のディレクトリにインストールした場合は、MetaBase.binファイルの復元先としてそのディレクトリを指定してください。

3. IIS Admin Serviceと、それに依存するサービスをすべて起動します。

kb.cfgファイルの編集

ドライバの中には、正常に動作するために必要な機能が複数のファイルに分かれているものがあります。それらがkb.cfgファイルに逐次列挙されていなければ、Data ProtectorはDRイメージファイルの作成中にすべてのドライバファイルを特定できません。この場合、それらのファイルは障害復旧操作システムに含まれず、その結果、DR OSの起動後に一部のドライバやサービスが動作しなくなります。

kb.cfgファイルはData_Protector_home¥bin¥drim¥configディレクトリにあり、%SystemRoot%ディレクトリにあるドライバファイルの位置に関する情報を含んでいます。テストプランの実行時に、OSが起動した後、必要なサービスがすべて実行中で、必要なドライバがすべて動作することを確認してください。

これらのドライバ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ファイルに適切な形式で追加します。この形式についての指示は、kb.cfgファイルの最初に記述されています。

このファイルを編集する最も簡単な方法は、既存の行をコピー、ペーストして適切な情報に書き換えることです。パスの区切り文字が/(スラッシュ)であることに注意してください。パス名が引用符で囲まれている場合以外、空白は無視されます。したがって、エントリを複数行にまたがって記述することもできます。また、#(シャープ)記号で始まり行末で終わるコメント行も追加できます。

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DRイメージに含めるために、「準備」(59ページ)の記述に従ってフルクライアントバックアップを再度実行します。

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。そのため、自らの責任でこのファイルを変更して、ドライバや他のファイルを含めてください。

このファイルへのあらゆる変更はユーザーの責任であり、Hewlett-Packardのサポート対象外となります。

⚠ 警告!

kb.cfg ファイルの編集後に復旧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必要があります。

編集後のSRDファイルを使用した復旧

障害復旧を実行する時点で、SRDファイルに保存されているバックアップデバイスまたはメディアに関する情報が古くなっている場合もあります。オンライン復旧を実行する場合

には、必要な情報がCell ManagerのIDBに保存されているため、これは問題となりません。しかし、オフライン復旧を行う場合には、IDBの保存されている情報に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、更新されたSRDファイル(recovery. srd) に保存されているバックアップデバイスに関する情報が正しくないため、復旧に失敗します。この場合は、更新されたSRDファイルを障害復旧のフェーズ2を実行する前に編集して、復旧が正常終了するように不正な情報を更新します。

SRDファイルを編集するには、テキストエディタを使ってSRDファイルを開き、変更された情報を更新します。

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、復旧しようとしているシステムのクライアント名が変更されている場合は、-hostオプションの値を書き換えます。以下に示す項目についても情報の修正が可能です。

- Cell Managerクライアント名(-cm)
- Media Agentクライアント(-mahost)
- 論理デバイスまたはドライブ(ライブラリ)の名前(-dev)
- デバイスの種類(-devtype)

  -devtypeオプションに指定可能な値については、sanconfマンページまたは『HP Data Protector command line interface reference』を参照してください。
- デバイスのSCSIアドレス(-devaddr)
- デバイスのポリシー(-devpolicy)

  ポリシーには、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エクスチェンジャライブラリ)、9(STKサイロメディアライブラリ)、10(SCSI-IIライブラリ)のいずれかを定義します。
- ロボティクスのSCSIアドレス(-devioctl)
- ライブラリスロット(-physloc)
- 論理ライブラリ名 (-storname)

ファイルの編集が完了したら、Unicode(UTF-16)形式で元の場所に保存します。

例

MAクライアントの変更

old_mahost.company.com クライアントに接続されたバックアップデバイスを使用して、障害復旧バックアップを実行した場合を考えてみましょう。障害復旧時には、このバックアップデバイスがnew_mahost.company.comクライアントに同じSCSIアドレスで接続されていたとします。この場合、障害復旧を適切に実行するには、障害復旧のフェーズ2を開始する前に、(変更された)SRDファイル内の-mahost old_mahost.company.comという文字列を-mahost new_mahost.company.comに変更する必要があります。

新しいMAクライアント上でバックアップデバイスのSCSIアドレスが変更されている場合は、更新したSRDファイル内の-devaddrオプションの値を適切に変更してください。

例

バックアップデバイスとMAクライアントの変更

バックアップ時とは異なるデバイスを使用して障害復旧を実行するには(MAクライアントは同じものを使用)、更新されたSRDファイル内の次のオプションの値を変更します。-dev, -devaddr, -devtype, -devpolicy, and -devioctl。復元用にライブラリデバイスを使用する場合は、SRDファイル内の次のオプションの値も変更してください。-physloc と -storname。

たとえば、障害復旧の目的で、HP StorageWorks Ultriumスタンドアロンデバイスを使用してバックアップが実行した場合を考えてみましょう。デバイス名はUltrium_dagnjaで、MAホストdagnja (Windows)に接続されています。ただし、障害復旧時には、HP StorageWorks Ultriumロボティクスライブラリを使用するものとします。このライブラリの論理ライブラリ名はAutoldr_keralaで、ドライブUltrium_keralaがMAクライアントkerala(Linux)に接続されています。

最初にkerala上でdevbra -devコマンドを実行して、構成されているデバイスとその構成情報の一覧を確認しておきます。この情報は、更新されたSRDファイル内の以下のオプション値を変更するために必要です。

-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.

編集後のSRDファイルを障害復旧に使用する手順は、それぞれの障害復旧の方法により異なります。詳細は個々の障害復旧の方法に関する項を参照してください。

重要:

セキュリティ上の理由から、SRDファイルへのアクセスは制限する必要があります。

AMDR/ASR

通常のAMDR/ASR復旧手順を実行する前に、以下を実行します。

1. 最初のdrsetup/ASRディスクにあるrecovery.srd ファイルをテキストエディタで開き、必要な変更を行います。
2. Unicode(UTF-16)形式で元の場所に保存します。

EADR/OBDR

通常のEADR/OBDR 復旧手順を実行する前に、以下を実行します。

1. 障害復旧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、**[完了]**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、障害復旧のフェーズ1を完了できます。Install onlyを選択した場合、障害復旧のフェーズ2が自動的には開始されません。

図 9 障害復旧ウィザードのInstall onlyオプション

2. Windows タスクマネージャを実行します(**Alt+Ctrl+Del** キーを押し、**[タスクマネージャ]**を選択)。
3. **[ファイル]**をクリックし、**[新しいタスクの実行]**を選択します。notepad c:¥DRSYS¥System32¥OB2DR¥bin¥recovery.srdと入力して**Enter**キーを押します。SRDファイルがメモ帳で開きます。
4. SRDファイルを編集します。編集方法の詳細は、『「システム復旧データ(SRD)の更新と編集」(36ページ)』を参照してください。

5. SRDファイルを編集して保存したら、c:¥DRSYS¥System32¥OB2DR¥binディレクトリから以下のコマンドを実行します。

   omnidr -drimini c:¥$DRIM$.OB2¥OBRecovery.ini

6. 通常のEADR/OBDR 復旧手順における次の手順に進みます。

CLIインターフェースを使用したASRフロッピーディスクの更新

Data ProtectorにはASRフロッピーディスクを*自動的*に作成できるCLIコマンドはありません。ただし、omnisrdupdateコマンドを使用すると、ASR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。ASR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。

```
omnisrdupdate -session 11/04/2005-1 -host computer1.com -location a:¥
-asr
```

ASRフロッピーディスクを*手動*で作成するには、さらに、Data_Protector_home¥Depot¥DRSetup¥Diskdisk_numberフォルダからDRdisk_number.cabファイルを適切なASRフロッピーディスクにコピーする必要があります。

WindowsのBitLockerドライブ暗号化でロックされたボリュームのロック解除

制限事項

- 障害復旧モジュールには、BitLockerドライブ暗号化を使用して暗号化されているボリュームを検出し、そのロックを解除するオプションがあります。特定のボリュームに対してロックを解除しない場合や、ボリュームが破損しておりロック解除ができないためにフォーマットを実行することが必要な場合、そのボリュームは*障害復旧後に暗号化されなくなります*。このような状況では、ボリュームを再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

障害復旧中に、暗号化されているボリュームを障害復旧モジュールが検出すると、ロックを解除するオプションが表示されます。

```
System storage inspection discovered n locked volume(s).
Unlock? [y/n]
```

```
(システムストレージの点検によりn個のロックされたボリュームが見つかりました。
ロックを解除しますか。[y/n])
```

暗号化されているボリュームをロック解除するには、以下の手順を実行します。

1. yを押してロック解除手順を開始します。
2. 2 ボタンを押して、選択メニューを開きます。
3. パスワードを含むボリューム(USBフラッシュドライブなど)が検索パスのリストに表示されているかどうか確認します。以下のようなメッセージが表示されます。

   ```
   Search dir(s): [a:¥]
   [d:¥]
   ```

   パスが表示されない場合:

   a. searchと入力します。新しいメニューが表示されます。

   b. 検索ディレクトリ(たとえば、USBフラッシュドライブがm:¥にマウントされている場合はm:)を入力します。一度に複数のディレクトリを追加できます。.

      ディレクトリが検索パスに表示されます。

      ```
      Search dir(s): [a:¥]
      [d:¥]
      [m:¥]
      ```

4. ロックを解除するボリュームを入力します (c:など)。ドライブ文字を使用せず、ボリュームのGUID(¥¥?¥Volume{GUID}など)でボリュームを指定したり、複数のボリュームを一度に指定することができます。

   全ボリュームのロックを解除するには、allと入力します。

   キーファイルがUSBフラッシュドライブやフロッピーディスクから取得できない場合は、以下のプロンプトが表示されます。

   ```
   Type one of the following:
   * External key path
   * Numerical password (groups separated by hyphens)
   * Exit
   ```

   (以下のいずれかを入力します。* 外部のキーのパス * 数値のパスワード(グループをハイフンで区切る) * 終了)

   数値のパスワードを入力します。

4 UNIXの障害復旧

HP-UXクライアントの手動による障害復旧

この項では、HP-UXクライアントの障害復旧の手順を説明します。

この手順は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フェースに加え)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。

Ignite-UXはターゲットクライアントの障害復旧に特化しているため(フェーズ1およびフェーズ2)、障害復旧のフェーズ3でユーザーデータとアプリケーションデータを復元するにはData Protectorを使用する必要があります。

注記:

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で、障害に対する準備と障害の復旧を行うには2つの方法があります。

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

ゴールドイメージを使用する方法は、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環境に適しています。一方、システム復旧ツールを使用する方法は、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の作成をサポートしています。

どちらの方法でも、DDSテープやCDなどのブート可能インストールメディアの作成が可能です。これらのメディアを使用して、システム管理者は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、ローカルに障害復旧を行うことができます。さらに、どちらの方法でも、故障したクライアントに適切なゴールドイメージ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。その

場合、クライアントはIgniteサーバーから直接ブートし、割り当てられたデポからインストールを実行します。このデポはネットワークの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。

カスタムインストールメディアの使用

概要

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、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、ゴールドイメージなど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パラメータを変更したり、Data Protectorなどのソフトウェアをイメージに追加したりする機能(Ignite-UXのmake_configコマンド)があります。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. **フェーズ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. **フェーズ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. **フェーズ3**
   a. Data Protectorの標準復元手順を使用して、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。

準備

以下に、クライアントシステムのゴールドイメージをターゲットシステム上に作成する手順を示します。ターゲットシステムは、NFSを介してゴールドイメージをネットワークに提供します。この例では、Data Protectorクライアントはすでにクライアントシステムにインストールされており、特別な構成手順を行わなくても“ゴールドイメージ”に含まれることになります。

1. Ignite-UXサーバーの/opt/ignite/data/scripts/make_sys_imageファイルを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、make_sys_image -dアーカイブのディレクトリ -nアーカイブ名.gz -s ターゲットシステムのIPアドレスコマンドを実行して、クライアントの圧縮イメージを他のシステム(ターゲットシステム)上に作成します。

   このコマンドにより、GZIPで圧縮されたファイルデポが-dオプションと-sオプションで指定したシステムの指定ディレクトリに作成されます。HP-UXクライアントが、ターゲットシステムへのパスワードなしのアクセス権を与えられていること(ターゲットシステムの.rhostsファイルにクライアントシステム名のエントリがあること)を確認してください。アクセス権がない場合、コマンドは失敗します。

3. ターゲットディレクトリをターゲットシステムの/etc/exportsディレクトリに追加し、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. Ignite-UXサーバーの構成で、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.11.11/
archive_HPUX11_11_DP50_CL.cfg
```

5. コピーした構成ファイルの以下のパラメータを確認して変更します。

   - 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_1"
     post_config_script =
     "/opt/ignite/data/scripts/os_arch_post_c"
     nfs_source = "IP Target System:Full Path"
     ```

   - 対応するOS archiveセクション:

     ```
     archive_path = "archive_name.gz
     ```

6. 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、出力を以下の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_11_DP50_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. 新しく作成したデポをIgnite-UXに認識させるには、/var/opt/ignite/INDEXファイルにcfgエントリを以下のレイアウトで追加します。

```
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_11_DP50_Client" {
description "HPUX 11.i OS incl Patches and DP50 Client"
"/opt/ignite/data/Rel_B.11.11/config"
"/var/opt/ignite/data/Rel_B.11.11/archive_HPUX11_11_DP50_CL.cfg
"
}
```

8. ブートするクライアント用に予約してある1つ以上のIPアドレスが、/etc/opt/ignite/instl_boottabファイル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。

上記の手順を完了すると、HP-UXクライアントのゴールドイメージ(固有のハードウェアおよびソフトウェア構成を含む)が作成されます。このイメージは、同様の構成のシステムを復旧するために使用することができます。

ハードウェアおよびソフトウェア構成が異なるシステムすべてに対して、ゴールドイメージの作成手順を繰り返します。

注記:

Ignite-UXを使用して、作成したゴールドイメージからブート可能テープ/CDを作成することができます。詳細は、『*Ignite-UX管理ガイド*』を参照してください。Ignite-UXを使用して、作成したゴールドイメージからブート可能テープ/CDを作成することができます。詳細は、『Ignite-UX管理ガイド』を参照してください。

復旧

ネットワークのNFS共有上にあるゴールドイメージを適用してHP-UXクライアントを復旧するには、以下の手順を実行してください。

1. *クライアントシステムでの手順*
   a. 障害が発生したハードウェアを交換します。
   b. 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
   c. [Welcome to Ignite-UX]画面が表示されたら、[Install HP-UX]を選択します。
   d. [UI Option]画面で[Remote graphical interface running on the Ignite-UX server]を選択します。
   e. ネットワーク構成ダイアログボックスに応答します。
   f. 以上で、Ignite-UXサーバーによるリモート制御インストールに対するクライアントシステムの準備は完了です。
2. *Ignite-UXサーバーでの作業*
   a. Ignite-UX GUIの[client]アイコンを右クリックし、[Install Client]→[New Install]]を選択します。
   b. インストールするゴールドイメージを選択し、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!]ボタンをクリックします。
   c. [client]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が確認できます。
   d. インストールが完了したら、Data Protectorの標準復元手順で、追加する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。

システム復旧ツールの使用

概要

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、Data Protectorのファイルやディレクトリなど)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ブートすることで、無人の障害復旧が可能となります。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ブートするか、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ブートは、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. **フェーズ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. **フェーズ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. **フェーズ3**
   a. Data Protectorの標準復元手順を使用して、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。

準備

HP-UXクライアントの復旧アーカイブを最も簡単に作成するには、Ignite-UXサーバー上でIgnite-UX GUIを使用します。GUIコマンドはすべて、コマンド行からも実行できます。詳細は、『*Ignite-UX管理ガイド*』を参照してください。

前提条件

システム障害に対する準備を行う前に、Ignite-UXファイルセットをクライアントにインストールして、Ignite-UXサーバーとクライアントが通信できるようにする必要があります。Ignite-UXファイルセットのリビジョンが、Ignite-UXサーバーとクライアントで同じであることを確認します。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サーバーで以下のコマンドを実行します。

