Hewlett Packard Enterprise

HPE Data Protector

ソフトウェアバージョン: 10.00

管理者ガイド

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

ご注意

保証

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

ここに記載する情報は、予告なしに変更されることがあります。

権利の制限

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

著作権について

© Copyright 2017 Hewlett Packard Enterprise Development LP

商標について

Adobe™はAdobe Systems Incorporatedの商標です。

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

UNIX®は、The Open Groupの登録商標です。

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

ドキュメントの更新情報

このマニュアルの表紙には、以下の識別情報が記載されています。

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

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

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

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

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

サポート

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

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

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

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

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

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

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

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

目次

第1章: 概要 1

Data Protectorについて 1
Data Protectorの主な特長 1

HPE Data Protectorアーキテクチャー 1
Cell Manager 1
インストールサーバー 2
クライアントシステム 2
バックアップ対象のシステム 2
バックアップデバイスが接続されているシステム 2

HPE Data Protectorセットアップ作業の概要 2
手順 3

HPE Data Protectorの操作 4
バックアップセッション 4
復元セッション 4
実行前コマンドと実行後コマンド 4
オブジェクトコピー、オブジェクト集約、およびオブジェクト検証セッション 5

ユーザーインターフェイス 5
グラフィカルユーザーインターフェイス 5
コマンドラインインターフェイス 5

GUIで言語設定をカスタマイズする 6
前提条件 6
制限事項 6
手順 6

HPE Data Protector GUIを起動する 6

Microsoft管理コンソール(MMC)の使用法 7
手順 7

Data ProtectorのGUIからHPEStorage Optimizerを起動する 7

第2章: 構成作業 8

システムのセキュリティ 8
セキュアな通信のための証明書の構成 8
GUIからCell Manager/Jumpstation UIに接続する 9
ユーザーのセキュリティ 10
ユーザー権限 10
[バックアップ仕様を開始]ユーザー権限 10
バックアップ仕様の内容にアクセスできないようにする 11
ホストの信頼 11
ユーザーグループ 11
ユーザー制限 11

ユーザーのチェック 11
厳密なホスト名チェック 12
制限事項 12
要件 12
ホスト名の解決 13
セキュリティログ 13
クライアントの保護イベント 13
Cell Managerのセキュリティイベント 13
ホストの信頼を構成する 14
手順 14
暗号化 14
データの暗号化について 14
AES 256ビット暗号化を有効化する 15
前提条件 15
制限事項 15
ファイルシステムのバックアップ仕様で暗号化を有効化する 15
手順 15
ディスクイメージバックアップ仕様で暗号化を有効化する 15
手順 15
内部データベースバックアップ仕様で暗号化を有効化する 16
手順 16
アプリケーション統合バックアップ仕様で暗号化を有効化する 16
制限事項 16
手順 16
暗号化されたバックアップを含むメディアのエクスポートとインポート 16
CMMDBを含まないCell Manager環境またはMoM環境 17
手順 17
CMMDBを含むMoM環境 17
手順 17
ドライブベースの暗号化の有効化 17
前提条件 18
制限事項 18
推奨事項 18
ドライブ構成でドライブベースの暗号化を有効化する 18
手順 18
バックアップ仕様でドライブベースの暗号化を有効化する 18
手順 18
自動メディア操作におけるドライブベースの暗号化を有効化する 19
手順 19
ユーザー認証とLDAPについて 19
LDAPログインモジュールを初期化して構成する 20
LDAPログインモジュールを初期化する 20
LDAPログインモジュールを構成する 22
HPE Data Protectorの権限をLDAPユーザーまたはグループに付与する 24
LDAPユーザーをData Protectorユーザーグループに追加する 24
LDAPグループをData Protectorユーザーグループに追加する 25

LDAP資格情報を使用してログインする 25
LDAP構成をチェックする 26
ファイアウォールのサポート 26
ファイアウォールのサポートについて 26
Data Protector内の通信 27
構成メカニズム 28
HPE Data Protector 9.09以降におけるポートの使用 29
制限事項 30
DMZ内のDisk Agent、Media Agent、およびApplication Agent 30
構成図 31
ポートを開く 31
制限事項 32