```
pkg_rec_depot -f
```

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。

クライアントにIgnite-UXをインストールしたら、Ignite-UXサーバーのGUIで、make_net_recoveryまたはmake_tape_recoveryを使用して復旧アーカイブを作成します。

make_tape_recoveryを使用したアーカイブの作成

make_tape_recoveryを使用してアーカイブを作成するには、以下の手順を実行します。

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. 以下のコマンドを実行して、Ignite-UX GUIを起動します。/opt/ignite/bin/ignite &
3. [client]アイコンを右クリックして、[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には、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. テープ作成プロセスが開始されます。[client]アイコンを右クリックし、[Client Status]を選択して、ステータスとIgnite-UXサーバー上のログファイルを確認します。

注記:

Ignite-UXでは、すべてのDDSがどのDDSドライブでも確実に使用できるように、90mのDDS1バックアップテープの使用を推奨しています。

make_net_recoveryを使用したアーカイブの作成

make_net_recoveryを使用した復旧アーカイブの作成手順は、make_tape_recoveryの場合とほとんど同じです。この方法の利点は、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ため、ローカルに接続するデバイスが不要であることです。

1. 以下のコマンドを実行して、Ignite-UX GUIを起動します。/opt/ignite/bin/ignite &
2. [client]アイコンを右クリックして、[Create Network Recovery Archive]を選択します。
3. 保存先のシステムとディレクトリを選択します。圧縮されたアーカイブを保存できるだけの容量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. アーカイブ作成プロセスが開始されます。[client]アイコンを右クリックし、[Client Status]を選択して、ステータスとIgnite-UXサーバー上のログファイルを確認します。

注記:

Ignite-UXでは、ブート可能なアーカイブテープを圧縮アーカイブファイルから作成することができます。『*Ignite-UX管理ガイド*』の「ネットワーク経由でのリカバリアーカイブの作成」を参照してください。

復旧

バックアップテープからの復旧

make_tape_recoveryで作成したブート可能なテープを使用してシステムの障害復旧を行うには、以下の手順を実行します。

1. 障害が発生したハードウェアを交換します。

2. 影響を受けた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. 用意した復旧テープからブートします。そのためには、boot adminメニューで「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出力します。どれがテープドライブであるかを確認して、ブートコマンドboot *hardware path*またはboot Pnumberを入力します。
4. 復旧プロセスが自動的に開始されます。
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

HP-UXクライアントの障害復旧をネットワーク経由で行うには、ゴールドイメージによる復旧手順に従います。インストールしたいアーカイブが選択されていることを確認します。

- **クライアントでの手順**
  1. 障害が発生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]画面で[**Install HP-UX**]を選択します。
  4. [UI Option]画面で[**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. 以上で、Ignite-UXサーバーからのリモート制御インストールに対するクライアントシステムの準備は完了です。
- **Ignite-UXサーバーでの作業**
  1. Ignite-UX GUIの[**client**]アイコンを右クリックし、[**Install Client**]→[**New Install**]を選択します。
  2. [Configurations]で、インストールする[**Recovery Archive**]を選択して設定(ネットワーク、ファイルシステム、タイムゾーンなど)を確認し、[**Go!**]ボタンをクリックします。
  3. [**client**]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が確認できます。
  4. 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。

UNIXクライアントのディスクデリバリーによる障害復旧

UNIXクライアントの障害復旧をディスクデリバリーで実行するには、影響を受けたシステムに、最低限のOSのインストールとData Protector Disk Agentが含まれているブート可能なディスクを接続します。管理者は、ディスクのフォーマットおよびパーティションの構成が正しく行われるよう、障害発生前に十分なデータを収集する必要があります。

サポート対象のオペレーティングシステムについては、『*HP Data Protector product announcements 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。

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。

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. **フェーズ0**
   a. 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)を実行します。
   b. 補助ディスクを作成します。
2. **フェーズ1**
   a. 問題のあるディスクを交換し、補助ディスクをターゲットシステムに接続した後、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。
3. **フェーズ2**
   a. Data Protectorの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。
4. **フェーズ3**
   a. Data Protectorの標準復元手順を使用して、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

- ここでは、クラスター環境の復旧については説明しません。クラスター環境の構成によっては、特別な手順や環境の変更が必要です。
- RAIDはサポートされていません。
- 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。

準備

この障害復旧の準備は、バックアップ仕様に関する情報の収集、ディスクの準備、バックアップ仕様の準備(実行前)、バックアップの実行など、数段階に分けて実行する必要があります。クライアントの障害復旧を実行する前に、これらの準備手順をすべて行うことが必要です。

この項では、復旧作業を正しく実行するため、バックアップ時に各ターゲットシステムに対して実行する必要のある項目を示します。これらの情報を実行前コマンドの一部として収集する場合は、これらのファイルのあるディレクトリを障害復旧プランに明記して、障害発生時にこの情報を見つけやすくしておくことが必要です。また、バージョン管理(バックアップごとの「補助情報」を集めたもの)についても考慮が必要です。

- バックアップ対象のシステムがアプリケーションプロセスを低実行レベルで実行している場合は、復旧後のエラーを避けるため、*最小限の動作*状態(修正*init*1*実行レベル*)を確立して、シングルユーザーモードに入ることが必要です(「整合性と関連性を兼ね備えたバックアップ」(34ページ)を参照してください)。詳細は、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*:**

例

1. 抹消リンクを/sbin/rc1.dから/sbin/rc0.dに移動して、ブートセクションに対する変更内容を補足します。抹消リンクには基本サービスが含まれており、上記の作業を行わなかった場合、実行レベル1に移行することによってこのサービスは中断されます。このサービスはバックアップに必要です。例として、「抹消リンクの移動(HP-UX 11.x)」(145ページ)を参照してください。

2. システムでrpcdを構成します(ファイル/etc/rc.config.d/dceで変数RPCD=1を構成します)。

   これにより、システムを最小限の動作状態で実行する準備ができました。この状態の特徴を以下に示します。

   - 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。
   - inetd、rpcd、swagentdの各プロセスも実行されます。

Solarisの場合:

例

1. rpc抹消リンクを/etc/rc1.dから/etc/rc0.dに移動して、ブートセクションに対する変更内容を補足します。抹消リンクには基本サービスが含まれており、上記の作業を行わなかった場合、実行レベル1に移行することによってこのサービスは中断されます。このサービスはバックアップに必要です。
2. 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、システムが最小限の動作状態で実行する準備ができました。この状態の特徴を以下に示します。

   - Init 1
   - ネットワークが稼動している必要があります。
   - inetd、rpcbindの各プロセスも実行されます。

Tru64の場合:

例

1. システムの電源がオフになっている場合は、システムをブートし、System Reference Manual (SRM)コンソール(ファームウェアコンソール)を起動します。
2. SRMコンソールから以下のコマンドを実行して、シングルユーザーモードに切り替えます。
   - boot -fl sで、生成済みのvmunixファイルを使用して起動します。
   - boot -fi genvmunix -fl sで、一般的なカーネルを使用するシングルユーザーモードに入ります。
3. システムの電源が既に投入されており、システムが既に稼動している場合は、init sコマンドを実行して現在の実行レベルからシングルユーザーモードに切り替えます。

AIXの場合:

操作は必要ありません。補助ディスクの作成に使用するalt_disk_installコマンドにより、システムの動作状態を最小限にしなくてもディスクイメージの整合性が保証されるためです。

- 補助ディスクを使用して障害復旧を行う場合は、補助ブートディスクを準備する必要があります。1つのサイトとプラットフォームにつき、ブート可能な補助ディスクが1台だけ必要です。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おり、ブート可能であることが必要です。
- 以下を実行する実行前スクリプトを作成します。
  - 保管場所の物理的および論理的保存構造
  - 現在の論理ボリュームの構造(HP-UXの場合、vgcfgbackupとvgdisplay -vを使用)
  - MC/ServiceGuardの構成データ、ディスクミラーリング、ストライピング
  - ファイルシステムとマウントポイントの概要(HP-UX の場合、bdf、または/etc/fstabのコピーを使用)
  - システムのページングスペース情報(HP-UXの場合、swapinfoコマンドの出力を使用)
  - I/O構造の概要(HP-UXの場合、ioscan -funとioscan -fknを使用)
  - クライアントのネットワーク設定

  環境に関して必要なすべての情報を収集して、収集した情報を障害復旧時に使用可能な場所に保存します。このスクリプトは、容易にアクセスできる別のシステムに保存することをお勧めします。収集する情報を以下に示します。
  - データの非常用コピーもバックアップに保存できます。ただし、これを実行した場合は、実際の復旧を行う前にこの情報を取り出しておく必要があります。
  - システムからすべてのユーザーを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。
  - バックアップの実行中に他のユーザーがシステムにログオンできないように、システムへのネットワークアクセスを制限します(たとえば、HP-UXの場合、inetd.secを上書きして、inetd -cを使用します)。
  - 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上では、sbin/init 1を使用し、60秒待ち、run_levelが1になっている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。
- システムの実行レベルを標準にする実行後スクリプトを実行して、アプリケーションの再起動などを行います。

- Data Protector Cell Manager上のクライアントに対するバックアップ仕様を設定します。バックアップ仕様には、すべてのディスクを指定し(ディスクディスカバリを使用)、実行前/実行後スクリプトを指定することが必要です。
- 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)。

復旧

この項では、バックアップ実行時の状態にシステムを復元する方法を説明します。ディスクデリバリーによる障害復旧を正しく実行するには、以下が必要です。

- 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
- 適切なオペレーティングシステムとData Protectorエージェントを含む補助ディスク
- 復旧対象のクライアントの正常なフルバックアップ

以下のステップを実行します。

1. 問題のあるディスクを新しいディスク(同等サイズ)と交換します。
2. 補助ディスク(適切なオペレーティングシステムとData Protectorクライアントが含まれているディスク)をシステムに接続して、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の場合は、LVMを使用)。ルート以外のボリュームグループについては、保存されているデータを使用します(HP-UXの場合は、vgcfgrestoreまたはSAMを使用)。
5. さらに、復元対象のルートボリュームグループを修復済みディスク上に作成します(HP-UXの場合は、vgimportを使用)。このボリュームグループは、復元プロセス中はルートボリュームグループとはみなされません。これは、補助ディスクからOSを実行しているためです。vgimportの詳細については、同コマンドのマンページを参照してください。
6. 新しいディスクをブート可能にします。
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、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であれば、/etc_restoreのようにします。
9. マウントポイントにある復元対象のファイルをすべて削除して、マウントポイントを空の状態にします。

10. Data Protector GUIを起動して、Cell Managerとの接続を開始します。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。
11. 復元するバージョンを選択します。まず復元に必要なメディアをすべてリストして、それらが使用可能であることを確認します。[Restore As 新しいマウントポイント名]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。
12. 復元したシステムをシャットダウンします。
13. 補助ディスクをシステムから取り外します。
14. 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。

注記:

補助ディスクの代わりに、新しいディスクを、Disk Agentがインストールされているクライアントシステムに一時的に接続することもできます。復元後、新しいディスクを障害が発生したシステムに接続し、ブートします。

UNIX Cell Managerの手動による障害復旧

手動による障害復旧は、基本的な障害復旧の方法です。この方法には、最初にインストールした時と同様の方法でシステムを再インストールして復旧する他に、Data Protectorを使ってオペレーティングシステムを含むすべてのファイルを復元する方法があります。

概要

UNIXCell Managerの障害復旧を手動で実行する手順の概要は、以下のとおりです。

1. **フェーズ0**
   a. フルクライアントバックアップおよびIDBバックアップを実行します。
   b. 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。
2. **フェーズ1:**
   a. 障害が発生したハードウェアを交換します。
   b. 手動でディスク上にパーティションを再作成し、記憶データ構造を再確立します。

c. オペレーティングシステムを再インストールします。
d. パッチを再インストールします。

3. **フェーズ2**
   a. Data Protector Cell Managerを再インストールします。
   b. その他のファイルをメディアから復元する作業を簡単にするため、IDBの最新のバックアップを復元します。
   c. Data Protector構成情報(/etc/opt/omni)をバックアップに含まれている最新のData Protector構成情報で置き換え、以前の構成を再作成します。
4. **フェーズ3**
   a. Data Protectorの標準復元手順を使用して、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。
   b. システムを再起動します。

制限事項

サポート対象のオペレーティングシステムについては、『*HP Data Protector product announcements 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。

ここでは、クラスター環境の復旧については説明しません。クラスター環境の構成によっては、特別な手順や環境の変更が必要です。

準備

HP-UXまたはSolarisクライアントの手動による障害復旧に対する準備と同じ手順を行います(ただし補助ディスクに関する手順を除く)。詳細は、「準備」(121ページ)を参照してください。上記の手順とは別に、以下の手順も実行することが必要です。

1. IDBの通常バックアップを行います。このとき、別のバックアップ仕様を使って、Cell Manager自体のバックアップ完了後にバックアップが実行されるようスケジュール設定することをお勧めします。
2. Cell Managerシステム上の指定したデバイスにIDBと構成のバックアップを行います。これにより、管理者はそのデバイス内のメディアにIDBの最新バージョンが含まれていることが分かります。

復旧

以下の手順に従って、UNIX Cell Managerを復元します。

前提条件

ディスクデリバリーによる障害復旧を正しく実行するには、以下が必要です。

- Cell ManagerとIDBのルートパーティションの最新の有効なバックアップが含まれているメディア
- Cell Managerシステムに接続されたデバイス

以下の手順に従って、Cell Managerの復旧を実行します。

1. 影響があったディスクを交換します。
2. お使いの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。インストール方法については、お使いのシステムの管理者用マニュアルを参照してください。インストール時に、復旧準備手順(実行前スクリプト)で収集したデータを使って、保管場所の物理的および論理的保存構造、論理ボリューム構造、ファイルシステムとマウントポイント、ネットワーク設定などを再作成して構成します。
4. Cell ManagerにData Protectorを再インストールします。
5. データベースの最新バックアップと/etc/opt/omniを一時ディレクトリに復元します。これにより、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。

> **注記:**
>
> **データベースを直接復元することはできません。手順についてはは、オンラインヘルプを参照してください。この手順には、**`/opt/omni/sbin/omnisv -stop`**コマンドを使用してすべてのData Protectorプロセスを終了する操作が含まれます。これにより、使用中のファイルがない状態になります。**

6. /etc/opt/omniディレクトリを削除して、一時ディレクトリの/etc/opt/omniと置き換えます。これにより、前回の構成が再び作成されます。
7. /opt/omni/sbin/omnisv -startコマンドを使ってData Protectorプロセスを起動します。
8. Data Protectorユーザーインターフェースを起動して、すべての使用ファイルをバックアップから復元します。
9. システムを再起動します。

以上で、Cell Managerが正しく復旧されます。

5 障害復旧のトラブルシューティング

この章の内容

この章では、障害復旧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、ある特定の障害復旧の方法に関連する問題かどうかを検討した後、障害復旧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、「autodr.logファイル」(129ページ)を参照してください。

Data Protectorの一般的なトラブルシューティング情報については、『*HP 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。

作業を開始する前に

- 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ます。オンラインヘルプの索引「パッチ」を参照して、この方法を確認します。
- Data Protector の全般的な制限事項、既知の問題、および回避方法については、『*HP Data Protector product announcements 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。
- サポートされているバージョン、プラットフォーム、およびその他の情報の最新リストについては、http://www.hp.com/support/manualsを参照してください。

一般的なトラブルシューティング

autodr.logファイル

autodr.logは*Data_Protector_home*¥tmpディレクトリにあるログファイルで、自動障害復旧方法(EADR、OBDR、ASR)に関するメッセージが含まれています。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。そうしたエラーメッセージは通常、トレースバックとともにログファイルの最後に記録されています。

autodr.logに記録されるメッセージには次の4つのタイプ(レベル)がありますが、そのレベルは、バックアップセッションの最後にData Protector GUIに表示されるメッセージの報告レベルとは対応していないことに注意してください。

- 致命的エラー: 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。
- エラー:致命的である可能性もありますが、いくつかの要因に依存します。

  たとえば、autodr.log に、あるドライバが障害復旧オペレーティングシステムに含まれていないことが記録されていたとします。そのドライバがないことで、復旧後のシステムが動作しない場合もありますが、OSのブート後に重要でないサービスが実行されないだけの場合もあります。これは、どのドライバがバックアップされていなかったかに依存します。
- 警告および情報: 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には、次のようなものがあります。

- unsupported location:Data Protectorは、障害復旧オペレーティングシステム(DR OS)に含まれる予定のサービスやドライバに必要なファイルが、*%SystemRoot%*ディレクトリにないことを通知します。

  こうしたドライバは多くの場合、アンチウィルスソフトウェアやリモートコントロールソフトウェア(pcAnywhere など) で使用されます。必要なファイルが不足しているサービスやドライバがブート後に動作しない可能性があるため、このメッセージは重要です。障害復旧が正常終了するか失敗するかは、影響を受けるサービスやドライバに左右されます。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 *%System-Root%*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。

障害復旧セッションのデバッグ

Data Protectorに対して、障害復旧セッションの際にデバッグログを作成し、保存するよう指定できます。このオプションはEADRおよびOBDRでのみ使用可能です。

デバッグを設定するには:

1. 障害復旧ウィザードの[デバッグ]ボタンの左側にあるチェックボックスを選択します。

図 10 障害復旧セッション中のデバッグを有効にします。

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、[Debugs] 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。

注記:

Windows VistaシステムおよびWindows Server 2008システムの場合、%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、一般に32 MB未満に制限されています。RAMディスクの使用量がこの制限値に到達すると、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、障害復旧セッションで大量のデバッグ情報が発生することが予想される場合は、デバッグ情報の保存場所を変更する必要があります。

3. [Debug Options]ウィンドウが表示されます。

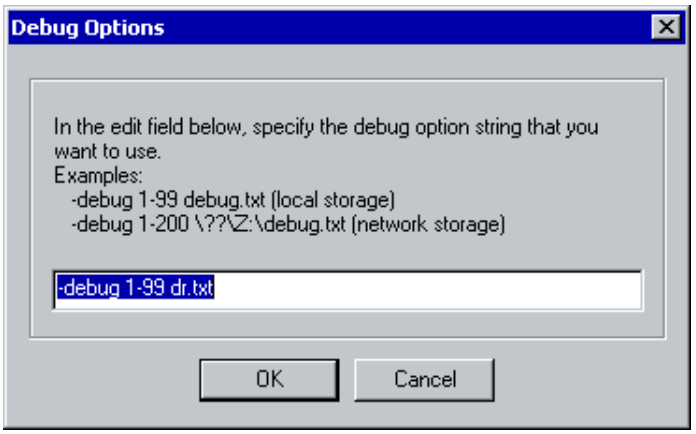


図 11 デバッグログの保存場所の変更

デバッグログを保存する場所を入力します。ドライブ文字の前に¥¥?を付ける必要があります。たとえば、¥¥?¥Z:¥debug.txtのようになります。

デバッグをネットワーク上の共有領域に保存する場合は、net useコマンドを使用して、デバッグログを書き込むネットワーク上の共有領域をドライブ文字にマッピングします。例:

```
NET USE X:¥¥SystemName¥SharedFolderForDebugOutput Password /
USER:Username
```

Windows上での障害復旧中のomnircオプションの設定

omnircオプションに関する一般情報は、『*HP 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上での障害復旧中にomnircオプションを設定する必要がある場合は(ディスクデリバリーによる障害復旧時を除く)、以下の手順を実行してください。

1. [障害復旧ウィザード]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。

図 12 障害復旧ウィザード

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. コマンド

   echo *variable* > %SystemRoot%¥system32¥OB2DR¥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。

   たとえば、次のように入力してください。

   echo OB2RECONNECT_RETRY=1000 > %SystemRoot%¥system32¥OB2DR¥omnirc

   このコマンド例では、障害復旧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変数に値1000秒を設定しています。
4. コマンドプロンプトを閉じ、[障害復旧ウィザード]内の**[次へ]**をクリックして、障害復旧を続行します。

drm.cfgファイル

Data Protector の障害復旧の構成は、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、障害復旧の処理に影響を与えるパラメータが、その影響の説明と一緒に記述されています。drm.cfgファイルはEADRおよびOBDRでのみ使用可能です。

これらの変数を変更するには、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。

   この一時ファイルは、インストールやアップグレードの際にData_Protector_home¥bin¥drim¥config に作成されます。変数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。変数に対して適切な値を設定します。ファイルの指示に従ってください。

全般的な問題

問題

障害復旧終了後のシステムへのログオン時の問題

システム復旧後、以下のエラーメッセージが表示される場合があります。

```
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.
(このドメインにログオンできません。 プライマリドメイ
ン内にシステムのコンピュータアカウントがないか、この
アカウントに対するパスワードが不適切なためです。)
```

この種類のメッセージは、通常以下のいずれかの理由により表示されます。

- 障害復旧プロセス(フルバックアップを含む)を正常に実行するためのすべての情報を収集した後、Windowsを再インストールして、要求を満たしていないドメインにシステムを(再度)追加した。
- 障害復旧プロセス(フルバックアップを含む)を正常に実行するためのすべての情報を収集した後、要求を満たしていないドメインからシステムを削除して、同じドメインまたはその他のドメインにシステムを(再度)追加した。

対策

このような場合、Windows は、障害復旧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。この場合の解決方法を以下に示します。

1. 管理者アカウントを使って、ローカルでシステムにログオンします。
2. [コントロールパネル]ウィンドウで **[ネットワーク]** をクリックし、[識別]タブを使って、このシステムを現在のドメインから一時的なワークグループ(TEMPなど)に移します。この後、システムを削除したドメインにこのシステムを再度追加します。この作業には、ドメイン管理者用パスワードが必要です。

3. コンピュータを再び適切なドメインに入れた後、[ネットワーク]ウィンドウで[OK]をクリックします。この時点でWindowsシステムの再起動が必要となります。
4. 障害復旧プロセスを使ってこの新しい状態を更新するには、もう一度必要な手順(システムデータの収集、バックアップ)をすべて実行することが必要です。詳細は、「障害復旧の準備」の項を参照してください。

問題

コピーからの障害復旧

メディアコピーまたはオブジェクトコピーから障害復旧を実行できない。

Data Protectorはデフォルトで、オリジナルメディアセットを使用して障害復旧を行います。したがって、Data Protector GUIの障害復旧ウィザードにはコピーオブジェクトのバージョンは表示されません。

対策

オリジナルメディアセットが使用できないまたは損傷した場合に、メディアコピーまたはオブジェクトコピーから障害復旧を実行するには、以下の手順を実行します。

- 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の障害復旧ウィザードでは、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。

  詳細は、オンラインヘルプの索引キーワード「メディア, エクスポート」および「システム復旧データ(SRD)の更新と編集」(36ページ)で表示される内容を参照してください。
- 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の障害復旧ウィザードでは、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。

  詳細は、「システム復旧データ(SRD)の更新と編集」(36ページ) を参照してください。

問題

自動障害復旧の各方法(EADR、OBDR、ASR)でデータを収集する際に、構成のバックアップが失敗します。

フルクライアントバックアップを実行しているときは、特定のバックアップ方法に必要なデータの収集中に構成のバックアップが失敗する場合があります。これは、そのバックアップ方法が障害復旧以外に使用されている場合でも発生します。デフォルトでは、Data Protector がすべての自動障害復旧方法のデータを収集するからです。たとえば、ブートディスクがLDMディスクの場合は、Data ProtectorがEADRのデータを収集する際にこれが発生します。

対策

失敗した障害復旧方法でのデータの自動収集を使用不可にします。これにより、Data Protector は必要なデータを他の方法で収集します。

変数OB2_TURNOFF_COLLECTING を以下のいずれかの値に設定します。

0 デフォルト設定、すべての自動方法(EADR, OBDR, ASR)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。ASRデータは収集されます。

2 ASRデータの収集をオフにします。EADR/OBDRデータは収集されます。

3 すべての方法での収集をオフにします。

「Windows上での障害復旧中のomnircオプションの設定」(132ページ) を参照してください。

半自動障害復旧

問題

Drstartレポート: “<filename>をコピーできない”

このエラーは、drstart ユーティリティが指定されたファイルをコピーできなかった場合に出力されます。1つの原因として、ファイルがシステムによってロックされていた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は、おそらくInetサービスがすでに実行中であると思われます。これは通常では考えられない状況で、クリーン インストールの後では起きないはずです。

対策

残りのファイルのコピーを続ける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はロックされたファイルをスキップして他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、障害復旧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]ボタンをクリックしてdrstartユーティリティをクローズすることもできます。

ディスクデリバリーによる障害復旧

問題

Cannot find physical location of drives selected for disk delivery(ディスクのデリバリー用に選択されたドライブの物理的位置が見つかりません。)

ディスクデリバリーによる障害復旧の実行中に、以下のエラーメッセージが返されることがあります。

Cannot find physical location of drives selected for disk delivery (ディスクのデリバリー用に選択されたドライブの物理的位置が見つかりません。)

以前は使用していなかったドライブ文字を選択した場合は、新しいディスク上にパーティションが作成される時点でオブジェクトが復元されます。

障害復旧処理では、オブジェクトを復元する前にディスク情報がチェックされます。このとき内部関数により、ディスクアドミニストレータにより作成されたInformationレジストリ値が読み取られます。ディスクアドミニストレータが複数回開始された場合は、Information値の形式が変更されて、パーサーは失敗します。

対策

HKEY_LOCAL_MACHINE¥SYSTEM¥Diskレジストリ値からInformation値を削除して、ディスクアドミニストレータを再起動します。

問題

オペレーティングシステムが見つからない

ディスクデリバリーによる障害復旧の実行中に、以下のエラーメッセージが返されることがあります。

オペレーティングシステムが見つからない

Windowsシステムの最後のスタートアップ時にエラーが報告され、失敗します。

対策

boot.iniファイルにパーティション情報の位置に関する情報があるかどうかを確認してください。詳細は、「「システム復旧データ(SRD)の更新と編集」(36ページ)」の項の手順4を参照してください。

問題

Media Agent クライアントのディスクデリバリーによる障害復旧

ディスクデリバリーによる障害復旧を実行する場合、Data Protectorはまず、バックアップデバイスが接続されていた元のクライアント(Media Agentクライアント)に接続し、同じデバイスを使って復元を実行しようとします。ただし、バックアップを実行したMedia Agentクライアントがクラッシュし、そのクライアントに対してディスクデリバリーによる障害復旧を実行した場合、Data Protectorはこのクライアントに接続できず、オフラインによる復元を実行して、復元用のローカルデバイスを検索します。ローカルデバイスが接続されていない場合は、その旨と障害復旧の中止を通知するメッセージが表示されます。

対策

これを回避する方法には以下の2通りがあります。

- メディアを別のメディアプールに移動します。これにより、メディアを新しいデバイスに割り当てることができます。その後、ディスクデリバリーによる障害復旧を続行します。
- 2番目の方法では、障害発生前の準備段階の作業が必要です。セル内にMedia Agentクライアントが2つある場合、障害発生前に第一のMedia Agentクライアントを第二のMedia Agentクライアント(およびその逆)にバックアップして、Media Agentクライアントのディスクデリバリーによる障害復旧実行時の問題を回避することができます。

拡張自動障害復旧とワンボタン障害復旧

問題

自動障害復旧情報が収集できない

EADE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。

自動障害復旧情報が収集できません。 システム復旧情報の収集を中止しています

対策

- 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がデバイスを“不明なデバイス” と表示している場合は、EADRまたはOBDRを実行する前に、正しいデバイスドライバをインストールする必要があります。
- 使用可能なレジストリスペースが十分にある必要があります。レジストリの最大サイズを、少なくとも現在のレジストリサイズの2倍に設定することをお勧めします。使用可能なレジストリスペースが十分にない場合、autodr.log に次と同様のエントリが記録されます。

  ```
  ERROR registry 'Exception while saving registry'
  ...
  ```

この問題が継続する場合は、Data Protector自動障害復旧モジュールをアンインストールして(手動およびディスクデリバリーによる障害復旧は可能)、当社サポート担当に連絡してください。

問題

致命的でないエラーが検出された

EADE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。

自動障害復旧データの収集中に重要でないエラーが検出されました。 自動障害復旧ログファイルを確認してください。

自動障害復旧モジュール実行中に致命的でないエラーが検出された場合は、そのバックアップがまだ障害復旧に使用できる可能性が高いことを示します。致命的でないエラーの原因はautodr.logに記録されています(ディレクトリは*Data_Protector_home*¥tmp)。

対策

- *%SystemRoot%*フォルダにないサービスやドライバ(ウィルススキャナなど)が検出されました。autodr.logには、次のようなエラーメッセージが記録されます。

  ERROR safeboot 'unsupported location' 'intercheck support 06' 2 u'¥¥??¥¥D:¥¥Program Files¥¥Sophos SWEEP for NT¥¥icntst06.sys'.

  これは障害復旧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。

問題

復元中にネットワークが使用できなくなった

対策

スイッチ、ケーブルなどに問題がないかどうかを確認します。他に考えられるのは、DNSサーバー(バックアップ時の構成と同じ)が復旧中にオフラインになっていることです。DR OSの構成はバックアップ時と同じであるため、ネットワークが使用できません。この場合はオフライン復元を行い、復旧後にDNSの設定を変更します。またフェーズ2の開始前にレジストリ(HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Tcpip¥Parameters)を変更することもできます。この場合は変更を有効にするために、フェーズ2実行前に再起動が必要です。フェーズ2完了後、フェーズ3を開始する前に設定を修正します。

△ 注意:

レジストリを不適切に編集すると、障害復旧が失敗する原因になります。

問題

自動ログオンが正常動作しない

対策

自動ログオンが正常に動作せず、DRM$ADMIN アカウントを使って手動でログオンしなくてはならない場合があります。

問題

コンピュータが応答しなくなった

対策

CD/テープが読み込み可能か確認します。CD-RW/テープを何回も再使用してはいけません。

問題

Microsoft Cluster ServerのEADR用のCD ISOイメージを作成できない

対策

CD ISOイメージを作成できるようにするためには、クォーラムディスクのバックアップを行う必要があります。

問題

フェーズ1でボリュームが再マウントされない

システムによっては(ディスクコントローラとその構成による)、別のボリュームのマウントポイントに対応づけられたボリューム(ドライブ文字の割り当てなし)が、障害復旧のフェーズ1で正しく再マウントされない場合があります。この現象は、マウントポイントが含まれる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します(たとえば、MiniOSを搭載したシステムボリュームなど)。この結果、オペレーティングシステムが「セーフモード」で起動して、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の検出が行われなくなります。そのため、障害復旧のモジュールでこのボリュームを認識できなくなり、drecovery.iniファイルにMISSINGとして報告されます。このようなボリュームは認識されないだけで、内容は無傷です。

対策

- ドライブ文字を付けてボリュームをマウントし、chkdsk /v /f コマンドを実行して検証するか、システムで復旧が完了するまで待機した後に元のマウントポイントを再作成します。

- システムをMiniOSに直接手動で再起動します(リカバリCDから再起動しないようにします)。以前にアンマウントされたボリュームが、ドライブ文字に対して自動的にマウントされます。

問題

Windows VistaまたはWindows Server 2008システムで、ネットワークドライバがないために、ネットワークが使用できない

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。

対策

見つからないドライバをDR OSイメージに挿入してください。「DR ISOイメージの作成」(63ページ)(EADRの場合)または「OBDRバックアップ」(75ページ)(OBDRの場合)を参照してください。

問題

ISOイメージの作成に失敗して、"Unsupported version of drecovery.ini"のメッセージが表示される

Windows Server 2003またはWindows XPで開始されたGUIからWindows 2000 Serverのクライアントのイメージを作成する際に、旧バージョンのData Protectorクライアントで作成されたバックアップを選択すると以下のエラーが表示されます。

Unsupported version of drecovery.ini file. The drecovery.ini file of your client is created with old version of Disaster Recovery Module and is not supported by the Disaster Recovery Module on this client. Go to the client that has the old version of Disaster Recovery Module and create ISO image for your client there.(サポートされていないバージョンのdrecovery.iniファイルです。お使いのクライアントのdrecovery.iniファイルは古いバージョンの障害復旧モジュールで作成されたので、このクライアントの障害復旧モジュールではサポートされません。古いバージョンの障害復旧モジュールのあるクライアントを使用して、そこからISOイメージを作成してください。)

Data ProtectorのバージョンA.05.50またはA.06.00(パッチDPWIN_00270不使用)からアップグレードしていない場合、障害復旧イメージはWindows 2000システムで開始したGUIからしか作成できません。これは、旧バージョンの障害復旧がWindows 2000システムにしかないためです。アップグレード後は、任意のクライアントのGUIを使用して任意のクライアントのイメージを作成できます。

対策

こののクライアントのISOイメージを作成するには、古いバージョンの障害復旧モジュールのあるクライアントを使用してください。

可能であれば、Windows 2000のクライアントを新バージョンにアップグレードしてください。

Intel Itanium固有の問題

問題

障害復旧の失敗または中断後に、起動記述子がEFIに残る

Intel Itaniumシステムでは、障害復旧セッションの失敗または中断後に起動記述子(DRM Temporary OS)がEFI環境に残ります。これにより、障害復旧プロセスを再起動した場合に、意図しない動作が発生する場合があります。

対策

範囲選択メニューから[Remove Boot Descriptor] オプションを使用して起動記述子を削除します。起動記述子を削除した後に、範囲を選択することによって障害復旧を続行できます。

問題

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

Intel Itaniumシステムで、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全く選択されません)。

対策

1. 範囲選択メニューから[Manual Disk Selection] を選択します。使用可能なディスクのリストが新しいメニューに表示されます。
2. 正しいブートディスクを指定します。oを押すと元のディスクに関する情報が表示され、dを押すと選択したディスクに関する情報が表示されます。
3. カーソルキーを使用してリストからディスクを選択し、bを押します。cを押すと選択が解除されます。

   ブートディスクがシステムディスクと同じでない場合は(通常2つのディスクは同じ)、システムディスクも選択する必要があります。

   [Back] を選択します。
4. 復旧範囲を選択すると、障害復旧が続行されます。

自動システム復旧

問題

ASR中のネットワーク障害

ASR中にはネットワーク障害が原因となって、さまざまな問題が発生する可能性があります。

たとえば、ターゲットシステムに2つのネットワークアダプタがインストールされており、片方が無効化された状態で障害復旧バックアップが実行されたとします。しかし、ASR 中には、すべてのデバイスがデフォルトで有効化されます。ASR中に両方のネットワークアダプタがターゲットシステム上で有効になっていると、ネットワークを正しく構成できないことがあり、その結果、Cell ManagerおよびMedia Agentクライアントへの接続に問題が生じる可能性があります。この場合、Data Protectorはオフライン復旧またはローカル復旧に切り替わり、接続エラーが出力されます。あるいは、ASRが失敗します。

対策

この問題を解決するには、通常のASR復旧手順を実施します。次のメッセージが障害復旧ウィザードに表示されたらF8 を押します。

ネットワーク構成をスキップするには、 この後5秒以内にF8を押します。

これにより、Data ProtectorASRネットワーク構成が、標準のMicrosoft ASRネットワーク構成に戻されます。

問題

ネットワークカードドライバが見つからない場合、ASRが中止される

この問題は、新しいモデルのマシン上でASRを実行している場合に発生します。このようなマシンの場合、WindowsインストールCDには適切なネットワークアダプタのドライバが見つからないためです。ネットワークアダプタが正しくインストールされていないため、omnidr で静的 IPアドレスを使用する設定を試みても、失敗します。

[重要]元のネットワーク(TCP/IP)構成を再作成できませんでした。 ネットワークアダプタが、 正しく取り付けられ動作していることを確認してください。

対策

- 適切なネットワークドライバをインストールしてから、omnidrを起動します。または、可能であれば、必要なネットワークドライバが含まれた最新(後続)バージョンのWindowsインストールCDを使用します。

障害復旧を開始する前にネットワークドライバをインストールするには、[ハードウェアの追加]ウィザードを使用します。このウィザードは以下のコマンドで起動できます。

```
%SystemRoot%¥system32¥rundll32 shell32.dll,Control_RunDLL hdwwiz.cpl
```

- デフォルトのASR (DHCP)のネットワークインストールも使用できます。

  通常のASR手順を行い、障害復旧ウィザードに次のテキストが表示されたら、**F8**を押します。ネットワーク構成をスキップするには、この後5秒以内にF8を押します。

  これにより、Data Protector ASRネットワーク構成が、標準のMicrosoft ASRネットワーク構成に戻されます。

A 詳細情報

抹消リンクの移動(HP-UX 11.x)

リンクを移動するには、バックアップ対象のシステム上で以下の手順を行います。