第3章: ユーザーとユーザーグループ 34
ユーザー管理について 34
ユーザー 34
UNIX 34
Windows 34
定義済みユーザー 34
ユーザーグループ 36
定義済みのユーザーグループ 36
利用可能なユーザー権限 37
ユーザーへのWebサービスアクセスの提供 37
HPE Data Protector GUIの使用 37
CLIの使用 37
ユーザーの構成 38
ユーザーを追加する 38
前提条件 38
手順 38
ユーザーを表示する 38
前提条件 39
手順 39
ユーザープロパティを変更する 39
前提条件 39
手順 39
他のユーザーグループにユーザーを移動する 39
前提条件 39
手順 40
ユーザーを削除する 40
前提条件 40
手順 40
ユーザーグループの構成 40
ユーザーグループを追加する 40

前提条件 41
手順 41
ユーザーグループを表示する 41
前提条件 41
手順 41
ユーザー権限を変更する 41
前提条件 42
手順 42
ユーザーグループを削除する 42
前提条件 42
手順 42

第4章: 内部データベース 43

IDBについて 43
IDBを使用する理由 43
IDBのサイズと増大に関する考慮事項 43
IDBの定期的バックアップ 43

IDBアーキテクチャー 44
IDBの構成要素 44
メディア管理データベース(MMDB) 45
MMDBレコード 45
MMDBのサイズと増加 45
MMDBの位置 45
カタログデータベース(CDB) 45
CDBレコード 45
CDB(オブジェクトと位置)のサイズと増加 45
CDBの位置 46
詳細カタログバイナリファイル(DCBF) 46
DCBF情報 46
DCBFのサイズと増加 46
DCBFの位置 46
セッション メッセージ バイナリ ファイル(SMBF) 47
SMBFレコード 47
SMBFのサイズと増加 47
SMBFの位置 47
暗号化キーストアとカタログファイル 47
キーストアの位置 47
カタログファイルの位置 48

IDBの操作 48
バックアップ 48
IDBバックアップとアーカイブログファイル 48
復元 48
オブジェクトコピーおよびオブジェクト集約 49
オブジェクト検証 49
メディアのエクスポート 49

詳細カタログの削除 49
内部データベースの構成 50
IDBの構成 50
IDB用のディスクスペースの割り当て 50
前提条件 50
ディスクスペースの必要量 50
事前に計画しておくべきこと 51
IDBディレクトリの位置 51
制限事項 51
IDBディレクトリの推奨位置 52
堅牢性に関する留意事項 53
IDBバックアップの構成 53
IDBのバックアップ仕様の準備と実行に関するヒント 53
内部データベースの保守 55
IDBの保守について 55
内部データベースのサイズ増加とパフォーマンス 55
IDBのサイズ増加とパフォーマンスについて 55
IDBの主なサイズ増加要因 55
IDBの主なパフォーマンス要因 56
IDBのサイズ増加とパフォーマンスに関する主なパラメーター 56
ロギングレベルがIDBに及ぼす影響 57
カタログ保護がIDBに及ぼす影響 57
IDBのサイズの見積もり 57
DCディレクトリの保守 57
IDBのサイズをチェックする 58
手順 59
IDBのサイズ増加率を減らす 59
ロギングレベルを下げる 59
手順 59
カタログ保護期間を短縮する 60
手順 60
IDBの現在のサイズを縮小する 60
セッションのカタログ保護を変更する 60
手順 61
オブジェクトのカタログ保護を変更する 61
手順 61
IDBサイズを拡張する 61
DCディレクトリをより大きな容量に再構成する 61
手順 61
IDBの整合性チェック 62
他のCell ManagerにIDBを移動する 62
手順 63
手順 63
Data Protectorのグローバルオプションをカスタマイズする 64
前提条件 64
GUI使用によるグローバルオプション設定 64

手順 64
グローバルファイルの編集によるオプションのカスタマイズ 65
手順 65
IDBレポートの構成 66
IDBレポート 66
IDB通知の構成 66
IDB通知 66
IDBを復元する 66
IDBを復元する 66
前提条件 67
制限事項 67
手順 67
暗号化されたバックアップからのIDB復元の準備 68
手順 68
IDBの回復について 68
完全回復(前回のIDBバックアップ以降の変更内容の復元と更新) 69
IDB回復方法の概要 69
最も効率的な完全回復 69
IDBの破損部分の除外(削除) 69
その他の回復方法 70
IDB破損レベル 70
IDBの破損レベルを特定する 71
手順 71
ガイド式自動回復(IDBの復元とアーカイブログファイルの再生)を実行する 71
前提条件 72
手順 72
IDBのDCBF部分の[警戒域]レベルの破損に対処する 73
DCバイナリファイル喪失時の回復 73
手順 73
DCバイナリファイル破損時の回復 73
手順 74
IDB復旧ファイルと新しいデバイスを使ってIDBを復元する 74
前提条件 74
手順 75
IDB復旧ファイルを使わずにIDBを復元する 75
前提条件 75
手順 76
特定のIDBセッションからIDBを復元する 77
前提条件 77
手順 78
異なるCell Managerホスト上でIDBデータベースを復元する 78
メディアをインポートしてIDBを更新する 80
手順 80