```
# The system will go from "run-level" 4 to "run-level 1"
# retaining the 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.dKxx") "K...-link" in rc0.d
# Move K430dce K500inetd K660net K900swagentd into ../rc0.d BELOW
#the lowest kill link!!!
echo "may needto 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
```

Windowsでの手動による障害復旧準備用テンプレート

次ページに示すテンプレートは、第3章(41ページ)で説明しているWindowsでの半自動障害復旧に備えてお使いください。

クライアントプロパティ	コンピュータ名	
	ホスト名	
ドライバ		

Windows Service Pack		
TCP/IPのプロパティ	IPアドレス	
	デフォルトゲートウェイ	
	サブネットマスク	
	DNSの順序	
メディアラベル/バーコード番号		
パーティション情報と順序	最初のディスクラベル	
	第1パーティションの長さ	
	第1ドライブの文字	
	第1ファイルシステム	
	2番目のディスクラベル	
	第2パーティションの長さ	
	第2ドライブの文字	
	第2ファイルシステム	
	3番目のディスクラベル	
	第3パーティションの長さ	
	第3ドライブの文字	
	第3ファイルシステム	

用語集

ACSLS

*(StorageTek固有の用語)*Automated Cartridge System Library Serverの略語。ACS(Automated Cartridge System: 自動カートリッジシステム)を管理するソフトウェア。

Active Directory

*(Windows固有の用語)*Windowsネットワークで使用されるディレクトリサービス。ネットワーク上のリソースに関する情報を格納し、ユーザーやアプリケーションからアクセスできるように維持します。このディレクトリサービスでは、サービスが実際に稼動している物理システムの違いに関係なく、リソースに対する名前や説明の付加、検索、アクセス、および管理を一貫した方法で実行できます。

AES 256-ビット暗号化

Data Protector256ビット長のランダムキーを使用するAES-CTR(Advanced Encryption Standard in Counter Mode)暗号化アルゴリズムを基にしたソフトウェア暗号化。暗号化と復号化の両方で同じキーが使用されます。データはネットワークを介して転送される前およびメディアに書き込まれる前に、AES256ビット暗号化機能によって暗号化されます。

AML

*(EMASS/GRAU固有の用語)*Automated Mixed-Media library(自動混合メディアライブラリ)の略。

ASRセット

フロッピーディスク上に保存されたファイルのコレクション。交換用ディスクの適切な再構成(ディスクパーティション化と論理ボリュームの構成)およびフルクライアントバックアップでバックアップされた元のシステム構成とユーザーデータの自動復旧に必要となります。これらのファイルは、バックアップメディア上に保存されると共に、Cell Manager上のASRアーカイブファイルとしてディレクトリData_Protector_program_data¥Config¥Server¥dr¥asr(Windows Server 2008の場合)、Data_Protector_home¥Config¥Server¥dr¥asr(他のWindowsシステム)、または/etc/opt/omni/server/dr/asr/(UNIXシステムの場合)に保存されます。障害発生後、ASRアーカイブファイルは、ASRを実行する必要があるフロッピーディスクに展開されます。

BACKINT

*(SAP R/3固有の用語)*SAP R/3バックアッププログラムが、オープンインタフェースへの呼び出しを通じてData Protector backintインタフェースソフトウェアを呼び出し、Data Protectorソフトウェアと通信できるようにします。バックアップ時および復元時には、SAP R/3プログラムがData Protectorbackintインタフェースを通じてコマンドを発行します。

BC EVA

*(HP StorageWorks EVA固有の用語)*Business Copy EVAは、ローカル複製ソフトウェアソリューションです。EVAファームウェアのスナップショット機能とクローン機能を使用して、ソースボリュームのポイントインタイムコピー(複製)を作成できます。
「複製、ソースボリューム、スナップショット、およびCA+BC EVAも参照。」を参照。

BC VA

*(HP StorageWorks Virtual Array固有の用語)*Business Copy VAの略。BCを使うと、HP StorageWorks Virtual Array LUNの内部コピーを同じ仮想アレイにデータバックアップやデータ複製などの目的で維持できます。コピー(子またはBusiness Copy LUN)は、バックアップやデータ解析、開発などさまざまな目的に使用できます。バックアップ目的で使用されるときは、元(親)のLUNはアプリケーションシステムに接続され、Business Copy(子)LUNはバックアップシステムに接続されます。
「HP StorageWorks Virtual Array LUN、アプリケーションシステム、およびバックアップシステムも参照。」を参照。

BC

*(EMC Symmetrix固有の用語)*Business Continuanceの略。BCは、EMC Symmetrix標準デバイスのインスタントコピーに対するアクセスおよび管理を可能にするプロセスです。
「BCVも参照。」を参照。

BC

*(HP StorageWorks Disk Array XP固有の用語)*Business Copy XPの略。BCを使うと、HP StorageWorks Disk Array XP LDEVの内部コピーをデータバックアップやデータ複製などの目的で維持できます。これらのコピー(セカンダリボリュームまたはS-VOL)は、プライマリボリューム(P-VOL)から分離して、バックアップや開発などの用途に応じた別のシステムに接続することができます。バックアップ目的の場合、P-VOLをアプリケーションシステムに接続し、S-VOL ミラー セットのいずれかをバックアップシステムに接続する必要があります。
「HP StorageWorks Disk Array XP LDEV、CA、Main Control Unit、アプリケーションシステム、およびバックアップシステムも参照。」を参照。

BCV

*(EMC Symmetrix固有の用語)*Business Continuance Volumesの略。BCVデバイスはICDA内であらかじめ構成された専用のSLDです。ビジネスの継続運用を可能にするために使用されます。BCVデバイスには、これらのデバイスによりミラー化されるSLDのアドレスとは異なる、個別のSCSIアドレスが割り当てられます。BCVデバイスは、保護を必要とする一次EMC Symmetrix SLDの分割可能なミラーとして使用されます。
「BCおよびBC Processも参照。」を参照。

BCプロセス

*(EMC Symmetrix固有の用語)*保護されたストレージ環境のソリューション。特別に構成されたEMC Symmetrixデバイスを、EMC Symmetrix標準デバイス上でデータを保護するために、ミラーとして、つまりBusiness Continuance Volumesとして規定します。
「BCVも参照。」を参照。

BRARCHIVE

*(SAP R/3固有の用語)*SAP R/3バックアップツールの1つ。アーカイブREDOログファイルをバックアップできます。BRARCHIVEでは、アーカイブプロセスのすべてのログとプロファイルも保存されます。
「BRBACKUPおよびBRRESTOREも参照。」を参照。

BRBACKUP

*(SAP R/3固有の用語)*SAP R/3バックアップツールの1つ。制御ファイル、個々のデータファイル、またはすべての表領域をオンラインでもオフラインでもバックアップできます。また、必要に応じて、オンラインREDOログファイルをバックアップすることもできます。
「BRARCHIVEおよびBRRESTOREも参照。」を参照。

BRRESTORE

*(SAP R/3固有の用語)*SAP R/3のツール。以下の種類のファイルを復元するために使います。

- BRBACKUPで保存されたデータベースデータファイル、制御ファイル、オンラインREDOログファイル
- BRARCHIVEでアーカイブされたREDOログファイル
- BRBACKUPで保存された非データベースファイル

ファイル、表領域、バックアップ全体、REDOログファイルのログシーケンス番号、またはバックアップのセッションIDを指定することができます。
「BRBACKUPおよびBRARCHIVEも参照。」を参照。

BSM

Data Protector Backup Session Managerの略。バックアップセッションを制御します。このプロセスは、常にCell Managerシステム上で稼動します。

CA

*(HP StorageWorks Disk Array XP固有の用語)*Continuous Access XPの略。CAでは、データ複製、バックアップ、および障害復旧などの目的でHP StorageWorks Disk Array XP LDEVのリモートコピーを作成および維持できます。CAを使用するには、メイン(プライマリ)ディスクアレイとリモート(セカンダリ)ディスクアレイが必要です。オリジナルのデータを格納し、アプリケーションシステムに接続されているCAプライマリボリューム(P-VOL)が、メインディスクアレイに格納されます。リモートディスクアレイには、バックアップシステムに接続されているCAセカンダリボリューム(S-VOL)が格納されます。
「BC *(HP StorageWorks Disk Array XP固有の用語)*、Main Control UnitおよびHP StorageWorks Disk Array XP LDEVも参照。」を参照。

CA+BC EVA

*(HP StorageWorks EVA固有の用語)*Continuous Access (CA) EVAとBusiness Copy (BC) EVAを併用すると、リモートEVA上にソースボリュームのコピー(複製)を作成して保持でき、その後、これらのコピーをそのリモートアレイ上でローカル複製のソースとして使用できます。
「BC EVA、複製、およびソースボリュームも参照。」を参照。

CAP

*(StorageTek固有の用語)*Cartridge Access Portの略。ライブラリのドアパネルに組み込まれたポートです。メディアの出し入れに使用されます。

CDB

カタログデータベース(Catalog Database)の略。CDBは、IDBのうち、バックアップ、復元、オブジェクトコピー、オブジェクト集約、オブジェクト検証、およびメディア管理セッションに関する情報を格納する部分。選択したロギングレベルによっては、ファイル名とファイルバージョンも格納されます。CDBは、常にセルに対してローカルとなります。
「MMDBも参照。」を参照。

CDFファイル

*(UNIX固有の用語)*Context Dependent File(コンテキスト依存ファイル)の略。CDFファイルは、同じパス名でグループ化された複数のファイルからなるファイルです。通常、プロセスのコンテキストに基づいて、これらのファイルのいずれかがシステムによって選択されます。このメカニズムにより、クラスター内のすべてホストから同じパス名を使って、マシンに依存する実行可能ファイル、システムデータ、およびデバイスファイルを正しく動作させることができます。

Cell Manager

セル内のメインシステム。Data Protectorの運用に不可欠なソフトウェアがインストールされ、すべてのバックアップおよび復元作業がここから管理されます。管理タスク用のGUIは、異なるシステムに

インストールできます。各セルにはCell Managerシステムが1つあります。

Change Journal

*(Windows固有の用語)*ローカルNTFSボリューム上のファイルやディレクトリへの変更が発生するたび、それに関するレコードをログに記録するWindowsファイルシステム機能。

Change Log Provider

*(Windows固有の用語)*ファイルシステム上のどのオブジェクトが作成、変更、または削除されたかを判断するために照会できるモジュール。

CMMDB

Data ProtectorのCMMDB(Centralized Media Management Database: メディア集中管理データベース)は、MoMセル内で、複数セルのMMDBをマージすることにより生成されます。この機能を使用することで、MoM環境内の複数のセルの間でハイエンドデバイスやメディアを共有することが可能になります。いずれかのセルからロボティクスを使用して、他のセルに接続されているデバイスを制御することもできます。CMMDBはManager-of-Manager上に置く必要があります。MoMセルとその他のData Protectorセルの間には、できるだけ信頼性の高いネットワーク接続を用意してください。「MoMも参照。」を参照。

CMMDB(Centralized Media Management Database: 集中型メディア管理データベース)。

「CMMDBを参照。」を参照。

COM+登録データベース

*(Windows固有の用語)*COM+登録データベースとWindowsレジストリには、COM+アプリケーションの属性、クラスの属性、およびコンピュータレベルの属性が格納されます。これにより、これらの属性間の整合性を確保でき、これらの属性を共通の方法で操作できます。

Command View (CV) EVA

*(HP StorageWorks EVA固有の用語)*HP StorageWorksEVAストレージシステムを構成、管理、モニターするためのユーザーインタフェース。さまざまなストレージ管理作業を行うために使用されます。たとえば、仮想ディスクファミリの作成、ストレージシステムハードウェアの管理、仮想ディスクのスナップクローンやスナップショットの作成などに使用されます。Command View EVAソフトウェアはHP Storageマネジメントアプライアンス上で動作し、Webブラウザからアクセスできます。
「HP StorageWorks EVA SMI-S AgentおよびHP StorageWorks SMI-S EVAプロバイダも参照。」を参照。

Command View VLS	*(VLS固有の用語)*LAN経由でVLSを構成、管理、モニターするのに使用するWebブラウザベースのGUI。 「仮想ライブラリシステム(VLS)」を参照。
CRS	Data Protector Cell Manager上で実行され、バックアップと復元セッションを開始、制御する、Cell Request Serverのプロセス(サービス)。このサービスは、Data ProtectorがCell Manager上にインストールされるとすぐに開始されます。Windowsシステムでは、CRSはインストール時に使用したユーザーアカウントで実行されます。UNIXシステムでは、CRSはアカウントルートで実行されます。
CSM	Data Protectorコピーおよび集約セッションマネージャ(Copy and Consolidation Session Manager)の略。このプロセスは、オブジェクトコピーセッションとオブジェクト集約セッションを制御し、Cell Managerシステム上で動作します。
Data Replication(DR)グループ	*(HP StorageWorks EVA固有の用語)*EVA仮想ディスクの論理グループ。共通の性質を持ち、同じCA EVAログを共有していれば、最大8組のコピー セットを含めることができます。 「コピーセットも参照。」を参照。
Data_Protector_home	Windows VistaおよびWindows Server 2008では、Data Protectorのプログラムファイルを含むディレクトリ。その他のWindowsオペレーティングシステムでは、Data Protectorのプログラムファイルとデータファイルを含むディレクトリ。デフォルトのパスは、%ProgramFiles%¥OmniBackですが、パスはインストール時にData Protectorセットアップウィザードで変更できます。 「Data_Protector_program_data.」を参照。
Data_Protector_program_data	Windows VistaおよびWindows Server 2008では、Data Protectorのデータファイルを含むディレクトリ。デフォルトのパスは、%ProgramData%¥OmniBackですが、パスはインストール時にData Protectorセットアップウィザードで変更できます。 「Data_Protector_home.」を参照。
Dbobject	*(Informix Server固有の用語)*Informix Server物理データベースオブジェクト。blobspace、dbspace、または論理ログファイルなどがそれにあたります。
DCBF	DCBF(Detail Catalog Binary Files: 詳細カタログバイナリファイル)ディレクトリは、IDBの一部です。IDBの約80%を占めるファイルバージョンと属性に関する情報を格納します。バックアップに使用されるData Protectorメディアごとに1つのDCバイナリファイルが作成さ

れます。サイズの最大値は、ファイルシステムの設定による制限を受けます。

DCディレクトリ

詳細カタログ(DC)ディレクトリには、詳細カタログバイナリファイル(DCBF)が含まれており、そのファイルの中にはファイルバージョンについての情報が保管されています。これは、IDBのDCBF部分を表し、IDB全体の約80%の容量を占めます。デフォルトのDCディレクトリはdcbfと呼ばれ、Data_Protector_program_data¥db40ディレクトリ(Windows Server 2008の場合)、Data_Protector_home¥db40ディレクトリ(その他のWindowsシステムの場合)、または/var/opt/omni/server/db40ディレクトリ(UNIXシステム)のCell Managerに置かれます。他のDCディレクトリを作成し、独自に指定した場所を使用することができます。1つのセルでサポートされるDCディレクトリは50個までです。DCディレクトリのデフォルト最大サイズは16GBです。

DHCPサーバー

Dynamic Host Configuration Protocol(DHCP)を通じて、DHCPクライアントにIPアドレスの動的割り当て機能とネットワークの動的構成機能を提供するシステム。

Disk Agent

クライアントのバックアップと復元を実行するためにクライアントシステム上にインストールする必要があるコンポーネントの1つ。Disk Agentは、ディスクに対するデータの読み書きを制御します。バックアップ セッション中には、Disk Agentがディスクからデータを読み取って、Media Agentに送信してデータをデバイスに移動させます。復元セッション中には、Disk AgentがMedia Agentからデータを受信して、ディスクに書き込みます。オブジェクト検証セッション中に、Disk AgentはMedia Agentからデータを取得し、確認処理を実行しますが、データはディスクには書き込まれません。

Disk Agentの同時処理数

1つのMedia Agentに対して同時にデータを送信できるDisk Agentの数。

DMZ

DMZ (Demilitarized Zone)は、企業のプライベートネットワーク(イントラネット)と外部のパブリックネットワーク(インターネット)の間に「中立地帯」として挿入されたネットワークです。DMZにより、外部のユーザーが企業のイントラネット内のサーバーに直接アクセスすることを防ぐことができます。

DNSサーバー

DNSクライアントサーバーモデルでは、DNSサーバーにインターネット全体で名前解決を行うのに必要なDNSデータベースに含まれている情報の一部を保持します。DNSサーバーは、このデータベースを使用して名前解決を要求するクライアントに対してコンピュータ名を提供します。

DR OS

障害復旧を実行するオペレーティングシステム環境。Data Protectorに対して基本的な実行時環境(ディスク、ネットワーク、テープ、およびファイルシステムへのアクセス)を提供します。Data Protector障害復旧を実行する前に、DR OSをディスクにインストールするかメモリにロードして、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、他のオペレーティングシステムの復元用ホスト環境として排他的に使用されます。このホスト環境には、ターゲットとなるオペレーティングシステムの構成データも置かれます。ターゲットシステムを元の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障害復旧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。

DRイメージ

一時障害復旧オペレーティングシステム(DR OS)のインストールおよび構成に必要なデータ。

EMC Symmetrix Agent (SYMA) *(EMC Symmetrix固有の用語)*

「Symmetrix Agent (SYMA)」を参照。

Exchange Replication Service

*(Microsoft Exchange Server固有の用語)*ローカル連続レプリケーション(LCR)か、クラスター連続レプリケーション(CCR)テクノロジのいずれかを使用して複製されたストレージグループを表すMicrosoft Exchange Serverのサービス。
「クラスター連続レプリケーションおよびローカル連続レプリケーション.」を参照。

FCブリッジ

「Fibre Channelブリッジ」を参照。

Fibre Channel

Fibre Channelは、高速のコンピュータ相互接続に関するANSI標準です。光ケーブルまたは銅線ケーブルを使って、大容量データファイルを高速で双方向送信でき、数km離れたサイト間を接続できます。ファイバチャンネルは、ノード間を3種類の物理トポロジー(ポイントトゥポイント、ループ、スイッチ式)で接続できます。

Fibre Channelブリッジ

Fibre Channelブリッジ(マルチプレクサ)は、RAIDアレイ、ソリッドステートディスク(SSD)、テープライブラリなどの既存のパラレルSCSIデバイスをファイバーチャネル環境に移行できるようにします。ブリッジ(マルチプレクサ)の片側にはFibre Channelインタフェースがあり、その反対側にはパラレルSCSIポートがあります。このブリッジ(マルチプレクサ)を通じて、SCSIパケットをFibre Channelとパラレル SCSIデバイスの間で移動することができます。

fnames.dat	IDBのfnames. datファイルには、バックアップしたファイルの名前に関する情報が格納されます。一般に、ファイル名が保存されている場合、それらのファイルはIDBの20%を占めます。
GUI	Data Protectorには、構成、管理、および操作に関するあらゆるタスクに簡単にアクセスできる、グラフィカルユーザーインタフェースが用意されています。Windows用のオリジナルのData Protector GUIの他に、Data Protectorには、さまざまなプラットフォームで実行できる、外観も操作も変わらないJavaベースのGUIも用意されています。
Holidaysファイル	休日に関する情報を格納するファイル。このファイルは、Data_Protector_program_data¥Config¥Server¥holidaysディレクトリ(Windows Server 2008の場合)、Data_Protector_home¥Config¥Server¥holidaysディレクトリ(その他のWindowsシステムの場合)、または/etc/opt/omni/server/Holidaysディレクトリ(UNIXシステムの場合)のCell ManagerのHolidaysファイルを編集することで、各種の休日を設定できます。
HP Operations Manager SMART Plug-In (SPI)	ドメイン監視機能を強化する完全に統合されたソリューションで、HP Operations Managerに追加するだけですぐに使えます。HP Operations Manager SMART Plug-Inとして実装されるData Protector用統合ソフトウェアを使用して、ユーザーはHP Operations Managerの拡張機能として任意の数のData Protector Cell Managerを監視できます。
HP Operations Manager	ネットワーク内の多数のシステムとアプリケーションの運用管理を強力な機能でサポートするHP Operations Manager。Data Protectorには、この管理製品を使用するための統合ソフトウェアが用意されています。この統合ソフトウェアは、Windows、HP-UX、SolarisおよびLinux上のHP Operations Manager管理サーバー用のSMART Plug-Inとして実装されています。以前のバージョンのHP Operations Managerは、IT/Operation、Operations Center、およびVantage Point Operations、OpenView Operationsと呼ばれていました。
HP StorageWorks Disk Array XP LDEV	HP StorageWorks Disk Array XPの物理ディスクの論理パーティション。LDEVは、Continuous Access XP (CA)構成およびBusiness Copy XP (BC)構成で複製することができるエンティティで、スタンドアロンのエンティティとしても使用できます。 「BC、CA (*HP StorageWorks Disk Array XP固有の用語*)、および複製も参照。」を参照。
HP StorageWorks EVA SMI-S Agent	Data Protectorのソフトウェアモジュール。HP StorageWorks Enterprise Virtual Array用統合ソフトウェアに必要なタスクをすべ

て実行します。EVA SMI-S Agentを使用すると、受信した要求とCV EVA間のやり取りを制御するHP StorageWorks SMI-S EVAプロバイダを通じてアレイを制御できます。
「Command View (CV) EVAおよびHP StorageWorks SMI-S EVAプロバイダも参照。」を参照。

HP StorageWorks SMI-S EVAプロバイダ

HP StorageWorks Enterprise Virtual Arrayを制御するために使用されるインタフェース。SMI-S EVAプロバイダはHPストレージマネジメントアプライアンスシステム上で個別のサービスとして動作し、受信した要求とCommand View EVA間のゲートウェイとして機能します。Data Protector HP StorageWorks EVA用統合ソフトウェアでは、SMI-S EVAプロバイダはEVA SMI-S Agentから標準化された要求を受け入れ、Command View EVAとやり取りして情報または方法を呼び出し、標準化された応答を返します。
「HP StorageWorks EVA SMI-S AgentおよびCommand View (CV) EVAも参照。」を参照。

HP StorageWorks Virtual Array LUN

HP StorageWorks Virtual Array内の物理ディスクの論理パーティション。LUNはHP StorageWorks Business Copy VA 構成で複製することができるエンティティで、スタンドアロンのエンティティとしても使用できます。
「 BC VAおよび複製も参照。」を参照。

IAPへのバックアップ

HP Integrated Archiving Platform(IAP)アプライアンスへのData Protectorベースのバックアップ。データチャンクごとに固有のコンテンツアドレスを作成して、保存データの冗長性をブロック(またはチャンク)レベルで排除するというIAP機能を活用します。変更されたチャンクのみがネットワーク上を転送され、ストアに追加されます。

ICDA

*(EMC Symmetrix固有の用語)*EMCのSymmetrixの統合キャッシュディスクアレイ(ICDA)は、複数の物理ディスク、複数のFWD SCSIチャンネル、内部キャッシュメモリ、およびマイクロコードと呼ばれる制御/診断ソフトウェアを備えたディスクアレイデバイスです。

IDB

Data Protector内部データベースは、Cell Manager上に保持される埋込み型データベースです。どのデータがバックアップされるか、どのメディアにバックアップされるか、バックアップセッションと復元セッションがどのように実行されるかどのデバイスやライブラリに構成されているかについての情報が格納されます。

IDB回復ファイル

IDBバックアップおよびバックアップ用のメディアとデバイスに関する情報を格納するIDBファイル(obrindex.dat)です。この情報により、IDBの復旧を大幅に簡素化できます。IDBトランザクションログと共

にこのファイルを他のIDBディレクトリとは別の物理ディスクに移動し、さらにこのファイルのコピーを作成することをお勧めします。

Inet

Data Protectorセル内の各UNIXシステムで動作するプロセスまたはWindowsシステム上で動作するサービス。このプロセスは、セル内のシステム間の通信と、バックアップおよび復元に必要なその他のプロセスの起動を受け持ちます。システムにData Protectorをインストールすると、Inetサービスが即座に起動されます。Inetプロセスは、inetdデーモンにより開始されます。

Information Store

*(Microsoft Exchange Server固有の用語)*ストレージ管理を行うMicrosoft Exchange Serverのサービス。Microsoft Exchange Serverのインフォメーションストアでは、メールボックスストアとパブリックフォルダストアの2種類のストアが管理されます。メールボックスストアは、個々のユーザーに属するメールボックスから成ります。パブリックフォルダストアには、複数のユーザーで共有するパブリックフォルダおよびメッセージがあります。
「キーマネージメントサービスおよびサイト複製サービス」を参照。

Informix Server

*(Informix Server固有の用語)*Informix Dynamic Serverのことです。

Informix Server用のCMDスクリプト

*(Informix Server固有の用語)*Informix Serverデータベースの構成時にINFORMIXDIR内に作成されるWindows CMDスクリプト。環境変数をInformix Serverにエクスポートするコマンド一式が含まれています。

Installation Server

特定のアーキテクチャ用のData Protectorソフトウェアパッケージのレポジトリを保持するコンピュータシステム。Installation ServerからData Protectorクライアントのリモートインストールが行われます。混在環境では、少なくとも2台のInstallation Serverが必要です。1台はUNIXシステム用で、1台はWindowsシステム用です。

Internet Information Services (IIS)

*(Windows固有の用語)*Microsoft Internet Information Servicesは、ネットワーク用ファイル/アプリケーションサーバーで、複数のプロトコルをサポートしています。IISでは、主に、HTTP(Hypertext Transport Protocol)によりHTML(Hypertext Markup Language)ページとして情報が転送されます。

IPアドレス

IP (インターネットプロトコル)アドレスは、ネットワーク上のシステムを一意に識別するアドレスで、数字で表されます。IPアドレスは、ピリオド(ドット)で区切られた4組の数字からなります。

ISQL

*(Sybase固有の用語)*Sybaseのユーティリティの1つ。Sybase SQL Serverに対してシステム管理作業を実行できます。

Java GUIクライアント

Java GUIクライアントはJava GUIコンポーネントの1つで、UI関連のインタフェースのみで構成されており、機能するためにはJava GUIサーバーとの通信が必要です。

Java GUIサーバー

Java GUIコンポーネントの1つ。Data Protector Cell Managerシステムにインストールされています。Java GUIサーバーは、Java GUIクライアントからの要求を受け取って処理し、応答をJava GUIクライアントに戻します。通信は、ポート5556でHypertext Transfer Protocol (HTTP)を通して行われます。

Key Management Service

*(Microsoft Exchange Server固有の用語)*拡張セキュリティのための暗号化機能を提供するMicrosoft Exchange Serverのサービス。
「インフォメーションストアおよびサイト複製サービスも参照。」を参照。

KMS

キー管理サーバー(KMS)はData Protectorの暗号化機能のためのキー管理を提供する、Cell Managerで実行する集中サービス。このサービスは、Data ProtectorがCell Manager上にインストールされるとすぐに開始されます。

LBO

*(EMC Symmetrix固有の用語)*Logical Backup Object(論理バックアップオブジェクト)の略。LBOは、EMC Symmetrix/Fastrax環境内で保存/取得されるデータオブジェクトです。LBOはEMC Symmetrixによって1つのエンティティとして保存/取得され、部分的には復元できません。

LISTENER.ORA

*(Oracle固有の用語)*Oracleの構成ファイルの1つ。サーバー上の1つまたは複数のTNSリスナを定義します。

log_fullシェルスクリプト

*(Informix Server UNIX固有の用語)*ON-Barに用意されているスクリプトの1つで、Informix Serverでlogfullイベント警告が発行された際に、論理ログファイルのバックアップを開始するために使用できます。Informix ServerのALARMPROGRAM構成パラメータは、デフォルトで、INFORMIXDIR/etc/log_full.shに設定されます。ここで、INFORMIXDIRは、Informix Serverホームディレクトリです。論理ログファイルを継続的にバックアップしたくない場合は、ALARMPROGRAM構成パラメータをINFORMIXDIR/etc/no_log.shに設定してください。

Lotus C API

*(Lotus Domino Server固有の用語)*Lotus Domino ServerとData Protectorなどのバックアップソリューションの間でバックアップ情報および復元情報を交換するためのインタフェース。

LVM

LVM (Logical Volume Manager: 論理ボリュームマネージャ)は、HP-UXシステム上で物理ディスクスペースを構造化し、論理ボリュームにマッピングするためのサブシステムです。LVMシステムは、複数のボリュームグループで構成されます。各ボリュームグループには、複数のボリュームが含まれます。

Main Control Unit (MCU)

*(HP StorageWorks Disk Array XP固有の用語)*CAとBC構成用のプライマリボリュームを含み、マスターデバイスとしての役割を果たすHP StorageWorks XPディスクアレイ。
「BC (HP StorageWorks Disk Array XP固有の用語)、CA*(HP StorageWorks Disk Array XP固有の用語)*およびHP StorageWorks Disk Array XP LDEVも参照。」を参照。

make_net_ recovery

make_net_recoveryは、Ignite-UXのコマンドの1つ。Ignite-UXサーバーまたはその他の指定システム上にネットワーク経由で復旧アーカイブを作成できます。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ブートするか、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ブートは、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。

make_tape_ recovery

make_tape_recoveryは、Ignite-UXのコマンドの1つ。システムに応じてカスタマイズしたブート可能テープ(インストールテープ)を作成できます。ターゲットシステムにバックアップデバイスを直接接続し、ブート可能な復旧テープからターゲットシステムをブートすることにより、無人障害復旧を実行できます。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。

Manager-of-Managers (MoM)

「MoM」を参照。

MAPI

*(Microsoft Exchange Server固有の用語)*MAPI (Messaging Application Programming Interface)は、アプリケーションおよびメッセージングクライアントがメッセージングシステムおよび情報システムと対話するためのプログラミングインタフェースです。

MCU

「Main Control Unit (MCU)」を参照。

Media Agent	デバイスに対する読み込み/書き込みを制御するプロセス。制御対象のデバイスはテープなどのメディアに対して読み込み/書き込みを行います。復元またはオブジェクト検証セッション中、Media Agentはバックアップ メディア上のデータを探して、処理するためにDisk Agentに送信します。復元セッションの場合、続いてDisk Agentはデータをディスクに書き込みます。Media Agentは、ライブラリのロボティクス制御も管理します。
Microsoft Exchange Server	多様な通信システムへの透過的接続を提供するクライアント/サーバー型のメッセージング/ワークグループシステム。電子メールシステムの他、個人とグループのスケジュール、オンラインフォーム、ワークフロー自動化ツールなどをユーザーに提供します。また、開発者に対しては、情報共有およびメッセージング サービス用のカスタムアプリケーション開発プラットフォームを提供します。
Microsoft SQL Server	分散型「クライアント/サーバー」コンピューティングのニーズを満たすように設計されたデータベース管理システム。
Microsoft Volume Shadow Copy Service (VSS)	VSS対応アプリケーションのバックアップと復元をそのアプリケーションの機能に関係なく統合管理する統一通信インタフェースを提供するソフトウェアサービスです。このサービスは、バックアップアプリケーション、ライター、シャドウコピープロバイダ、およびオペレーティングシステムカーネルと連携して、ボリュームシャドウコピーおよびシャドウコピーセットの管理を実現します。 「シャドウコピー、シャドウコピープロバイダ、複製およびライターも参照。」を参照。
Microsoft管理コンソール(MMC)	*(Windows固有の用語)*Windows環境における管理モデル。シンプルで一貫した統合型管理ユーザーインタフェースを提供します。同じGUIを通じて、さまざまなMMC対応アプリケーションを管理できます。
MMD	Media Management Daemon (メディア管理デーモン)の略。MMDプロセス(サービス)は、Data Protector Cell Manager上で稼動し、メディア管理操作およびデバイス操作を制御します。このプロセスは、Data ProtectorをCell Managerにインストールしたときに開始されます。
MMDB	Media Management Database(メディア管理データベース)の略。MMDBは、IDBの一部です。セル内で構成されているメディア、メディアプール、デバイス、ライブラリ、ライブラリドライブ、スロットに関する情報と、バックアップに使用されているData Protectorメディ

アに関する情報を格納します。エンタープライズバックアップ環境では、データベースをすべてのセル間で共有できます。
「CMMDB、CDBも参照。」を参照。

MoM

複数のセルをグループ化して、1つのセルから集中管理することができます。集中管理用セルの管理システムが、MoM(Manager-of-Managers)です。他のセルはMoMクライアントと呼ばれます。MoMを介して、複数のセルを一元的に構成および管理することができます。

mount request

デバイスに特定のメディアを挿入するように促す画面プロンプト。必要なメディアを挿入して確認することでマウント要求に応答すると、セッションが続行されます。

MSM

Data Protector Media Session Manager(メディアセッションマネージャ)の略。MSMは、Cell Manager上で稼動し、メディアセッション(メディアのコピーなど)を制御します。

MU番号

*(HP StorageWorks Disk Array XP固有の用語)*ミラーユニット番号。ファーストレベルミラーを示すために使う整数(0、1または2)です。
「ファーストレベルミラーも参照。」を参照。

obdrindex.dat

「IDB復旧ファイル」を参照。

OBDR対応デバイス

ブート可能ディスクを装填したCD-ROMドライブをエミュレートできるデバイス。バックアップデバイスとしてだけでなく、障害復旧用のブートデバイスとしても使用可能です。

ON-Bar

*(Informix Server固有の用語)*Informix Serverのためのバックアップと復元のシステム。ON-Barにより、Informix Serverデータのコピーを作成し、後でそのデータを復元することが可能になります。ON-Barのバックアップと復元のシステムには、以下のコンポーネントが含まれます。

- onbarコマンド
- バックアップソリューションとしてのData Protector
- XBSAインタフェース
- ON-Barカタログテーブル。これは、dbobjectをバックアップし、複数のバックアップを通してdbobjectのインスタンスをトラッキングするために使われます。

ONCONFIG

*(Informix Server固有の用語)*アクティブなONCONFIG構成ファイルの名前を指定する環境変数。ONCONFIG環境変数が存在し

ない場合、Informix ServerがINFORMIXDIR¥etc(Windowsの場合)、またはINFORMIXDIR/etc/(UNIXの場合)ディレクトリのONCONFIGファイルにある構成値を使います。

OpenSSH

さまざまな認証方式と暗号化方式を採用することにより、リモートマシンへの安全なアクセスを提供するネットワーク接続ツールのセット。セキュアシェルを使用してリモートインストールを実行する場合、Installation Serverとクライアントにこれをインストールして構成する必要があります。

Oracle Data Guard

*(Oracle固有の用語)*Oracle Data GuardはOracleの主要な障害復旧ソリューションです。プロダクション(一次)データベースのリアルタイムコピーであるスタンバイデータベースを最大9個まで保持することにより、破損、データ障害、人為ミス、および災害からの保護を提供します。プロダクション(一次)データベースに障害が発生すると、フェイルオーバーによりスタンバイデータベースの1つを新しい一次データベースにすることができます。また、プロダクション処理を現在の一次データベースからスタンバイデータベースに迅速に切り替えたり、元に戻したりできるため、保守作業のための計画ダウンタイムを縮小することができます。

ORACLE_SID

*(Oracle固有の用語)*Oracle Serverインスタンスの一意な名前。別のOracle Serverに切り替えるには、目的のORACLE_SIDを指定します。ORACLE_SIDは、TNSNAMES.ORAファイル内の接続記述子のCONNECT DATA部分とLISTENER.ORAファイル内のTNSリスナの定義に含まれています。

Oracleインスタンス

*(Oracle固有の用語)*1つまたは複数のシステムにインストールされた個々のOracleデータベース。1つのコンピュータシステム上で、複数のデータベースインスタンスを同時に稼動させることができます。

Oracleターゲットデータベースへのログイン情報

(OracleおよびSAP R/3固有の用語) ログイン情報の形式は*<user_name>/<password>@<service>*であり、

- *user_name*は、Oracle Serverおよびその他のユーザーに対して公開されるユーザー名です。各ユーザーがOracleターゲットデータベースに接続するには、ユーザー名とパスワードの両方を入力しなければなりません。ここでは、OracleのSYSDBA権限またはSYSOPER権限が付与されているユーザーを指定する必要があります。
- *password*には、Oracleパスワードファイル(orapwd)内に指定したのと同じパスワードを指定しなければなりません。パスワードは、データベースを管理するユーザーの認証に使用されます。

- *service*には、ターゲットデータベースのためのSQL*Netサーバー プロセスの識別に使用される名前を指定します。

P1Sファイル

P1Sファイルには、システムにインストールされているすべてのディスクを拡張自動ディザスタリカバリ(EADR)中にどのようにフォーマットするかに関する情報が格納されます。このファイルはフルバックアップ中に作成され、バックアップメディアとCell Managerに recovery.p1sというファイル名で保存されます。保存場所は、Data_Protector_program_data¥Config¥Se ver¥dr¥p1s ディレクトリ(Windows Server 2008の場合)、Data_Protector_home¥Config¥Server¥dr¥p1sディレクトリ(その他のWindowsシステムの場合)、/etc/opt/omni/server/dr/p1sディレクトリ(UNIXシステムの場合)です。.

RAID Manager XP

*(HP StorageWorks Disk Array XP固有の用語)*RAID Manager XPアプリケーションには、CAおよびBCアプリケーションのステータスをレポートおよび制御するための広範なコマンドリストが用意されています。これらのコマンドは、RAID Managerインスタンスを通じて、StorageWorks Disk Array XP Disk Control Unitと通信します。このインスタンスは、コマンドを一連の低レベルSCSIコマンドに変換します。

RAID

Redundant Array of Independent Disksの略。

RAIDマネージャライブラリ

*(HP StorageWorks Disk Array XP固有の用語)*Solarisシステム上のData Protectorでは、RAID Managerライブラリを内部的に使用して、HP StorageWorks Disk Array XPの構成データ、ステータスデータ、およびパフォーマンスデータにアクセスします。さらに、一連の低レベルSCSIコマンドに変換される関数呼び出しを通じて、HP StorageWorks Disk Array XPの主要な機能にアクセスします。

rawディスクバックアップ

「ディスクイメージバックアップ.」を参照。

RCU

「Remote Control Unit (RCU)」を参照。

RDBMS

Relational Database Management System (リレーショナルデータベース管理システム)の略。

RDF1/RDF2

*(EMC Symmetrix固有の用語)*SRDFデバイスグループの一種。RDFグループにはRDFデバイスだけを割り当てることができます。RDF1グループタイプにはソースデバイス(R1)が格納され、RDF2グループタイプにはターゲットデバイス(R2)が格納されます。

RDS

Raima Database Serverの略。RDSプロセス(サービス)は、Data ProtectorのCell Manager上で稼動し、IDBを管理します。このプロセスは、Data ProtectorをCell Managerにインストールしたときに開始されます。

Recovery Manager (RMAN)

*(Oracle固有の用語)*Oracleコマンド行インタフェース。これにより、Oracle Serverプロセスに接続されているデータベースをバックアップ、復元、および復旧するための指示がOracle Serverプロセスに出されます。RMANでは、バックアップについての情報を格納するために、リカバリカタログまたは制御ファイルのいずれかが使用されます。この情報は、後の復元セッションで使うことができます。

RecoveryInfo

Windows構成ファイルのバックアップ時、Data Protectorは、現在のシステム構成に関する情報(ディスクレイアウト、ボリューム、およびネットワークの構成に関する情報)を収集します。この情報は、障害復旧時に必要になります。

REDOログ

*(Oracle固有の用語)*各Oracleデータベースには、複数のREDOログファイルがあります。データベース用のREDOログファイルのセットをデータベースのREDOログと呼びます。Oracleでは、REDOログを使ってデータに対するすべての変更を記録します。

Remote Control Unit (RCU)

*(HP StorageWorks Disk Array XP固有の用語)*Remote Control Unit (RCU)は、CA構成の中でMCU (Main Contol Unit)のスレーブとしての役割を果たします。双方向の構成の中では、RCUはMCUとしての役割を果たします。

RMAN *(Oracle固有の用語)*

「Recovery Manager」を参照。

RSM

Data Protector Restore Session Managerの略。 復元セッションおよびオブジェクト検証セッションを制御します。このプロセスは、常にCell Managerシステム上で稼動します。

RSM

*(Windows固有の用語)*Removable Storage Managerの略。RSMは、アプリケーション、ロボティクスチェンジャ、およびメディアライブラリの間の通信を効率化するメディア管理サービスを提供します。これにより、複数のアプリケーションがローカルロボティクスメディアライブラリとテープまたはディスクドライブを共有でき、リムーバブルメディアを管理できます。

SIBF

サーバーレス統合バイナリファイル(SIBF)は、IDBのうち、NDMPのrawメタデータが格納される部分です。これらのデータは、NDMPオブジェクトの復元に必要です。

Site Replication Service

*(Microsoft Exchange Server固有の用語)*Exchange Server 5.5ディレクトリサービスをエミュレートすることで、Microsoft Exchange Server 5.5と互換性のあるMicrosoft Exchange Server 2000/2003のサービス。
「インフォメーションストアおよびキーマネージメントサービスも参照。」を参照。

SMB

「スプリットミラーバックアップを参照。」を参照。

SMBF

セッションメッセージバイナリファイル(SMBF)は、IDBのうち、バックアップ、復元、オブジェクトコピー、オブジェクト集約、オブジェクト検証、およびメディア管理のセッション中に生成されたセッションメッセージが格納される部分です。1つのセッションにつき1つのバイナリファイルが作成されます。ファイルは年毎や月毎に分類されます。

sqlhostsファイル

*(Informix Server固有の用語)*Informix Serverの接続情報ファイル(UNIX)またはレジストリ(Windows)。各データベースサーバーの名前の他、ホストコンピュータ上のクライアントが接続できるエイリアスが格納されます。

SRDF

*(EMC Symmetrix固有の用語)*EMC Symmetrix Remote Data Facilityの略。SRDFは、異なる位置にある複数の処理環境の間での効率的なリアルタイムデータ複製を実現するBusiness Continuationプロセスです。同じルートコンピュータ環境内だけではなく、互いに遠距離にある環境も対象となります。

SRDファイル

*(障害復旧固有の用語)*Unicode(UTF-16)形式のテキストファイルで、WindowsシステムのCONFIGURATIONバックアップ中に生成されCell Managerに格納されます。これには、障害発生時にターゲットシステム上のオペレーティングシステムをインストールおよび構成するために必要なシステム情報が含まれています。
「ターゲットシステム」を参照。

SSE Agent

*(HP StorageWorks Disk Array XP固有の用語)*スプリットミラーバックアップの統合に必要なタスクをすべて実行するData Protectorソフトウェアモジュール。RAID Manager XPユーティリティ(HP-UXシステムおよびWindowsシステムの場合)またはRAID Managerライブラリ(Solarisシステムの場合)を使い、HP StorageWorks Disk Array XPの保管システムと通信します。

sst.confファイル

/usr/kernel/drv/sst.confファイルは、マルチドライブライブラリデバイスが接続されているData Protector Sun Solarisクライアントのそれぞれにインストールされていなければならないファイルです。このファイルには、クライアントに接続されている各ライブラリデバイ

スのロボット機構のSCSIアドレスエントリが記述されていなければなりません。

st.confファイル

/kernel/drv/st. conf ファイルは、バックアップデバイスが接続されているData Protector Solarisクライアントのそれぞれにインストールされていなければならないファイルです。このファイルには、クライアントに接続されている各バックアップドライブのデバイス情報とSCSIアドレスが記述されていなければなりません。シングルドライブデバイスについては単一のSCSIエントリが、マルチドライブライブラリデバイスについては複数のSCSIエントリが、それぞれ必要です。

StorageTek ACSライブラリ

*(StorageTek固有の用語)*ACS (Automated Cartridge System)は、1つのライブラリ管理ユニット(LMU)と、このユニットに接続された1～24個のライブラリ記憶域モジュール(LSM)からなるライブラリシステム(サイロ)です。

Sybase Backup Server API

*(Sybase固有の用語)*Sybase SQL ServerとData Protectorなどのバックアップソリューションの間でのバックアップ情報および復旧情報交換用に開発された業界標準インタフェース。

Sybase SQL Server

*(Sybase固有の用語)*Sybaseの「クライアントサーバー」アーキテクチャ内のサーバー。Sybase SQL Serverは、複数のデータベースと複数のユーザーを管理し、ディスク上のデータの実位置を追跡します。さらに、物理データストレージ域に対する論理データ記述のマッピングを維持し、メモリ内のデータキャッシュとプロシージャキャッシュを維持します。

Symmetrix Agent (SYMA)

*(EMC Symmetrix固有の用語)*EMC Symmetrix環境でのバックアップ操作と復元操作を可能にするData Protectorソフトウェアモジュール。

System Backup to Tape

*(Oracle固有の用語)*Oracleがバックアップ要求または復元要求を発行したときに正しいバックアップデバイスをロード、ラベリング、およびアンロードするために必要なアクションを処理するOracleインタフェース。

SysVol

*(Windows固有の用語)*ドメインのパブリックファイルのサーバーコピーを保存する共有ディレクトリで、ドメイン内のすべてのドメインコントローラ間で複製されます。

TimeFinder

*(EMC Symmetrix固有の用語)*単一または複数のEMC Symmetrix論理デバイス(SLD)のインスタントコピーを作成するBusiness Continuationプロセス。インスタントコピーは、BCVと呼ばれる専用

	の事前構成SLD上に作成され、システムに対する別個のプロセスを経由してアクセスできます。
TLU	Tape Library Unit (テープライブラリユニット)の略。
TNSNAMES.ORA	*(OracleおよびSAP R/3固有の用語)*サービス名にマッピングされた接続記述子を格納するネットワーク構成ファイル。このファイルは、1か所で集中的に管理してすべてのクライアントで使用することも、また、ローカルに管理して各クライアントで個別に使用することもできます。
TSANDS.CFGファイル	*(Novell NetWare固有の用語)*バックアップを開始するコンテナの名前を指定するファイル。このファイルはテキストファイルで、TSANDS.NLMがロードされるサーバーのSYS:SYSTEM¥TSAディレクトリにあります。
UIProxy	Java GUI Server(UIProxyサービス)はData Protector Cell Managerで実行されます。Java GUI Serverでは、Java GUI ClientとCell Managerとの間の通信を行います。また、ビジネスロジック操作を実行し、重要な情報のみをクライアントに送信する必要があります。このサービスは、Data ProtectorがCell Manager上にインストールされるとすぐに開始されます。
User Account Control (UAC)	Windows VistaおよびWindows Server 2008のセキュリティコンポーネント。管理者が権限レベルを上げるまで、アプリケーションソフトウェアを標準のユーザー権限に限定します。
VMware管理クライアント	*(VMware用統合ソフトウェア固有の用語)*Data Protectorを使用してVMware Virtual Infrastructureと通信するクライアント。VirtualCenter Serverシステム(VirtualCenter環境)、またはESX Serverシステム(スタンドアロンESX Server環境)のどちらかです。
volser	*(ADICおよびSTK固有の用語)*ボリュームシリアル(VOLume SERial)番号は、メディア上のラベルで、大容量ライブラリ内の物理テープの識別に使用されます。VOLSERは、ADIC/GRAUデバイスおよびStorageTekデバイス固有の命名規則です。
Volume Shadow Copy Service	「Microsoft Volume Shadow Copy Service.」を参照。
VSS	「Microsoft Volume Shadow Copy Service.」を参照。
VSS準拠モード	*(HP StorageWorks Disk Array XP VSSプロバイダ固有の用語)*2つのXP VSSハードウェアプロバイダ操作モードの1つ。XP プ

ロバイダがVSS準拠モードであると、ソースボリューム(P-VOL)とその複製(S-VOL)は、バックアップ後、単純非対状態になります。したがって、ローテーションされる複製数(P-VOL当たりのS-VOL数)に制限はありません。このような構成でのバックアップからの復元は、ディスクの切り替えによってのみ可能となります。「resyncモード、ソースボリューム、プライマリボリューム(P-VOL)、複製、セカンダリボリューム(S-VOL)、および複製セットローテーションも参照。」を参照。

VxFS

Veritas Journal Filesystemの略。

VxVM (Veritas Volume Manager)

Veritas Volume Managerは、Solarisプラットフォーム上でディスクスペースを管理するためのシステムです。VxVMシステムは、論理ディスクグループに編成された1つまたは複数の物理ボリュームの任意のグループからなります。

Wake ONLAN

節電モードで動作しているシステムを同じLAN上の他のシステムからのリモート操作により電源投入するためのサポート。

Webレポート

Data Protectorの機能の1つ。バックアップステータス、オブジェクトコピーステータスおよびオブジェクト集約ステータスとData Protector構成に関するレポートをWebインタフェース経由で表示できます。

Windows CONFIGURATION バックアップ