第5章: Manager-of-Managers環境 81

MoM環境について 81
CMMDBについて 81
メディアの共有方法 81
メディアの初期化方法 82
MoM環境の構成手順 82
前提条件 82
MoM環境の構成手順 82
MoM Managerを設定する 82
手順 83
MoMの管理者をセルに追加する 83
前提条件 83
手順 83
セルをインポートする 83
前提条件 83
手順 84
MoMでのHPE Data Protectorサービスを再起動する 84
Data Protectorのサービスを停止する 84
非クラスター環境のCell Managerの場合 84
HPE Serviceguard上のCell Managerの場合 84
Symantec Veritas Cluster Server上のCell Managerの場合 84
Microsoft Cluster Server上のCell Managerの場合 84
Data Protectorのサービスを開始する 84
非クラスター環境のCell Managerの場合 84
HPE Serviceguard上のCell Managerの場合 85
Symantec Veritas Cluster Server上のCell Managerの場合 85
Microsoft Cluster Server上のCell Managerの場合 85
CMMDBを構成する 85
必要な作業 85
前提条件 85
クライアントセルでCMMDBを構成する 85
手順 85
MoM ManagerでCMMDBを構成する 86
手順 86
集中型ライセンスについて 87
集中型ライセンスを設定する 87
前提条件 87
手順 87
集中型ライセンスを無効にする 88
手順 88
MoM環境の管理について 89
セルをエクスポートする 89
手順 89
セル間でクライアントシステムを移動する 89
手順 90
集中型ライセンスを無効にする 90
前提条件 90

手順 90
HPE Data Protectorユーザーの構成 90
手順 91
ユーザーを他のセルに追加する 91
手順 91
ユーザーをセルから削除する 91
手順 91
特定のセル用のデバイスとメディアを管理する 92
手順 92
特定のセルに対して内部データベースを管理する 92
手順 92

第6章: クラスター 93

クラスターについて 93
HPE Data ProtectorのMicrosoft Cluster Server用統合ソフトウェアについて 93
ライセンスとMSCS 93
構成 93
クラスター対応バックアップの管理方法 94
Data Protectorのフェイルオーバー 94
Data Protector以外のアプリケーションのフェイルオーバー 94
Microsoft Cluster Serverのディザスタリカバリについて 95
考えられるシナリオ 95
HPE Data ProtectorのHPE Serviceguard用統合ソフトウェアについて 95
ライセンスとHPE Serviceguard 96
構成 96
HPE Data ProtectorのHACMPクラスター用統合ソフトウェアについて 96
ノード 97
共有外部ディスクインターフェイス 97
ネットワーク 98
クライアント 98
タスク 98

第7章: ホームコンテキスト 99

ダッシュボード 99
テレメトリー 101
テレメトリーの機能 102
スケジューラー 103
以前のバージョンからのスケジュールの移行 103
スケジュール用オプション 105
休日中のスケジュールの除外 105
定義済みスケジュールの使用 106
スケジュール重複の処理 106
異なるタイムゾーンでのスケジュール設定 106
スケジュールの優先順位付け 106

制限事項 107
スケジューラーのユーザーインターフェイス 107
スケジューラーのタスク 109
スケジュールの作成 110
既存のスケジュールの編集 113
スケジュールの表示 115
スケジュールの有効/無効の切り替え 117
手順 117
休日のスケジュールの有効/無効の切り替え 117
手順 117
特定の日時のスケジュールの設定 118
手順 118
定期的なスケジュールの設定 118
定義済みのバックアップスケジュールを使用する 119
手順 119
繰り返しスケジュールの構成 119
手順 119
スケジュール設定のヒント 120

第8章: デバイス 122

バックアップデバイスについて 122
バックアップデバイスとは 122
バックアップデバイスの構成について 122

バックアップデバイスの種類 123
スタンドアロン 123
ディスクへのバックアップデバイス 123
SCSIライブラリ 123
スタッカー 125
マガジンデバイス 125
ジュークボックス 125
スタンドアロンファイルデバイス 125
ファイルライブラリデバイス 125
外部制御 126
ADIC/GRAU DASライブラリ 126
StorageTek ACSライブラリ 127