Data Protectorでは、Windows CONFIGURATION(構成データ)をバックアップできます。Windowsレジストリ、ユーザープロファイル、イベントログ、WINSサーバーデータおよびDHCPサーバーデータ(システム上で構成されている場合)を1回の操作でバックアップできます。

Windowsレジストリ

オペレーティングシステムやインストールされたアプリケーションの構成情報を保存するため、Windowsにより使用される集中化されたデータベース。

WINSサーバー

Windowsネットワークのコンピュータ名をIPアドレスに解決するWindowsインターネットネームサービスソフトウェアを実行しているシステム。Data Protectorでは、WINSサーバーデータをWindowsの構成データの一部としてバックアップできます。

XBSAインタフェース

*(Informix Server固有の用語)*ON-BarとData Protectorの間の相互通信には、X/Open Backup Services Application Programmer's Interface (XBSA)が使用されます。

XCopyエンジン

*(ダイレクトバックアップ固有の用語)*SCSI-3のコピーコマンド。SCSIソースアドレスを持つストレージデバイスからSCSIあて先アドレ

スを持つバックアップデバイスにデータをコピーし、ダイレクトバックアップを可能にします。データは、ソースデバイス(ブロックまたはストリーミング、つまりディスクまたはテープ)からあて先デバイス(ブロックまたはストリーミング)へ、XCopyを介して流れていきます。これにより、データをストレージデバイスから読み込んであて先デバイスに書き込むまでの一連の処理が、制御サーバーをバイパスして行われます。
「ダイレクトバックアップも参照。」を参照。

ZDB

「ゼロダウンタイムバックアップ(ZDB)」を参照。

ZDBデータベース

*(ZDB固有の用語)*ソースボリューム、複製、セキュリティ情報などのZDB関連情報を格納するIDBの一部。ZDBデータベースはZDB、インスタントリカバリ、スプリットミラー復元に使用されます。
「ゼロダウンタイムバックアップ(ZDB)も参照。」を参照。

アーカイブREDOログ

*(Oracle固有の用語)*オフラインREDOログとも呼びます。Oracleデータベースが ARCHIVELOGモードで動作している場合、各オンラインREDOログが最大サイズまで書き込まれると、アーカイブ先にコピーされます。このコピーをアーカイブREDOログと呼びます。各データベースに対してアーカイブREDOログを作成するかどうかを指定するには、以下の2つのモードのいずれかを指定します。

- ARCHIVELOG – 満杯になったオンラインREDOログファイルは、再利用される前にアーカイブされます。そのため、インスタンスやディスクにエラーが発生した場合に、データベースを復旧することができます。「ホット」バックアップを実行できるのは、データベースがこのモードで稼動しているときだけです。
- NOARCHIVELOG – オンラインREDOログファイルは、いっぱいになってもアーカイブされません。

「オンラインREDOログも参照。」を参照。

アーカイブロギング

*(Lotus Domino Server固有の用語)*Lotus Domino Serverのデータベースモードの1つ。トランザクションログファイルがバックアップされて初めて上書きされるモードです。

アクセス権限

「ユーザー権限」を参照。

アプリケーションエージェント

クライアント上でオンラインデータベース統合ソフトウェアを復元およびバックアップするために必要なコンポーネント。
「[Disk Agent]」を参照。

アプリケーションシステム

*(ZDB固有の用語)*このシステム上でアプリケーションやデータベースが実行されます。アプリケーションまたはデータベースデータは、ソースボリューム上に格納されています。
「バックアップシステムおよびソースボリューム」を参照。

暗号化キー

Data Protector暗号化アルゴリズムで使用されるランダムに生成された256ビットの数値。これを使用して、AES 256ビットソフトウェア暗号化またはドライブベースの暗号化が指定されたバックアップ中に情報を暗号化します。これに続く情報の復号化では、同じキーが使用されます。Data Protectorセルの暗号化キーは、Cell Manager上の中央キーストアに保存されます。

暗号化キー KeyID-StoreID

Data Protector Key Management Serverで使用される結合識別子。これを使用して、Data Protectorで使用される暗号化キーを識別および管理します。KeyIDは、キーストア内のキーを識別します。StoreIDは、Cell Manager上のキーストアを識別します。Data Protectorを暗号化機能付きの旧バージョンからアップグレードした場合、同じCell Manager上で使用されるStoreIDが複数存在する可能性があります。

イベントログ

*(Windows固有の用語)サービスの開始または停止、ユーザーのログオンとログオフなど、Windowsがすべてのイベントを記録したファイル。*Data Protectorは、Windowsイベントログを Windows構成バックアップの一部としてバックアップできます。

イベントログ(Data Protectorイベントログ)

イベントログには、Data Protector関連のすべての通知が書き込まれます。デフォルトの送信方法では、すべての通知がイベントログに送信されます。このイベントログにアクセスできるData Protectorユーザーは、Adminユーザーグループに所属しているか、または「レポートと通知」のユーザー権限が付与されているData Protectorユーザーだけです。イベントログ内のイベントは、すべてブラウズしたり削除することができます。

インスタントリカバリ

*(ZDB固有の用語)*ディスクへのZDBセッションまたはディスク+テープへのZDBセッションで作成された複製を使用して、ソースボリュームの内容を複製が作成された時点の状態に復元するプロセスです。これにより、テープからの復元を行う必要がなくなります。関連するアプリケーションやデータベースによってはインスタントリカバリだけで十分な場合もあれば、完全に復旧するためにトランザクションログファイルを適用するなどその他にも手順が必要な場合もあります。
「複製、ゼロダウンタイムバックアップ(ZDB)、ディスクへのZDB、およびディスク/テープへのZDBも参照。」を参照。

上書き

復元中のファイル名競合を解決するモードの1つ。既存のファイルの方が新しくても、すべてのファイルがバックアップから復元されます。
「マージも参照。」を参照。

エクスチェンジャ

SCSIエクスチェンジャとも呼ばれます。
「ライブラリ」を参照。

エンタープライズバックアップ環境

複数のセルをグループ化して、1つのセルから集中管理することができます。エンタープライズバックアップ環境には、複数のData Protectorセル内のすべてのクライアントが含まれます。これらのセルは、Manager of Managers (MoM)のコンセプトにより集中管理用のセルから管理されます。
「MoMも参照。」を参照。

オートチェンジャー

「ライブラリ」を参照。

オートローダ

「ライブラリ」を参照。

オブジェクト

「バックアップオブジェクト」を参照。

オブジェクトID

*(Windows固有の用語)*オブジェクトID(OID)を使用すると、システムのどこにファイルがあるかにかかわらず、NTFS 5ファイルにアクセスできます。Data Protectorでは、ファイルの代替ストリームとしてOIDを扱います。

オブジェクト検証

Data Protectorの観点で見たバックアップオブジェクトのデータ整合性と、それらを必要なあて先に送信するData Protectorの機能を確認するプロセス。このプロセスは、バックアップ、オブジェクトコピー、またはオブジェクト集約セッションによって作成されたオブジェクトバージョンを復元する機能に信頼レベルを付与するために使用できます。

オブジェクト検証セッション

指定のバックアップオブジェクトまたはオブジェクトバージョンのデータ整合性と、指定のホストにそれらを送信するための選択済みData Protectorネットワーク コンポーネントの機能を確認するプロセス。オブジェクト検証セッションは、対話式に実行することも、自動ポストバックアップまたはスケジュール仕様の指定通りに実行することもできます。

オブジェクトコピー

特定のオブジェクトバージョンのコピー。オブジェクトコピーセッション中またはオブジェクトミラーのバックアップセッション中に作成されます。

オブジェクトコピー
選択されたオブジェクトバージョンを特定のメディアセットにコピーするプロセス。1つまたは複数のバックアップセッションから、コピーするオブジェクトバージョンを選択できます。

オブジェクトコピーセッション
バックアップデータの追加コピーを別のメディアセット上に作成するプロセス。オブジェクトコピー セッション中に、選択されたバックアップオブジェクトがソースからターゲットメディアへコピーされます。

オブジェクト集約
1つのフルバックアップと1つ以上の増分バックアップで構成されたバックアップオブジェクトの復元チェーンを、新規に集約されるバージョンのオブジェクトにマージするプロセス。このプロセスは、合成バックアップの一部です。このプロセスの結果、指定のバックアップオブジェクトの合成フルバックアップが出力されます。

オブジェクト集約セッション
フルバックアップと少なくとも1つの増分バックアップで構成されたバックアップオブジェクトの復元チェーンを、新規に集約されるバージョンのオブジェクトにマージするプロセス。

オブジェクトミラー
オブジェクトのミラーリングを使用して作成されるバックアップオブジェクトのコピー。オブジェクトのミラーは、通常、オブジェクトコピーと呼ばれます。

オブジェクトミラーリング
バックアップセッション中に、いくつかのメディアセットに同じデータを書き込むプロセス。Data Protectorを使用すると、1つまたは複数のメディアセットに対し、すべてまたは一部のバックアップオブジェクトをミラーリングすることができます。

オフラインREDOログ
「アーカイブREDOログ」を参照。

オフラインバックアップ
実行中はアプリケーションデータベースがアプリケーションから使用できなくなるバックアップ。

- 単純なバックアップ方法の場合(ZDBではない)、データベースはバックアップ中(数分から数時間)オフライン状態となり、バックアップシステムからは使用できますが、アプリケーションシステムからは使用できません。たとえばテープへのバックアップの場合、テープへのデータストリーミングが終わるまでの間となります。
- ZDBの方法を使うと、データベースはオフライン状態になりますが、所要時間はデータ複製プロセス中のわずか数秒間です。残りのバックアッププロセスでは、データベースは通常の稼動を再開できます。

データベースは、データ複製プロセスの間(数秒間)オフライン状態となります。残りのバックアッププロセスでは、データベースは通常の稼動を再開できます。
「ゼロダウンタイムバックアップ(ZDB)およびオンラインバックアップも参照。」を参照。

オフライン復旧

オフライン復旧は、ネットワーク障害などによりCell Managerにアクセスできない場合に行われます。オフライン復旧では、スタンドアロンデバイスおよびSCSIライブラリデバイスのみが使用可能です。Cell Managerの復旧は、常にオフラインで行われます。

表領域

データベース構造の一部。各データベースは論理的に1つまたは複数の表スペースに分割されます。各表領域には、データファイルまたはrawボリュームが排他的に関連付けられます。

オンラインREDOログ

*(Oracle固有の用語)*まだアーカイブされていないが、インスタンスでデータベースアクティビティを記録するために利用できるか、または満杯になっており、アーカイブまたは再使用されるまで待機しているREDOログ。
「アーカイブREDOログも参照。」を参照。

オンラインバックアップ

データベースアプリケーションを利用可能な状態に維持したまま行われるバックアップ。データベースは、バックアップアプリケーションが元のデータオブジェクトにアクセスする必要がある間、特別なバックアップモードで稼動します。この期間中、データベースは完全に機能しますが、パフォーマンスに多少影響が出たり、ログファイルのサイズが急速に増大したりする場合もあります。

- 単純なバックアップ方法の場合(ZDBではない)、バックアップモードはバックアップ期間全体(数分から数時間)必要となります。たとえばテープへのバックアップの場合、テープへのデータストリーミングが終わるまでの間となります。
- ZDBの方法を使うと、バックアップモードに必要な時間はデータ複製プロセス中のわずか数秒間です。残りのバックアッププロセスでは、データベースは通常の稼動を再開できます。

場合によっては、データベースを整合性を保って復元するために、トランザクションログもバックアップする必要があります。
「ゼロダウンタイムバックアップ(ZDB)およびオフラインバックアップも参照。」を参照。

階層ストレージ管理(HSM)

使用頻度の低いデータを低コストの光磁気プラッタに移動することで、コストの高いハードディスク記憶域を有効利用するための仕組み。移動したデータが必要になった場合は、ハードディスク記憶域

に自動的に戻されます。これにより、ハードディスクからの高速読み取りと光磁気プラッタの低コスト性のバランスが維持されます。

拡張可能ストレージエンジン(ESE)

*(Microsoft Exchange Server固有の用語)*Microsoft Exchange Serverで情報交換用の記憶システムとして使用されているデータベーステクノロジ。

拡張増分バックアップ

従来の増分バックアップでは、前回のバックアップより後に変更されたファイルがバックアップされますが、変更検出機能に限界があります。これに対し、拡張増分バックアップでは、名前が変更されたファイルや移動されたファイルのほか、属性が変更されたファイルについても、信頼性のある検出とバックアップが行われます。

仮想コントローラソフトウェア(VCS)

*(HP StorageWorks EVA固有の用語)*HSVコントローラを介したCommand View EVAとの通信など、記憶システムの処理すべてを管理するファームウェア。
「Command View (CV) EVAも参照。」を参照。

仮想サーバー

仮想マシンとは、ネットワークIP名およびIPアドレスでドメイン内に定義されるクラスター環境を意味します。アドレスはクラスターソフトウェアによりキャッシュされ、仮想サーバーリソースを現在実行しているクラスターノードにマップされます。こうして、特定の仮想サーバーに対するすべての要求が特定のクラスターノードにキャッシュされます。

仮想ディスク

*(HP StorageWorks EVA固有の用語)*HP StorageWorks Enterprise Virtual Arrayストレージプールから割り当てられたストレージのユニット。仮想ディスクは、HP StorageWorks Enterprise Virtual Arrayのスナップショット機能により複製されるエンティティです。
「ソースボリュームおよびターゲットボリュームも参照。」を参照。

仮想テープ

*(VLS固有の用語)*テープに保存された場合と同様にディスクドライブにデータをバックアップするアーカイブ式ストレージテクノロジ。バックアップスピードおよびリカバリスピードの向上、運用コストの削減など仮想テープシステムとしての利点がある。
「仮想ライブラリ システム(VLS)および仮想テープライブラリも参照。」を参照。

仮想テープライブラリ(VTL)

*(VLS固有の用語)*従来のテープベースのストレージ機能を提供する、エミュレートされるテープライブラリ。
「仮想ライブラリシステム(VLS)も参照」を参照。

仮想デバイスインタフェース
*(Microsoft SQL Server固有の用語)*SQL Server のプログラミングインタフェースの1つ。大容量のデータベースを高速でバックアップおよび復元できます。

仮想フルバックアップ
コピーするのではなくポインタを使用してデータが集約される、効率の良い合成バックアップ。配布ファイルメディア形式を使用する1つのファイルライブラリにすべてのバックアップ(フルバックアップ、増分バックアップ、およびその結果である仮想フルバックアップ)が書き込まれる場合に実行されます。

仮想ライブラリシステム (VLS)
1つまたは複数の仮想テープライブラリ(VTL)をホストする、ディスクベースのデータストレージデバイス。

カタログ保護
バックアップデータに関する情報(ファイル名やファイルバージョンなど)をIDBに維持する期間を定義します。
「データ保護」を参照。

監査情報
セル全体に対し、ユーザーが定義した拡張期間にわたって実施された、全バックアップセッションに関するデータ。

監査レポート
監査ログファイルの保存されたデータから作成される、ユーザーが判読可能な形式の監査情報出力。

監査ログ
監査情報が保存されるデータファイル。

キーストア
すべての暗号化キーはCell Managerのキーストアに集中的に格納され、キー管理サーバー(KMS)により管理されます。

キーチェーン
秘密キーを復号化する際、手動でパスフレーズを入力する手間を省くツール。セキュアシェルを使用してリモートインストールを実行する場合、このツールをインストールサーバーにインストールして構成する必要があります。

共有ディスク
あるシステム上に置かれたWindowsのディスクをネットワーク上の他のシステムのユーザーが使用できるように構成したもの。共有ディスクを使用しているシステムは、Data Protector Disk Agentがインストールされていなくてもバックアップ可能です。

緊急ブートファイル
*(Informix Server固有の用語)*Informix Server構成ファイル ixbar.server_id。このファイルは、INFORMIXDIR/etcディレクトリ(Windowsの場合)、またはINFORMIXDIR¥etcディレクトリ(UNIXの場合)に置かれています。INFORMIXDIRはInformix Serverのホームディレクトリ、server_idはSERVERNUM構成パラメータの値です。緊急ブートファイルの各行は、1つのバックアップオブジェクトに対応します。

クライアントバックアップ

Data Protectorクライアントにマウントされているすべてのファイルシステムのバックアップ。
実際にバックアップされる対象は、バックアップ仕様でユーザーが選択したオブジェクトによって決まります。

- クライアントシステム名の横にあるチェックボックスを選択する場合、Client Systemタイプが作成されます。その結果、バックアップ時にData Protectorは選択されたクライアントにマウントされているすべてのボリュームを最初に検出してから、それらをバックアップします。Windowsクライアントの場合、CONFIGURATIONもバックアップされます。
- クライアントシステムにマウントされているすべてのボリュームを別々に選択する場合、Filesystemタイプの個別バックアップオブジェクトがボリュームごとに作成されます。その結果、バックアップ時に、選択されたボリュームのみがバックアップされます。バックアップ仕様が作成された後にクライアントにマウントされた可能性があるボリュームは、バックアップされません。

クライアントまたはクライアントシステム

セル内でData Protectorの機能を使用できるように構成された任意のシステム。

クラスター対応アプリケーション

クラスタアプリケーションプログラミングインタフェースをサポートしているアプリケーション。クラスター対応アプリケーションごとに、クリティカルリソースが宣言されます。これらのリソースには、ディスクボリューム(Microsoft Cluster Serverの場合)、ボリュームグループ(MC/ServiceGuardの場合)、アプリケーションサービス、IP名およびIPアドレスなどがあります。

クラスター連続レプリケーション

*(Microsoft Exchange Server固有の用語)*クラスター連続レプリケーション(CCR)はクラスター管理とフェイルオーバーオプションを使用して、ストレージグループの完全なコピー(CCRコピー)を作成および維持する高可用性ソリューションです。ストレージグループは個別のサーバーに複製されます。CCRはExchangeバックエンドサーバーで発生した単発箇所の障害を取り除きます。CCRコピーが存在するパッシブExchange ServerノードでVSSを使用してバックアップを実行すれば、アクティブノードの負荷が軽減されます。CCRコピーへの切り替えは数秒で完了するため、CCRコピーは障害復旧に使用されます。複製されたストレージグループは、Exchangeライターの新しいインスタンス(Exchange Replication Service)として表示され、元のストレージグループと同様にVSSを使用してバックアップできます。
「Exchange Replication ServiceおよびローカルCCR連続レプリケーションも参照。」を参照。

グループ

*(Microsoft Cluster Server固有の用語)*特定のクラスター対応アプリケーションを実行するために必要なリソース(ディスクボリューム、アプリケーションサービス、IP名およびIPアドレスなど)の集合。

グローバルオプションファイル

Data Protectorをカスタマイズするためのファイル。このファイルでは、Data Protectorのさまざまな設定(特に、タイムアウトや制限)を定義でき、その内容はData Protectorセル全体に適用されます。このファイルは、Data_Protector_program_data¥Config¥Server¥Optionsディレクトリ(Windows Server 2008の場合)、Data_Protector_home¥Config¥Server¥0ptionsディレクトリ(その他のWindowsシステム)、または/etc/opt/omni/server/optionsディレクトリ(HP-UX またはSolaris システムの場合)のCell Managerに置かれています。

検証

指定したメディア上のData Protectorデータが読み取り可能かどうかをチェックする機能。また、CRC(巡回冗長検査)オプションをオンにして実行したバックアップに対しては、各ブロック内の整合性もチェックできます。

合成バックアップ

データに関しては従来のフルバックアップと同じである合成フルバックアップを、生産サーバーやネットワークに負担をかけずに出力するバックアップソリューション。合成フルバックアップは、前回のフルバックアップと任意の数の増分バックアップを使用して作成されます。

合成フルバックアップ

バックアップオブジェクトの復元チェーンが新たな合成フルバージョンのオブジェクトにマージされるオブジェクト集約処理の結果。合成フルバックアップは、復元速度の面では従来のフルバックアップと同じです。

コピーセット

*(HP StorageWorksEVA固有の用語)*ローカルEVA上にあるソースボリュームとリモートEVA上にあるその複製とのペア。
「ソースボリューム、複製、およびCA+BC EVAも参照。」を参照。

コマンドラインインタフェース(CLI)

CLIには、DOSコマンドやUNIXコマンドと同じようにシェルスクリプト内で使用でできるコマンドが用意されています。これらを使用して、Data Protectorの構成、バックアップ、復元、および管理の各タスクを実行することができます。

再解析ポイント

*(Windows固有の用語)*任意のディレクトリまたはファイルに関連付けることができるシステム制御属性。再解析属性の値は、ユーザー制御データをとることができます。このデータの形式は、データを保存したアプリケーションによって認識され、データの解釈用にインストールされており、該当ファイルを処理するファイルシステムフィルタによっても認識されます。ファイルシステムは、再解析ポ

イント付きのファイルを検出すると、そのデータ形式に関連付けられているファイルシステムフィルタを検索します。

再同期モード

*(HP StorageWorks Disk Array XP VSSプロバイダ固有の用語)*2つのXP VSSハードウェアプロバイダ操作モードの1つ。XPプロバイダが再同期モードであると、ソースボリューム(P-VOL)とその複製(S-VOL)は、バックアップ後、中断ミラー関係になります。MU範囲が0-2(つまり、0、1、2)の場合、ローテーションされる最大複製数(P-VOL当たりのS-VOL数)は3となります。このような構成でのバックアップからの復元は、S-VOLをそのP-VOLと再同期することによってのみ可能となります。
「VSS準拠モード, ソースボリューム、プライマリボリューム(P-VOL), 複製、セカンダリボリューム(S-VOL), MU番号、および複製セットローテーションも参照。」を参照。

差分同期(再同期)

*(EMC Symmetrix固有の用語)*BCVまたはSRDF制御操作。BCV制御操作では、差分同期(Incremental Establish)により、BCVデバイスが増分的に同期化され、EMC Symmetrixミラー化メディアとして機能します。EMC Symmetrixデバイスは、事前にペアにしておく必要があります。SRDF制御操作では、差分同期(Incremental Establish)により、ターゲットデバイス(R2)が増分的に同期化され、EMC Symmetrixミラー化メディアとして機能します。EMC Symmetrixデバイスは、事前にペアにしておく必要があります。

差分リストア

*(EMC Symmetrix固有の用語)*BCVまたはSRDF制御操作。BCV制御操作では、差分リストアにより、BCVデバイスがペア内の2番目に利用可能な標準デバイスのミラーとして再割り当てされます。これに対し、標準デバイスの更新時には、オリジナルのペアの分割中にBCVデバイスに書き込まれたデータだけが反映され、分割中に標準デバイスに書き込まれたデータはBCVミラーからのデータで上書きされます。SRDF制御操作では、差分リストアにより、ターゲットデバイス(R2)がペア内の2番目に利用可能なソースデバイス(R1)のミラーとして再割り当てされます。これに対し、ソースデバイス(R1)の更新時には、オリジナルのペアの分割中にターゲットデバイス(R2)に書き込まれたデータだけが反映され、分割中にソースデバイス(R1)に書き込まれたデータはターゲットミラー(R2)からのデータで上書きされます。

システム状態

*(Windows固有の用語)*システム状態データには、レジストリ、COM+クラス登録データベース、システム起動ファイル、および証明書サービスデータベース(証明書サーバーの場合)が含まれます。サーバーがドメインコントローラの場合は、Active DirectoryサービスとSYSVOLディレクトリもシステム状態データに含まれます。サーバーがクラスターサービスを実行している場合、システム状態データにはリソー

スレジストリチェックポイントとクォーラムリソースリカバリ ログが含まれ、最新のクラスターデータ情報が格納されます。

システムデータベース

*(Sybase固有の用語)*Sybase SQL Serverを新規インストールすると、以下の4種類のデータベースが生成されます。

- マスターデータベース(master)
- 一時データベース(tempdb)
- システムプロシージャデータベース(sybsystemprocs)
- モデルデータベース(model)

システム復旧データファイル

「SRDファイル」を参照。

システムボリューム/ディスク/パーティション

オペレーティングシステムファイルが格納されているボリューム/ディスク/パーティション。ただし、Microsoftの用語では、ブートプロセスの開始に必要なファイルが入っているボリューム/ディスク/パーティションをシステムボリューム/システムディスク/システムパーティションと呼んでいます。

事前割当てリスト

メディアプール内のメディアのサブセットをバックアップに使用する順に指定したリスト。

実行後

オブジェクトのバックアップ後、またはセッション全体の完了後にコマンドまたはスクリプトを実行するバックアップオプション。実行後コマンドは、Data Protectorで事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows上で動作する実行可能ファイルまたはバッチファイル、UNIX上で動作するシェルスクリプトなどを使用できます。
「実行前も参照。」を参照。

実行前コマンドおよび実行後コマンド

実行前コマンドおよび実行後コマンドは、バックアップセッションまたは復元セッションの前後に付加的な処理を実行する実行可能ファイルまたはスクリプトです。実行前コマンドおよび実行後コマンドは、Data Protectorで事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows上で動作する実行可能ファイルまたはバッチファイル、UNIX上で動作するシェルスクリプトなどを使用できます。

実行前

オブジェクトのバックアップ前、またはセッション全体の開始前にコマンドまたはスクリプトを実行するバックアップオプション。実行前コマンドおよび実行後コマンドは、Data Protectorで事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows上で動作する実行可能ファイルまたは

バッチファイル、UNIX上で動作するシェルスクリプトなどを使用できます。
「実行後も参照。」を参照。

自動移行

*(VLS固有の用語)*データのバックアップをまずVLSの仮想テープに作成し、それを物理テープ(1つの仮想テープが1つの物理テープをエミュレート)に移行する操作を、中間バックアップアプリケーションを使用せずに実行する機能。
「仮想ライブラリシステム(VLS)と仮想テープも参照。」を参照。

自動ストレージ管理

*(Oracle固有の用語)*自動ストレージ管理は、Oracleデータベースファイルを管理するOracle 10g/11g統合型ファイルシステムおよびボリュームマネージャです。データとディスクの管理の複雑さを解消するとともに、ストライプ化とミラー化によってパフォーマンスの最適化も行います。

シャドウコピー

*(Microsoft VSS固有の用語)*特定の時点におけるオリジナルボリューム(元のボリューム)の複製を表すボリューム。オリジナルボリュームからではなく、シャドウコピーからデータがバックアップされます。オリジナルボリュームはバックアップ処理中も更新が可能ですが、ボリュームのシャドウコピーは同じ内容に維持されます。
「Microsoft Volume Shadow Copy Serviceおよび複製も参照。」を参照。

シャドウコピーセット

*(Microsoft VSS固有の用語)*同じ時点で作成されたシャドウコピーのコレクション。
「シャドウコピーおよび複製セットも参照。」を参照。

シャドウコピープロバイダ

*(Microsoft VSS固有の用語)*ボリュームシャドウコピーの作成と表現を行うエンティティ。プロバイダは、シャドウコピーデータを所有して、シャドウコピーを公開します。プロバイダは、ソフトウェア(システムプロバイダなど)で実装することも、ハードウェア(ローカルディスクやディスクアレイ)で実装することもできます。
「シャドウコピーも参照。」を参照。

ジュークボックス

「ライブラリ」を参照。

ジュークボックスデバイス

光磁気メディアまたはファイルメディアを格納するために使用する、複数のスロットから成るデバイス。ファイルメディアの格納に使用する場合、ジュークボックスデバイスは「ファイルジュークボックスデバイス」と呼ばれます。

集中型ライセンス

Data Protectorでは、複数のセルからなるエンタープライズ環境全体にわたってライセンスの集中管理を構成できます。すべてのData

Protectorライセンスは、エンタープライズCell Managerシステム上にインストールされます。ライセンスは、実際のニーズに応じてエンタープライズCell Managerシステムから特定のセルに割り当てることができます。
「MoMも参照。」を参照。

循環ログ

*(Microsoft Exchange ServerおよびLotus Domino Server固有の用語)*循環ログは、Microsoft Exchange Serverデータベースおよびデータベースモードの1つ。このモードでは、トランザクションログファイルのコンテンツは、対応するデータがデータベースにコミットされると、定期的に上書きされます。循環ログにより、ディスク記憶領域の要件が軽減されます。

障害復旧

クライアントのメインシステムディスクを(フル)バックアップの実行時に近い状態に復元するためのプロセスです。

障害復旧オペレーティングシステム (DR OS)

「DR OS」を参照。

障害復旧の段階0

障害復旧の準備(障害復旧を成功させるための必須条件)。

障害復旧の段階1

DR OSのインストールと構成(以前の記憶領域構造の構築)。

障害復旧の段階2

オペレーティングシステム(環境を定義する各種の構成情報を含む)とData Protectorの復元。

障害復旧の段階3

ユーザーデータとアプリケーションデータの復元。

初期化

メディアをData Protectorで使用できるように初期化するプロセス。メディア上の既存データはすべて消去されます。メディアに関する情報(メディアID、説明、場所)は、IDBおよび該当するメディア(メディアヘッダ)に保存されます。Data Protectorのメディアは、保護の期限が切れるか、またはメディアの保護が解除されるかメディアがリサイクルされるまで、フォーマットされません。

初期化

「フォーマット」を参照。

所有権

バックアップ所有権は、データを参照および復元するユーザーの能力に影響します。各バックアップセッションとその中でバックアップされたすべてのデータはオーナーに割り当てられます。所有者は、対話型バックアップを開始するユーザー、CRSプロセスを実行するときに使用するアカウント、またはバックアップ仕様オプションで所有者として指定されたユーザーです。

ユーザーが既存のバックアップ仕様を修正せずにそのまま起動した場合、そのバックアップセッションは対話型とみなされません。ユーザーがバックアップ仕様を修正して起動すると、以下の条件が成立しない限り、そのユーザーがオーナーになります。

- そのユーザーが[セッションの所有権を切り替え]ユーザー権限を持っている。
- バックアップ仕様内でバックアップセッションオーナーを明示的に定義するには、ユーザー名、グループ名またはドメイン名、およびシステム名を指定します。

UNIXCell Manager上でスケジュールしたバックアップの場合、上記の条件が成立しない限り、root: sysがセッションオーナーになります。
Windows Cell Manager上でスケジューリングしたバックアップの場合は、上記の条件が成立していない限り、インストール時に指定されたユーザーがセッションオーナーになります。

スイッチオーバー　「フェイルオーバー」を参照。

スキャン　デバイス内のメディアを識別する機能。これにより、MMDBを、選択した位置(たとえば、ライブラリ内のスロット)に実際に存在するメディアと同期させることができます。

スキャン　デバイス内のメディアを識別する機能。これにより、MMDBを、選択した位置(たとえば、ライブラリ内のスロット)に実際に存在するメディアと同期させることができます。デバイスに含まれる実際のメディアをスキャンしてチェックすると、第三者がData Protectorを使用せずにメディアを操作(挿入または取り出しなど)していないかどうかなどを確認できます。

スケジューラー　自動バックアップの実行タイミングと頻度を制御する機能。スケジュールを設定することで、バックアップの開始を自動化できます。

スタッカー　メディア記憶用の複数のスロットを備えたデバイス。通常は、1ドライブ構成です。スタッカーは、スタックからシーケンシャルにメディアを選択します。これに対し、ライブラリはレポジトリからメディアをランダムに選択します。

スタンドアロンファイルデバイス　ファイルデバイスとは、ユーザーがデータのバックアップに指定したディレクトリにあるファイルのことです。

ストレージグループ　*(Microsoft Exchange Server固有の用語)*同じログファイルを共有する複数のメールボックスストアとパブリックフォルダストアのコレ

クション。Exchange Serverでは、各ストレージグループを個別のサーバープロセスで管理します。

ストレージボリューム

*(ZDB固有の用語)*ストレージボリュームは、オペレーティングシステムまたはボリューム管理システム、ファイルシステム、他のオブジェクトが存在可能なその他のエンティティに提供可能なオブジェクトを表します(たとえば仮想化機構)。ボリューム管理システム、ファイルシステムはこの記憶域に構築されます。これらは通常、ディスクアレイなどの記憶システム内に作成または存在します。

スナップショット

*(HP StorageWorks VAおよびHP StorageWorks EVA固有の用語)*スナップショット作成技法を使用して作成された複製の形式。使用するアレイ/技法に応じて、特徴の異なるさまざまな種類のスナップショットが使用できます。このような複製は動的で、スナップショットの種類と作成からの経過時間によって、仮想コピーにあるか、ソースボリュームの内容に引き続き依存するか、または独立した正確な複製(クローン)になります。
「複製およびスナップショット作成も参照。」を参照。

スナップショット作成

*(HP StorageWorks VAおよびHP StorageWorks EVA固有の用語)*複製を作成する技法で、ストレージ仮想化技法を使用して、ソースボリュームのコピーが作成されます。複製はある一時点で作成されたものとみなされ、事前構成することなく、即座に使用できます。ただし、通常は複製作成後もコピープロセスはバックグラウンドで継続されます。
「スナップショットも参照。」を参照。

スナップショットのバックアップ(*HP StorageWorks VAおよびHP StorageWorks EVA固有の用語*)

「テープへのZDB、ディスクへのZDB、およびディスク+テープへのZDB」を参照。

スパースファイル

ブロックが空の部分を含むファイル。例として、データの一部または大部分にゼロが含まれるマトリクス、イメージアプリケーションからのファイル、高速データベースなどがあります。スパースファイルの処理を復元中に有効にしておかないと、スパースファイルを復元できなくなる可能性があります。

スプリットミラー

*(EMC SymmetrixおよびHP StorageWorks Disk Array XP固有の用語)*スプリットミラー技法を使用して作成した複製。複製によ

り、ソースボリュームの内容について独立した正確な複製(クローン)が作成されます。
「複製およびスプリットミラーの作成も参照。」を参照。

スプリットミラー作成

*(EMC SymmetrixおよびHP StorageWorks Disk Array XP固有の用語)*事前構成したターゲットボリュームのセット(ミラー)を、ソースボリュームの内容の複製が必要になるまでソースボリュームのセットと同期化し続ける複製技法。その後、同期を停止(ミラーを分割)すると、分割時点でのソースボリュームのスプリットミラー複製はターゲットボリュームに残ります。
「スプリットミラーも参照。」を参照。

スプリットミラーバックアップ*(EMC Symmetrix固有の用語)*

「テープへのZDB」を参照。

スプリットミラーバックアップ*(HP StorageWorks Disk Array XP固有の用語)*

「テープへのZDB、ディスクへのZDBおよびディスク+テープへのZDB」を参照。

スプリットミラー復元

*(EMC SymmetrixおよびHP StorageWorks Disk Array XP固有の用語)*テープへのZDBセッションまたはディスク+テープへのZDBセッションでバックアップされたデータをテープメディアからスプリットミラー複製へ復元し、その後ソースボリュームに同期させるプロセス。この方法では、完全なセッションを復元することも個々のバックアップオブジェクトを復元することも可能です。
「テープへのZDB、ディスク/テープへのZDBおよび複製も参照。」を参照。

スマートコピー

*(VLS固有の用語)*仮想テープから物理テープライブラリへ作成されたバックアップデータのコピー。スマートコピーのプロセスによって、Data Protectorではソースメディアとターゲットメディアを区別できるため、メディア管理が可能になります。
「仮想ライブラリシステム(VLS)」を参照。

スマートコピープール

*(VLS固有の用語)*指定されたソース仮想ライブラリに対してどのコピー先ライブラリスロットをスマートコピーターゲットとして使用できるかどうかを定義するプール。
「仮想ライブラリシステム(VLS)およびスマートコピーも参照。」を参照。

スレッド

*(Microsoft SQL Server固有の用語)*1つのプロセスのみに属する実行可能なエンティティ。プログラムカウンタ、ユーザーモードスタック、カーネルモードスタック、および1式のレジスタ値からなります。同じプロセス内で複数のスレッドを同時に実行できます。

スロット

ライブラリ内の機械的位置。各スロットがDLTテープなどのメディアを1つずつ格納できます。Data Protectorでは、各スロットを番号で参照します。メディアを読み取るときには、ロボット機構がメディアをスロットからドライブに移動します。

制御ファイル

*(OracleおよびSAP R/3固有の用語)*データベースの物理構造を指定するエントリが記述されたOracleデータファイル。復旧に使用するデータベース情報の整合性を確保できます。

セカンダリボリューム(S-VOL)

*(HP StorageWorks Disk Array XP固有の用語)*セカンダリボリューム(S-VOL)は、別のLDEV(P-VOL)のセカンダリなCAミラーまたはBCミラーの役割を果たすXP LDEVです。CAの場合、S-VOLをMetroCluster構成内のフェイルオーバーデバイスとして使うことができます。S-VOLには、P-VOLによって使用されるアドレスとは異なる、個別のSCSIアドレスが割り当てられます。
「プライマリボリューム(P-VOL)およびMain Control Unit (MCU)も参照。」を参照。

セッション

「バックアップセッション、メディア管理セッションおよび復元セッション」を参照。

セッションID

バックアップ、復元、オブジェクトコピー、オブジェクト集約、オブジェクト検証、またはメディア管理セッションの識別子で、セッションを実行した日付と一意の番号から構成されます。

セッションキー

実行前スクリプトおよび実行後スクリプト用の環境変数。Data Protectorプレビューセッションを含めたセッションを一意に識別します。セッションキーはデータベースに記録されず、omnimntomnistat、およびomniabort コマンドのオプション指定に使用されます。

セル

1台のCell Managerに管理されているシステムの集合。セルには、一般に、同じLANに接続されたサイトや組織エンティティ上のシステムが含まれます。集中管理によるバックアップおよび復元のポリシーやタスクの管理が可能です。

ゼロダウンタイムバックアップ(ZDB)

ディスクアレイにより実現したデータ複製技術を用いて、アプリケーションシステムのバックアップ処理の影響を最小限に抑えるバックアップアプローチ。バックアップされるデータの複製がまず作成さ

れます。その後のすべてのバックアップ処理は、元のデータではなく複製データを使って実行し、アプリケーションシステムは通常の処理に復帰します。
「ディスクへのZDB、テープへのZDB、ディスク/テープへのZDB、およびインスタントリカバリも参照。」を参照。

増分1メールボックスバックアップ
増分1メールボックスバックアップでは、前回のフルバックアップ以降にメールボックスに対して行われた変更をすべてバックアップします。

増分ZDB
ファイルシステムZDBからテープへ、またはZDBからディスク+テープへのセッション。前回の保護されたフルバックアップまたは増分バックアップからの変更のみがテープにストリーミングされます。
「フルZDBも参照。」を参照。

増分バックアップ
*(Microsoft Exchange Server固有の用語)*前回のフルバックアップまたは増分バックアップ以降の変更だけをバックアップするMicrosoft Exchange Serverデータのバックアップ。増分バックアップでは、バックアップ対象はトランザクションログだけです。
「バックアップの種類も参照。」を参照。

増分バックアップ
前回のバックアップ以降に変更があったファイルだけを選択するバックアップ。増分バックアップには複数のレベルがあり、復元チェーンの長さを細かく制御できます。
「バックアップの種類も参照。」を参照。

増分メールボックスバックアップ
増分メールボックスバックアップでは、前回の各種バックアップ以降にメールボックスに対して行われた変更をすべてバックアップします。

ソースデバイス(R1)
*(EMC Symmetrix固有の用語)*ターゲットデバイス(R2)とのSRDF操作に参加するEMC Symmetrixデバイス。このデバイスに対するすべての書き込みは、リモートEMC Symmetrixユニット内のターゲットデバイス(R2)にミラー化されます。R1デバイスは、RDF1グループタイプに割り当てる必要があります。
「ターゲットデバイス(R2)も参照。」を参照。

ソースボリューム
*(ZDB固有の用語)*複製されるデータを含むストレージボリューム。

ターゲットシステム
*(障害復旧固有の用語)*コンピュータの障害が発生した後のシステム。ターゲットシステムは、ブート不能な状態になっていることが多く、そのような状態のシステムを元のシステム構成に戻すことが障害復旧の目標となります。クラッシュしたシステムがそのままターゲットシステムになるのではなく、正常に機能していないハードウェ

アをすべて交換することで、クラッシュしたシステムがターゲットシステムになります。

ターゲットデータベース

*(Oracle固有の用語)*RMANでは、バックアップまたは復元対象のデータベースがターゲットデータベースとなります。

ターゲットデバイス(R2)

*(EMC Symmetrix固有の用語)*ソースデバイス(R1)とのSRDF操作に参加するEMC Symmetrixデバイス。リモートEMC Symmetrixユニット内に置かれます。ローカルEMC Symmetrixユニット内でソースデバイス(R1)とペアになり、ミラー化ペアから、すべての書き込みデータを受け取ります。このデバイスは、通常のI/O操作ではユーザーアプリケーションからアクセスされません。R2デバイスは、RDF2グループタイプに割り当てる必要があります。
「ソースデバイス(R1)も参照。」を参照。

ターゲットボリューム

*(ZDB固有の用語)*複製されるデータを含むストレージボリューム。

ターミナルサービス

*(Windows固有の用語)*Windowsのターミナルサービスは、サーバー上で実行されている仮想Windowsデスクトップセッションと Windowsベースのプログラムにクライアントからアクセスできるマルチセッション環境を提供します。

単一インスタンス

*(IAP固有の用語)*オブジェクト全体とチャンクレベルの両方でデータの冗長性を認識する処理。この処理では、データチャンクごとに強力なハッシュを計算し、それを重複データを保存しようとしているのかどうかの判断に必要な固有のコンテンツアドレスとして使用します。
「IAPへのバックアップも参照。」を参照。

チャンク

*(IAP固有の用語)*データをブロック(チャンク)に分割する処理。各チャンクには固有のコンテンツアドレスが割り振られます。このアドレスは、特定のチャンクがIAPアプライアンスにバックアップ済みかどうかを判断するのに使用されます。データの重複が検出された場合(2つのアドレスが一致している、つまりIAPに保存済みの他のデータチャンクとアドレスが同じ)、そのようなデータはバックアップされません。これにより、データの冗長性が排除され、最適なデータ保存が実現されます。
「IAPへのバックアップ」を参照。

チャンネル

*(Oracle固有の用語)*Oracle Recovery Managerリソース割り当て。チャンネルが割り当てられるごとに、新しいOracleプロセスが開始され、そのプロセスを通じてバックアップ、復元、および復旧が行わ

れます。割り当てられるチャンネルの種類によって、使用するメディアの種類が決まります。

- diskタイプ
- sbt_tapeタイプ

OracleがData Protectorと統合されており、指定されたチャンネルの種類がsbt_tapeタイプの場合は、上記のサーバー プロセスがData Protectorに対してバックアップの読み取りとデータファイルの書き込みを試行します。

直接バックアップ

SCSI Extended Copy (Xcopy)コマンドを使用してディスクからテープ(または他の2次ストレージ)へのデータの直接移動を効率化する、SANベースのバックアップソリューション。ダイレクトバックアップは、SAN環境内のシステムへのバックアップI/O負荷を軽減します。ディスクからテープ(または他の2次ストレージ)へのデータの直接移動をSCSI Extended Copy (XCopy)コマンドで効率化します。このコマンドは、ブリッジ、スイッチ、テープライブラリ、ディスクサブシステムなど、インフラストラクチャの各要素でサポートされています。
「XCopyエンジンも参照。」を参照。

ディスク+テープへのZDB

*(ZDB固有の用語)*ゼロダウンタイムバックアップの1つの形式。ディスクへのZDBと同様に、作成された複製が特定の時点でのソースボリュームのバックアップとしてディスクアレイに保持されます。ただし、テープへのZDBと同様、複製データはバックアップメディアにもストリーミングされます。このバックアップ方法を使用した場合、同じセッションでバックアップしたデータは、インスタントリカバリ、Data Protector標準のテープからの復元を使用して復元できます。スプリットミラーアレイではスプリットミラー復元が可能です。
「ゼロダウンタイムバックアップ(ZDB)、ディスクへのZDB、テープへのZDB、インスタントリカバリ、複製、および複製セットローテーションも参照。」を参照。

ディスクイメージ(rawディスク)バックアップ

ディスクイメージのバックアップでは、ファイルがビットマップイメージとしてバックアップされるため、高速バックアップが実現します。ディスクイメージ(rawディスク)バックアップでは、ディスク上のファイルおよびディレクトリの構造はバックアップされませんが、ディスクイメージ構造がバイトレベルで保存されます。ディスクイメージバックアップは、ディスク全体か、またはディスク上の特定のセクションを対象にして実行できます。

ディスククォータ

コンピュータシステム上のすべてのユーザーまたはユーザーのサブセットに対してディスクスペースの消費を管理するためのコンセプト。このコンセプトは、いくつかのオペレーティングシステムプラットフォームで採用されています。

ディスクグループ

*(Veritas Volume Manager固有の用語)*VxVMシステムのデータストレージの基本ユニット。ディスクグループは、1つまたは複数の物理ボリュームから作成できます。同じシステム上に複数のディスクグループを置くことができます。

ディスクステージング

データをいくつかの段階に分けてバックアップする処理。これにより、バックアップと復元のパフォーマンスが向上し、バックアップデータの格納費用が節減され、データの可用性と復元時のアクセス性が向上します。バックアップステージは、最初に1種類のメディア(たとえば、ディスク)にデータをバックアップし、その後データを異なる種類のメディア(たとえば、テープ)にコピーすることから構成されます。

ディスクへのZDB

*(ZDB固有の用語)*ゼロダウンタイムバックアップの1つの形式。作成された複製が、特定の時点でのソースボリュームのバックアップとしてディスクアレイに保持されます。同じバックアップ仕様を使って別の時点で作成された複数の複製を、複製セットに保持することができます。テープにZDBした複製はインスタントリカバリプロセスで復元できます。
「ゼロダウンタイムバックアップ(ZDB)、テープへのZDB、ディスク/テープへのZDB、インスタントリカバリ、および複製セットローテーションも参照。」を参照。

ディファレンシャルデータベースバックアップ

前回のフルデータベースバックアップ以降にデータベースに対して加えられた変更だけを記録するデータベースバックアップ。

ディファレンシャルバックアップ

*(Microsoft SQL Server固有の用語)*前回のフルデータベースバックアップ以降にデータベースに対して加えられた変更だけを記録するデータベースバックアップ。
「バックアップの種類も参照。」を参照。

ディファレンシャルバックアップ

前回のフルバックアップより後の変更をバックアップする増分バックアップ。このバックアップを実行するには、増分1バックアップを指定します。
「増分バックアップも参照。」を参照。

ディレクトリ接合

*(Windows固有の用語)*ディレクトリ接合は、Windowsの再解析ポイントのコンセプトに基づいています。NTFS 5ディレクトリ接合では、ディレクトリ/ファイル要求を他の場所にリダイレクトできます。

データストリーム

通信チャンネルを通じて転送されるデータのシーケンス。

データファイル

*(OracleおよびSAP R/3固有の用語)*Oracleによって作成される物理ファイル。表や索引などのデータ構造を格納します。データファイルは、1つのOracleデータベースにのみ所属できます。

データベースサーバー

大規模なデータベース(SAP R/3データベースやMicrosoft SQLデータベースなど)が置かれているコンピュータ。サーバー上のデータベースへは、クライアントからアクセスできます。

データベース並列処理

十分な台数のデバイスが利用可能であり、並列バックアップを実行できる場合には、複数のデータベースが同時にバックアップされます。

データベースライブラリ

Data Protectorのルーチンのセット。Oracle Serverのようなオンラインデータベース統合ソフトウェアのサーバーとData Protectorの間でのデータ転送を可能にします。

データ保護

メディア上のバックアップデータを保護する期間を定義します。この期間中は、データが上書きされません。保護期限が切れると、それ以降のバックアップセッションでメディアを再利用できるようになります。
「カタログ保護も参照。」を参照。

テープなしのバックアップ*(ZDB固有の用語)*

「ディスクへのZDB」を参照。

テープへのZDB

*(ZDB固有の用語)*ゼロダウンタイムバックアップの1つの形式。作成された複製内のデータが、バックアップメディア(通常はテープ)にストリーミングされます。このバックアップ形式ではインスタントリカバリはできませんが、バックアップ終了後にディスクアレイ上に複製を保持する必要がありません。バックアップデータはData Protector標準のテープからの復元を使用して復元できます。スプリットミラーアレイでは、スプリットミラー復元も使用することができます。
「ゼロダウンタイムバックアップ(ZDB)、ディスクへのZDB、インスタントリカバリ、ディスク/テープへのZDB、および複製も参照。」を参照。

デバイス

ドライブまたはより複雑な装置(ライブラリなど)を格納する物理装置。

デバイスグループ

*(EMC Symmetrix固有の用語)*複数のEMC Synnetrixデバイスを表す論理ユニット。デバイスは1つのデバイスグループにしか所属できません。デバイスグループのデバイスは、すべて同じEMC Symmetrix装置に取り付けられている必要があります。デバイスグループにより、利用可能なEMC Symmetrixデバイスのサブセットを指定し、使用することができます。

デバイスストリーミング

デバイスがメディアへ十分な量のデータを継続して送信できる場合、デバイスはストリーミングを行います。そうでない場合は、デバイスはテープを止めてデータが到着するのを待ち、テープを少し巻き戻した後、テープへの書込みを再開します。言い換えると、テープにデータを書き込む速度が、コンピュータシステムがデバイスへデータを送信する速度以下の場合、デバイスはストリーミングを行います。ストリーミングは、スペースの使用効率とデバイスのパフォーマンスを大幅に向上します。

デバイスチェーン

デバイスチェーンは、シーケンシャルに使用するように構成された複数のスタンドアロンデバイスから成ります。デバイスチェーンに含まれるデバイスのメディアで空き容量がなくなると、自動的に次のデバイスのメディアに切り替えて、バックアップを継続します。

デルタバックアップ

差分バックアップ(delta backup)では、前回の各種バックアップ以降にデータベースに対して加えられたすべての変更がバックアップされます。
「バックアップの種類も参照。」を参照。

統合オブジェクト

OracleまたはSAP DBなどの統合ソフトウェアのバックアップオブジェクト。

同時処理数

「Disk Agentの同時処理数を参照。」を参照。

動的(ダイナミック)クライアント

「ディスクディカバリによるクライアントバックアップ」を参照。

ドメインコントローラ

ユーザーのセキュリティを保護し、別のサーバーグループ内のパスワードを検証するネットワーク内のサーバー。

ドライブ

コンピュータシステムからデータを受け取って、磁気メディア(テープなど)に書き込む物理装置。データをメディアから読み取って、コンピュータシステムに送信することもできます。

ドライブのインデックス

ライブラリデバイス内のドライブの機械的な位置を識別するための数字。ロボット機構によるドライブアクセスは、この数に基づいて制御されます。

ドライブベース暗号化

Data Protectorのドライブベース暗号化では、ドライブの暗号化機能を使用します。バックアップの実行中、ドライブではメディアに書き込まれるデータとメタデータの両方が暗号化されます。

トランザクション

一連のアクションを単一の作業単位として扱えるようにするためのメカニズム。データベースでは、トランザクションを通じて、データベースの変更を追跡します。

トランザクションバックアップ

*(SybaseおよびSQL固有の用語)*トランザクションログをバックアップすること。トランザクションログには、前回のフルバックアップまたはトランザクションバックアップ以降に発生した変更が記録されます。

トランザクションバックアップ

トランザクションバックアップは、一般に、データベースのバックアップよりも必要とするリソースが少ないため、データベースのバックアップよりも高い頻度で実行できます。トランザクションバックアップを適用することで、データベースを問題発生以前の特定の時点の状態に復旧することができます。

トランザクションログ

*(Data Protector固有の用語)*IDBに対する変更を記録します。IDB復旧に必要なトランザクションログファイル(前回のIDBバックアップ以降に作成されたトランザクションログ)が失われることがないように、トランザクションログのアーカイブを有効化しておく必要があります。

トランザクションログテーブル

*(Sybase固有の用語)*データベースに対するすべての変更が自動的に記録されるシステムテーブル。

トランザクションログバックアップ

トランザクションログバックアップは、一般に、データベースのバックアップよりも必要とするリソースが少ないため、データベースのバックアップよりも高い頻度で実行できます。トランザクションログバックアップを用いることにより、データベースを特定の時点の状態に復旧できます。

トランザクションログファイル

データベースを変更するトランザクションを記録するファイル。データベースが破損した場合にフォールトトレランスを提供します。

トランスポータブルスナップショット

*(Microsoft VSS固有の用語)*アプリケーションシステム上に作成されるシャドウコピー。このシャドウコピーは、バックアップを実行するバックアップシステムに提供できます。
「Microsoft Volume Shadow Copy Service (VSS)も参照」を参照。

ハートビート

特定のクラスターノードの動作ステータスに関する情報を伝達するタイムスタンプ付きのクラスターデータセット。このデータセット(パケット)は、すべてのクラスターノードに配布されます。

ハード復旧

*(Microsoft Exchange Server固有の用語)*トランザクションログファイルを使用し、データベースエンジンによる復元後に実行されるMicrosoft Exchange Serverのデータベース復旧。

配布ファイルメディア形式

ファイルライブラリで利用できるメディア形式。仮想フルバックアップと呼ばれる容量効率のいい合成バックアップをサポートしています。

この形式を使用することは、仮想フルバックアップにおける前提条件です。
「仮想フルバックアップも参照。」を参照。

バックアップAPI

Oracleのバックアップ/復元ユーティリティとバックアップ/復元メディア管理層の間にあるOracleインタフェース。このインタフェースによってルーチンのセットが定義され、バックアップメディアのデータの読み書き、バックアップファイルの作成や検索、削除が行えるようになります。

バックアップID

統合ソフトウェアオブジェクトの識別子で、統合ソフトウェアオブジェクトのバックアップのセッションIDと一致します。バックアップIDは、オブジェクトのコピー、エクスポート、またはインポート時に保存されます。

バックアップオーナー

IDBの各バックアップオブジェクトにはオーナーが定義されています。デフォルトのオーナーは、バックアップセッションを開始したユーザーです。

バックアップオブジェクト

1つのディスクボリューム(論理ディスクまたはマウントポイント)からバックアップされた項目すべてを含むバックアップ単位。バックアップ項目は、任意の数のファイル、ディレクトリ、ディスク全体またはマウントポイントの場合が考えられます。また、バックアップオブジェクトはデータベース/アプリケーションエンティティまたはディスクイメージ(rawディスク)の場合もあります。