StoreOnceソフトウェア重複排除コンポーネントについて 129
インストール 129
前提条件 129
ファイアウォールの構成 129
インストール手順 129
StoreOnceソフトウェア重複排除の追加手順 129
Data ProtectorのStoreOnceソフトウェア重複排除コンポーネントのリモートインストール 130
Data ProtectorのStoreOnceソフトウェア重複排除コンポーネントのローカルインストール 130

StoreOnceSoftwareサービス/デーモンの設定 130
インストールディレクトリの構造 131
トラブルシューティング 131
ディスクスペース不足の警告 131
system.dbファイルのバックアップ 132
StoreOnceストアおよびDD Boost重複排除デバイス 134
マルチインターフェイスサポート 135
ソース側重複排除 136
B2Dデバイスの追加 137
バックアップ 137
復元 139
ソース側重複排除に関する注意 140
Catalyst over Fibre Channel用のStoreOnce Catalystクライアント構成 140
Windowsクライアント 140
Linuxクライアント 141
AIXクライアント 142
HP-UXクライアント 142
Solarisクライアント 142
B2Dデバイス関連のOmnircオプション 143
クラウド(Helion)デバイスについて 145
前提条件 145
制限事項 145
推奨事項 146
クラウド(Helion)デバイスの準備 146
クラウド(Azure)デバイスについて 147
前提条件 147
制限事項 148
推奨事項 148
クラウド(Azure)デバイスの準備 149
デバイスのパフォーマンスチューニング 149
ブロックサイズ 149
最適なブロックサイズを特定する 150
制限事項 150
ブロックサイズを変更する 150
デバイスのパフォーマンス 151
新しいデバイスのサポート 151
バックアップデバイスを準備する 152
前提条件 152
手順 152
SAN環境の場合 152
手順 152
ファイルデバイス 153
手順 153
マガジン 153

手順 153
SCSIライブラリ、ジュークボックス、外部制御 153
手順 153
Windowsのロボティクスドライバー 153
手順 154
Windowsシステム上でSCSIアドレスを作成する 154
光磁気デバイス 154
テープデバイス 154
Windowsでネイティブテープドライバーを使用していない場合 154
Windowsでネイティブテープドライバーを使用している場合 155
手順 155
UNIXシステム上でデバイスファイル名を検索する 155
HP-UX上でデバイスファイル名を検索する 155
前提条件 155
手順 155
Solaris上でデバイスファイル名を検索する 156
手順 156
UNIXシステム上でデバイスファイルを作成する 156
HP-UXシステム上でデバイスファイルを作成する 156
前提条件 156
手順 156
Solarisシステム上でデバイスファイルを作成する 157
前提条件 157
手順 157
デバイスファイル名およびSCSIアドレスを自動検出する 158
既存のData Protectorデバイス定義を変更する場合 158
手順 158
新しいData Protectorデバイス定義を作成する場合 158
手順 158
デバイスファイル名およびライブラリ用SCSIアドレスを自動検出する 158
構成済みのライブラリの場合 159
手順 159
ライブラリを構成中の場合 159
手順 159
バックアップデバイスの構成について 159
ライブラリ管理コンソールについて 159
ライブラリ管理コンソールとは 159
Data Protectorでのライブラリ管理コンソールのサポート 160
制限事項 160
バックアップデバイスを自動構成する 160
前提条件 161
デバイスの自動構成 161
手順 161
SAN環境でのデバイスの自動構成 161
制限事項 162
手順 162

スタンドアロンデバイスを構成する 162
手順 163
ディスクへのバックアップデバイスを構成する 163
マルチインターフェイスサポート 164
手順 164
ディスクへのバックアップデバイスを構成する - StoreOnce 165
手順 165
ストアのキャッシュを更新する 167
HPE Data Protector GUIを使用してキャッシュを更新する 167
HPE Data Protector GLIを使用してキャッシュを更新する 167
ディスクへのバックアップデバイスを構成する - StoreOnceソフトウェア 168
重複排除ストアのルートディレクトリの構成 168
ストアの作成 169
ディスクへのバックアップデバイスを構成する - データドメインブースト 170
前提条件 170
制限事項 171
手順 171
AIXシステムでのデータドメインブーストの構成 172
手順 172
ディスクへのバックアップデバイスを構成する - Smart Cache 173
Smart Cacheを構成する 173
前提条件 173
制限事項 173
手順 174
クラウドデバイス(Helion)を構成する 175
HPE Public Cloudプロジェクト名を取得する 175
手順 175
認証サービスURLを取得する 175
手順 175
アクセスキーを作成する 176
手順 176
ディスクへのバックアップデバイスを構成する - クラウド(Helion) 177
手順 177
ディスクへのバックアップデバイスを構成する - クラウド(Azure) 178
手順 178
ファイルライブラリデバイスを構成する 178
前提条件 178
制限事項 178
手順 179
デバイスに対する複数パスの構成について 180
複数のパスを使う理由 180
パスの選択 180
以前のバージョンとの互換性 181
制限事項 182
[デバイス/メディア]の拡張オプションを設定する 182
手順 182