バックアップオブジェクトは以下のように定義されています。

- クライアント名: バックアップオブジェクトが保存されるData Protectorクライアントのホスト名
- マウントポイント: ファイルシステムオブジェクトを対象とする場合ーバックアップオブジェクトが存在するクライアント(Windowsではドライブ、UNIXではマウントポイント)上のディレクトリ構造におけるアクセスポイント。統合オブジェクトを対象とする場合ーバックアップストリームID。バックアップされたデータベース項目/アプリケーション項目を示します。
- 説明: ファイルシステムオブジェクトを対象とする場合ー同一のクライアント名とマウントポイントを持つオブジェクトを一意に定義します。統合オブジェクトを対象とする場合ー統合の種類を表示します(例: SAPまたはLotus)。
- 種類:バックアップオブジェクトの種類。ファイルシステムオブジェクトを対象とする場合ーファイルシステムの種類(例: WinFS)。統合オブジェクトを対象とする場合ー「Bar」

バックアップシステム

*(ZDB固有の用語)*1つ以上のアプリケーションシステムのターゲットボリュームに接続しているシステム。典型的なバックアップシステムは、バックアップデバイスに接続され、複製内のデータのバックアップを実行します。
「アプリケーションシステム、ターゲットボリュームおよび複製」を参照。

バックアップ仕様

バックアップ対象オブジェクトを、使用するデバイスまたはドライブのセット、仕様内のすべてのオブジェクトに対するバックアップオプション、およびバックアップを行いたい日時とともに指定したリスト。オブジェクトとなるのは、ディスクやボリューム全体、またはその一部、たとえばファイル、ディレクトリ、Windowsレジストリなどです。インクルードリストおよびエクスクルードリストを使用して、ファイルを選択することもできます。

バックアップ世代

1つのフルバックアップとそれに続く増分バックアップを意味します。次のフルバックアップが行われると、世代が新しくなります。

バックアップセッション

データのコピーを記憶メディア上に作成するプロセス。バックアップ仕様に処理内容を指定することも、対話式に操作を行うこと(対話式セッション)もできます。1つのバックアップ仕様の中で複数のクライアントが構成されている場合、すべてのクライアントが同じバックアップの種類(フルまたは増分) を使って、1回のバックアップセッションで同時にバックアップされます。バックアップセッションの結果、1式のメディアにバックアップデータが書き込まれます。これらのメディアは、バックアップセットまたはメディアセットとも呼ばれます。
「バックアップ仕様、増分バックアップ、およびフル バックアップも参照。」を参照。

バックアップセット

*(Oracle固有の用語)*RMANバックアップコマンドを使用して作成したバックアップファイルの論理グループ。バックアップセットは、バックアップに関連したすべてのファイルのセットです。これらのファイルはパフォーマンスを向上するため多重化することができます。バックアップセットにはデータファイルまたはアーカイブログのいずれかを含めることができますが、両方同時に使用できません。

バックアップセット

バックアップに関連したすべての統合ソフトウェアオブジェクトのセットです。

バックアップチェーン

「復元チェーン」を参照。

バックアップデバイス

記憶メディアに対するデータの読み書きが可能な物理デバイスをData Protectorで使用できるように構成したもの。たとえば、スタンドアロンDDS/DATドライブやライブラリなどをバックアップデバイスとして使用できます。

バックアップの種類

「増分バックアップ、ディファレンシャルバックアップ、トランザクションバックアップ、フルバックアップおよびデルタバックアップ」を参照。

バックアップビュー

Data Protectorでは、バックアップ仕様のビューを切り替えることができます。
[種類別]を選択すると、バックアップ/テンプレートで利用できるデータの種類に基づいたビューが表示されます。(デフォルト)
[グループ別]を選択すると、バックアップ仕様/テンプレートの所属先のグループに基づいたビューが表示されます。
[名前別]を選択すると、バックアップ仕様/テンプレートの名前に基づいたビューが表示されます。
[Manager別](MoMの実行時のみ有効)を選択すると、バックアップ仕様/テンプレートの所属先のCell Managerに基づいたビューが表示されます。

パッケージ

*(MC/ServiceGuardVeritas Cluster固有の用語)*特定のクラスター対応アプリケーションを実行するために必要なリソース(ボリュームグループ、アプリケーションサービス、IP名およびIPアドレスなど)の集合。

パブリック/プライベートバックアップデータ

バックアップを構成する際は、バックアップデータをパブリックまたはプライベートのいずれにするかを選択できます。

- パブリックデータ ― すべてのData Protectorユーザーに対してアクセスと復元が許可されます。
- プライベートデータ ― バックアップの所有者および管理者に対してのみ表示と復元が許可されます。

パブリックフォルダストア

*(Microsoft Exchange Server固有の用語)*インフォメーションストアのうち、パブリックフォルダ内の情報を維持する部分。パブリックフォルダストアは、バイナリリッチテキスト.edbファイルと、ストリーミングネイティブインターネットコンテンツを格納する.stmファイルから構成されます。

ファーストレベルミラー

*(HP StorageWorks Disk Array XP固有の用語)*HP StorageWorks Disk Array XPでは、プライマリボリュームのミラーコピーを最大3つまで作成することができ、このコピー1つにつきさら

に2つのコピーを作成できます。最初の3つのミラーコピーはファーストレベルミラーと呼ばれます。
「プライマリボリュームおよびMU番号も参照。」を参照。

ファイルシステム
ハードディスク上に一定の形式で保存されたファイルの集まり。ファイルシステムは、ファイル属性とファイルの内容がバックアップメディアに保存されるようにバックアップされます。

ファイルジュークボックスデバイス
ファイルメディアを格納するために使用する、複数のスロットからなるディスク上に存在するデバイス。

ファイルツリーウォーク
*(Windows固有の用語)*どのオブジェクトが作成、変更、または削除されたかを判断するためにファイルシステムを巡回する処理。

ファイルデポ
バックアップからファイルライブラリデバイスまでのデータを含むファイル。

ファイルバージョン
フルバックアップや増分バックアップでは、ファイルが変更されている場合、同じファイルが複数回バックアップされます。バックアップのロギングレベルとして[すべてログに記録]を選択している場合は、ファイル名自体に対応する1つのエントリとファイルの各バージョンに対応する個別のエントリがIDB内に維持されます。

ファイル複製サービス(FRS)
Windowsサービスの1つ。ドメインコントローラのストアログオンスクリプトとグループポリシーを複製します。また、分散ファイルシステム(DFS)共有をシステム間で複製したり、任意のサーバーから複製作業を実行することもできます。

ファイルライブラリデバイス
複数のメディアからなるライブラリをエミュレートするディスク上に存在するデバイス。ファイルデポと呼ばれる複数のファイルが格納されます。

ブートボリューム/ディスク/パーティション
ブートプロセスの開始に必要なファイルが入っているボリューム/ディスク/パーティション。Microsoftの用語では、オペレーティングシステムファイルが入っているボリューム/ディスク/パーティションをブートボリューム/ブートディスク/ブートパーティションと呼んでいます。

ブール演算子
オンラインヘルプシステムの全文検索には、AND、OR、NOT、NEARの各ブール演算子を使用できます。複数の検索条件をブール演算子で組み合わせて指定することで、検索対象をより正確に絞り込むことができます。複数単語の検索に演算子を指定しなければ、ANDを指定したものとみなされます。たとえば、「manual disaster recovery」という検索条件は、「manual AND disaster AND recovery」と同じ結果になります。

フェイルオーバー

*(HP StorageWorks EVA固有の用語)*CA+BC EVA構成におけるソースとあて先の役割を逆にする操作。
「CA+BC、EVA.も参照。」を参照。

フェイルオーバー

あるクラスターノードから別のクラスターノードに最も重要なクラスターデータ(Windowsの場合はグループ、UNIXの場合はパッケージ)を転送すること。フェイルオーバーは、主に、プライマリノードのソフトウェア/ハードウェア障害発生時や保守時に発生します。

負荷調整

デフォルトでは、デバイスが均等に使用されるように、バックアップ用に選択されたデバイスの負荷(使用率)が自動的に調整されます。負荷調整では、各デバイスに書き込まれるオブジェクトの個数を調整することで、使用率を最適化します。負荷調整はバックアップ時に自動的に実行されるので、データが実際にどのようにバックアップされるかを管理する必要はありません。使用するデバイスを指定する必要があるだけです。負荷調整機能を使用しない場合は、バックアップ仕様に各オブジェクトに使用するデバイスを選択できます。Data Protectorは、指定した順にデバイスにアクセスします。

復元セッション

バックアップメディアからクライアントシステムにデータをコピーするプロセス。

復元チェーン

特定の時点までのバックアップオブジェクトの復元に必要なバックアップすべて。復元チェーンは、オブジェクトのフルバックアップ1つと、任意の数の増分バックアップで構成されます。

複製

*(ZDB固有の用語)*ユーザー指定のバックアップオブジェクトを含む、特定の時点におけるソースボリュームのデータのイメージ。イメージは、作成するハードウェアまたはソフトウェアによって、物理ディスクレベルでの記憶ブロックの独立した正確な複製(クローン)になる(スプリットミラーやスナップクローンなど)場合もあれば、仮想コピーになる(スナップショットなど)場合もあります。基本的なオペレーティングシステムの観点からすると、バックアップオブジェクトを含む物理ディスク全体が複製されます。しかし、UNIXでボリュームマネージャを使用するときは、バックアップオブジェクトを含むボリュームまたはディスクグループ全体が複製されます。Windowsでパーティションを使用する場合、選択したパーティションを含む物理ボリューム全体が複製されます。
「スナップショット、スナップショット作成、スプリットミラー、およびスプリットミラーの作成も参照。」を参照。

複製セット

*(ZDB固有の用語)*同じバックアップ仕様を使って作成される複製のグループ。
「複製および複製セットローテーションも参照。」を参照。

複製セットローテーション

*(ZDB固有の用語)*通常のバックアップ作成のために継続的に複製セットを使用すること。複製セットの使用を必要とする同一のバックアップ仕様が実行されるたびに、新規の複製がセットの最大数になるまで作成され、セットに追加されます。その後、セット内の最も古い複製は置き換えられ、セット内の複製の最大数が維持されます。
「複製および複製セットも参照。」を参照。

物理デバイス

ドライブまたはより複雑な装置(ライブラリなど)を格納する物理装置。

プライマリボリューム(P-VOL)

*(HP StorageWorks Disk Array XP固有の用語)*CAとBC構成用のプライマリボリュームとしての役割を果たす標準HP StorageWorks XP Disk Array XP LDEV。P-VOLはMCU内に配置されています。
「セカンダリボリューム(S-VOL)およびMain Control Unit (MCU)も参照。」を参照。

フラッシュリカバリ領域

*(Oracle固有の用語)*フラッシュリカバリ領域は、バックアップと復旧に関係するファイル(リカバリファイル)の集中管理ストレージ領域として機能する、Oracle 10g/11gによって管理されるディレクトリ、ファイルシステム、または自動ストレージ管理のディスクグループです。
「リカバリファイルも参照。」を参照。

フリープール

フリープールは、メディアプール内のすべてのメディアが使用中になっている場合にメディアのソースとして補助的に使用できるプールです。ただし、メディアプールでフリープールを使用するには、明示的にフリー プールを使用するように構成する必要があります。

フルZDB

前回のバックアップから変更がない場合でも選択されたすべてのオブジェクトをテープにストリーミングする、テープへのZDBセッションまたはディスク+テープへのZDBセッション。
「増分ZDBも参照。」を参照。

フルデータベースバックアップ

最後に(フルまたは増分)バックアップした後に変更されたデータだけではなく、データベース内のすべてのデータのバックアップ。フルデータベースバックアップは、他のバックアップに依存しません。

フルバックアップ

フルバックアップでは、最近変更されたかどうかに関係なく、選択されたオブジェクトをすべてバックアップします。
「バックアップの種類も参照。」を参照。

フルメール

フルメールボックスバックアップでは、メールボックス全体の内容をバックアップします。

分散ファイルシステム(DFS)

複数のファイル共有を単一の名前空間に接続するサービス。対象となるファイル共有は、同じコンピュータに置かれていても、異なるコンピュータに置かれていてもかまいません。DFSは、リソースの保存場所の違いに関係なくクライアントがリソースにアクセスできるようにします。

ペアステータス

*(HP StorageWorks Disk Array XP固有の用語)*ミラー化されたディスクのペアは、そのペア上で実行されるアクションによって、さまざまなステータス値を持ちます。重要なステータス値は以下の3つです。

- コピー－ミラー化されたペアは、現在再同期中。データは一方のディスクからもう一方のディスクに転送されます。2つのディスクのデータは同じではありません。
- ペア－ミラー化されたペアは完全に同期され、両方のディスク(プライマリボリュームとミラー化されたボックス)に同じデータが格納されます。
- 中断－ミラー化されたディスク間のリンクは中断されています。両方のディスクが別々にアクセスされ、更新されています。ただし、ミラー関係はまだ保持されており、このペアは、ディスク全体を転送することなく、再同期することができます。

並行復元

単一のMedia Agentからデータを受信するDisk Agentを複数実行して、バックアップされたデータを複数のディスクに同時に(つまり並行して)復元すること。並行復元を行うには、複数のディスクまたは論理ボリュームに置かれているデータを選択し、同時処理数を2以上に設定してバックアップを開始し、異なるオブジェクトのデータを同じデバイスに送信する必要があります。並行復元中には、復元対象として選択した複数のオブジェクトがメディアから同時に読み取られるので、パフォーマンスが向上します。

並列処理

1つのオンラインデータベースから複数のデータストリームを読み取ること。

保護

「データ保護およびカタログ保護」を参照。

ホストシステム
ホストシステムとは、ディスクデリバリーによる障害復旧に使用される、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。

ボリュームグループ
LVMシステムにおけるデータストレージ単位。ボリュームグループは、1つまたは複数の物理ボリュームから作成できます。同じシステム上に複数のボリュームグループを置くことができます。

ボリュームマウントポイント
*(Windows固有の用語)*ボリューム上の空のディレクトリを他のボリュームのマウントに使用できるように構成したもの。ボリュームマウントポイントは、ターゲットボリュームへのゲートウェイとして機能します。ボリュームがマウントされていれば、ユーザーやアプリケーションがそのボリューム上のデータをフル(マージ)ファイルシステムパスで参照できます(両方のボリュームが一体化されている場合)。

マージ
復元中のファイル名競合を解決するモードの1つ。復元するファイルと同じ名前のファイルが復元先に存在する場合、変更日時の新しい方が維持されます。既存のファイルと名前が重複しないファイルは、常に復元されます。
「上書き.」を参照。

マウントポイント
ディレクトリ構造内において、ディスクまたは論理ボリュームにアクセスするためのアクセスポイント(/optやd:など)。UNIXでは、bdfコマンドまたはdfコマンドを使ってマウントポイントを表示できます。

マジックパケット
「Wake ONLAN」を参照。

マルチドライブサーバー
単一システム上でMedia Agentを無制限に使用できるライセンス。このライセンスは、Cell ManagerのIPアドレスにバインドされており、新しいバージョンでは廃止されました。

ミラー*(EMC Symmetrixおよび HP StorageWorks Disk Array XP固有の用語)*
「ターゲットボリューム」を参照。

ミラーローテーション*(HP StorageWorks Disk Array XP固有の用語)*
「複製セットローテーション」を参照。

無人操作
「lights-out operation」を参照。

無人操作
(lights-out operationまたはunattended operation)

オペレータの介在なしで、通常の営業時間外に実行されるバックアップ操作または復元操作。オペレータが手動で操作することなく、バックアップアプリケーションやサービスのマウント要求などが自動的に処理されます。

メールボックス

*(Microsoft Exchange Server固有の用語)*電子メールが配信される場所。管理者がユーザーごとに設定します。電子メールの配信場所として複数の個人用フォルダが指定されている場合は、メールボックスから個人用フォルダに電子メールがルーティングされます。

メールボックスストア

*(Microsoft Exchange Server固有の用語)*インフォメーションストアのうち、ユーザーメールボックス内の情報を維持する部分。メールボックスストアは、バイナリデータを格納するリッチテキスト. edbファイルと、ストリーミングネイティブインターネットコンテンツを格納する. stmファイルからなります。

メディアID

Data Protectorがメディアに割り当てる一意な識別子。

メディア位置

バックアップ メディアが物理的に収納されている場所を示すユーザー定義の識別子。"building 4"や"off-site storage"のような文字列です。

メディア管理セッション

初期化、内容のスキャン、メディア上のデータの確認、メディアのコピーなどのアクションをメディアに対して実行するセッション。

メディア状態

メディア状態要素から求められるメディアの品質。テープ メディアの使用頻度が高く、使用時間が長ければ、読み書きエラーの発生率が高くなります。状態が[不良]になったメディアは交換する必要があります。

メディア状態要素

使用回数のしきい値と上書きのしきい値。メディアの状態の判定基準となります。

メディアセット

バックアップセッションでは、メディアセットと呼ばれるメディアのグループにデータをバックアップします。メディアの使用法によっては、複数のセッションで同じメディアを共有できます。

メディアのインポート

メディアに書き込まれているバックアップセッションデータをすべて再読み込みして、IDBに取り込むプロセス。これにより、メディア上のデータにすばやく、簡単にアクセスできるようになります。
「メディアのエクスポートも参照。」を参照。

メディアのエクスポート
メディアに格納されているすべてのバックアップセッション情報(システム、オブジェクト、ファイル名など)をIDBから削除するプロセス。メディア自体に関する情報やメディアとプールの関係に関する情報もIDBから削除されます。メディア上のデータは影響されません。「メディアのインポート」を参照。

メディアの種類
メディアの物理的な種類(DDSやDLTなど)。

メディアの使用法
メディアの使用法は、すでに使用されているメディアに対してバックアップをどのように追加するかを制御します。メディアの使用法は、[追加可能]、[追加不可能]、[増分のみ追加可能]のいずれかに設定できます。

メディアのボールティング
メディアを安全な別の場所に収納すること。メディアが復元に必要になった場合や、今後のバックアップにメディアを再使用する場合は、メディアをデータセンターに戻します。ボールティング手順は、会社のバックアップ戦略やデータ保護/信頼性ポリシーに依存します。

メディアプール
同じ種類のメディア(DDSなど)のセット。グループとして追跡されます。フォーマットしたメディアは、メディアプールに割り当てられます。

メディアラベル
メディアに割り当てられるユーザー定義の識別子。

メディア割り当てポリシー
メディアをバックアップに使用する順序を決定します。[Strict]メディア割り当てポリシーでは、特定のメディアに限定されます。[Loose]ポリシーでは、任意の適切なメディアを使用できます。[フォーマットされていないメディアを先に割り当てる]ポリシーでは、ライブラリ内に利用可能な非保護メディアがある場合でも、不明なメディアが優先されます。

元のシステム
あるシステムに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。

ユーザーアカウント(Data Protector ユーザーアカウント)
Data Protectorおよびバックアップデータに対する無許可のアクセスを制限するために、Data Protectorユーザーとして許可を受けたユーザーにしかData Protectorを使用できないようになっています。Data Protector 管理者がこのアカウントを作成するときには、ユーザーログオン名、ユーザーのログオン元として有効なシステム、およびData Protectorユーザーグループのメンバーシップを指定します。ユーザーがData Protectorのユーザーインタフェースを起動するか、または特定のタスクを実行するときには、このアカウントが必ずチェックされます。

ユーザーグループ
各Data Protectorユーザーは、ユーザーグループのメンバーです。各ユーザーグループには1式のユーザー権限があり、それらの権限がユーザーグループ内のすべてのユーザーに付与されます。ユーザー権限を関連付けるユーザーグループの数は、必要に応じて定義できます。Data Protectorには、デフォルトでAdmin、Operator、Userの3つのユーザーグループが用意されています。

ユーザー権限
特定のData Protectorタスクの実行に必要なパーミッションをユーザー権限またはアクセス権限と呼びます。主なユーザー権限には、バックアップの構成、バックアップセッションの開始、復元セッションの開始などがあります。ユーザーには、そのユーザーの所属先ユーザーグループに関連付けられているアクセス権限が割り当てられます。

ユーザーディスク割り当て
NTFSの容量管理サポートを使用すると、共有ストレージボリュームに対して、拡張された追跡メカニズムの使用およびディスク容量に対する制御が行えるようになります。Data Protectorでは、システム全体にわたるユーザーディスク割り当てが、すべてのユーザーに対して一度にバックアップされます。

ユーザープロファイル
*(Windows固有の用語)*ユーザー別に保持される構成情報。この情報には、デスクトップ設定、画面表示色、ネットワーク接続などが含まれます。ユーザーがログオンすると、そのユーザーのプロファイルがロードされ、Windows環境がそれに応じて設定されます。

ライター
*(Microsoft VSS固有の用語)*オリジナルボリューム上のデータの変更を開始するプロセス。主に、永続的なデータをボリューム上に書き込むアプリケーションまたはシステムサービスがライターとなります。ライターは、シャドウコピーの同期化プロセスにも参加し、データの整合性を保証します。

ライブラリ
オートチェンジャー、ジュークボックス、オートローダー、またはエクスチェンジャとも呼ばれます。ライブラリには、複数のレポジトリスロットがあり、それらにメディアが格納されます。各スロットがメディア(DDS/DATなど)を1つずつ格納します。スロット/ドライブ間でのメディアの移動は、ロボット機構によって制御され、メディアへのランダムアクセスが可能です。ライブラリには、複数のドライブを格納できます。

リカバリカタログ
*(Oracle固有の用語)*Recovery ManagerがOracleデータベースについての情報を格納するために使用するOracleの表とビューのセット。この情報は、Recovery ManagerがOracleデータベースのバックアップ、復元、および復旧を管理するために使用されます。リカバリカタログには、以下の情報が含まれます。

- Oracleターゲットデータベースの物理スキーマ
- データファイルおよびアーカイブログのバックアップセット
- データファイルのコピー
- アーカイブREDOログ
- ストアドスクリプト

リカバリカタログデータベース

*(Oracle固有の用語)*リカバリカタログスキーマを格納するOracleデータベース。リカバリカタログはターゲットデータベースに保存しないでください。

リカバリカタログデータベースへのログイン情報

*(Oracle固有の用語)*リカバリカタログデータベース(Oracle)へのログイン情報の形式は*<user_name>/<password>@<service>*で、ユーザー名、パスワード、サービス名の説明は、Oracleターゲットデータベースへの Oracle SQL*Net V2ログイン情報と同じです。ただし、この場合の*service*はOracleターゲットデータベースではなく、リカバリカタログデータベースに対するサービス名となります。ここで指定するOracleユーザーは、Oracleのリカバリカタログのオーナーでなければならないことに注意してください。

リカバリファイル

*(Oracle固有の用語)*リカバリファイルはフラッシュリカバリ領域に存在するOracle 10g/11g固有のファイルで、現在の制御ファイル、オンラインREDOログ、アーカイブREDOログ、フラッシュバックログ、制御ファイル自動バックアップ、データファイルコピー、およびバックアップピースがこれにあたります。
「フラッシュリカバリ領域も参照。」を参照。

リサイクル

メディア上のすべてのバックアップデータのデータ保護を解除して、以降のバックアップで上書きできるようにするプロセス。同じセッションに所属しているデータのうち、他のメディアに置かれているデータも保護解除されます。リサイクルを行っても、メディア上のデータ自体は変更されません。

リムーバブル記憶域の管理データベース

*(Windows固有の用語)*Windowsサービスの1つ。リムーバブルメディア(テープやディスクなど)と記憶デバイス(ライブラリ)の管理に使用されます。リムーバブル記憶域により、複数のアプリケーションが同じメディアリソースを共有できます。

ローカル復旧とリモート復旧

リモート復旧は、SRDファイルで指定されているMedia Agentホストがすべてアクセス可能な場合にのみ実行されます。いずれかのホストがアクセス不能になっていると、障害復旧プロセスがローカルモードにフェイルオーバーされます。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。複数のデバイスが見つかった場合は、デバイスが選択できるプロンプトが表示され、ユーザーが選択したデバイスが復元に使用されます。

ローカル連続レプリケーション

*(Microsoft Exchange Server固有の用語)*ローカル連続レプリケーション(LCR)はストレージグループの完全コピー(LCRコピー)を作成および維持するシングルサーバーソリューション。LCRコピーは元のストレージグループと同じサーバーに配置されます。LCRコピーが作成されると、変更伝播(ログリプレイ)テクノロジで最新に保たれます。LCRの複製機能では未複製のログが削除されません。この動作の影響により、ログを削除するモードでバックアップを実行しても、コピー中のログと複製に十分な余裕がある場合、実際にはディスクの空き容量が解放されない場合があります。
LCRコピーへの切り替えは数秒で完了するため、LCRコピーは障害復旧に使用されます。元のデータとは異なるディスクに存在するLCRコピーをバックアップに使用すると、プロダクションデータベースの入出力の負荷が最小になります。
複製されたストレージグループは、Exchangeライターの新しいインスタンス(Exchange Replication Service)として表示され、通常のストレージグループのようにVSSを使用してバックアップできます。
「クラスター連続レプリケーションおよびExchange Replication Serviceも参照。」を参照。

ロギングレベル

ロギングレベルは、バックアップ、オブジェクトのコピー、またはオブジェクトの集約時にファイルとディレクトリに関する情報をどの程度まで詳細にIDBに記録するかを示します。バックアップ時のロギングレベルに関係なく、データの復元は常に可能です。Data Protectorには、[すべてログに記録]、[ディレクトリレベルまでログに記録]、[ファイルレベルまでログに記録]、[ログなし]の4つのロギングレベルがあります。ロギングレベル設定によって、IDBのサイズ増加、バックアップ速度、および復元データのブラウザのしやすさが影響を受けます。

ログインID

*(Microsoft SQL Server固有の用語)*Microsoft SQL Serverにログインするためにユーザーが使用する名前。Microsoft SQL Serverのsysloginシステムテーブル内のエントリに対応するログインIDが有効なログインIDとなります。

ロック名

複数のデバイス名を使うことにより、同じ物理デバイスを異なる特性で何度も構成することができます。そのようなデバイス(デバイス名)が複数同時に使用された場合に重複を防ぐ目的で、デバイス構成をロックするためにロック名が使用されます。ロック名はユーザーが指定する文字列です。同一の物理デバイスを使用するデバイス定義には、すべて同じロック名を使用します。

論理ログファイル　論理ログファイルは、変更されたデータがディスクにフラッシュされる前に書き込まれるファイルです。変更されたデータがディスクにフラッシュされる前に書き込まれるファイルです。障害発生時には、これらの論理ログファイルを使用することで、コミット済みのトランザクションをすべてロールフォワードするとともに、コミットされていないトランザクションをロールバックすることができます。

ワイルドカード文字　1文字または複数文字を表すために使用できるキーボード文字。たとえば、通常、アスタリスク(*)は1文字以上の文字を表し、疑問符(?)は1文字を示します。ワイルドカード文字は、名前により複数のファイルを指定するための手段としてオペレーティングシステムで頻繁に使用されます。

索引

あ

お

か

き

く

さ

し

せ

た

て

と

は

ひ

ふ

へ

ほ

よ

ろ

わ