VTLデバイスを構成する 182
手順 182
スタッカーデバイスを構成する 183
手順 183
スタッカーデバイスメディアの管理 184
ジュークボックスデバイス(光磁気ライブラリ)を構成する 184
ジュークボックスデバイスの構成 184
手順 184
ジュークボックスデバイス内のドライブの構成 184
手順 184
SCSIライブラリデバイスまたはマガジンデバイスを構成する 185
SCSIライブラリロボティクスの構成 185
手順 185
ライブラリ内のドライブの構成 186
手順 186
SAN環境でデバイスを構成する 187
考慮事項 187
構成方法 187
GUIを使ったデバイスの自動構成 187
制限事項 187
CLI(sanconfコマンド)を使用したデバイスの自動構成 188
デバイスのロック 189
制限事項 189
推奨事項 189
UNIXシステムでの手動構成 189
構成の段階 189
SAN環境でデバイスを手動で構成する 190
前提条件 190
構成の段階 190
SAN環境内のライブラリの構成 190
手順 190
ライブラリ内のドライブの構成 191
手順 191
SAN環境でlibtabファイルを構成する 192
手順 193
ADIC/GRAU DASライブラリデバイスを構成する 193
構成の段階 193
ライブラリドライブを接続する 194
手順 194
Media Agentのインストールを準備する 194
手順 194
Media Agentのインストール 195
前提条件 195
手順 196
ADIC/GRAU DASライブラリデバイスの構成 197
手順 197

ADIC/GRAU DASライブラリデバイス内のドライブの構成 197
手順 197
StorageTek ACSライブラリデバイスを構成する 198
構成の段階 198
ライブラリドライブを接続する 199
手順 199
Media Agentのインストール 199
前提条件 199
手順 200
StorageTek ACSライブラリデバイスを構成する 201
手順 201
StorageTek ACSライブラリデバイス内のドライブの構成 201
手順 201
バックアップデバイスの使用について 202
[デバイス/メディア]の拡張オプション 202
拡張オプション - 設定 203
オプション 203
拡張オプション - サイズ 203
拡張オプション - その他 203
マウント要求 203
デバイスのロック名 203
複数の種類のドライブを使用するライブラリ 203
同一密度に設定 204
ドライブの種類ごとにメディアプールを設定 204
フリープールサポート 204
スキャンについて 204
スキャンを実行するタイミング 205
制限事項 205
ドライブクリーニング 205
制限事項 206
自動クリーニングの条件 206
スケジュールに基づいたメディアの取り出し 207
デバイスのロック 207
バックアップデバイスを無効化する 208
バックアップデバイスを手動で無効化する 208
手順 208
バックアップデバイスを自動で無効化する 208
バックアップデバイス名を変更する 209
手順 209
バックアップデバイスを削除する 209
手順 209
マウント要求に応答する 210
前提条件 210
手順 210
Storage Area Network (SAN)について 210
SANとは 210

FC-ALおよびLIP 211
SAN環境におけるデバイスのロック 212
Data Protectorによって排他的に使用されるデバイスロックメカニズム 213
複数のアプリケーションで使用されるデバイスロックメカニズム 213
間接ライブラリアクセスと直接ライブラリアクセス 213
間接ライブラリアクセス 213
直接ライブラリアクセス 213
SAN環境でデバイスを構成する 214
考慮事項 214
構成方法 214
GUIを使ったデバイスの自動構成 214
制限事項 214
CLI(sanconfコマンド)を使用したデバイスの自動構成 215
デバイスのロック 216
制限事項 216
推奨事項 216
UNIXシステムでの手動構成 216
構成の段階 216
ディスクへのバックアップについて 217
ディスクベースのバックアップデバイスとは 217
ディスクベースのデバイスの構成方法 217
ディスクへのバックアップデバイスについて 217
重複排除について 218
重複排除を使用するタイミング 219
重複排除の利点 219
重複排除テクノロジ 219
StoreOnceソフトウェア重複排除 219
HPE StoreOnceバックアップシステムデバイス 219
重複排除の設定 220
ソース側重複排除 220
サーバー側重複排除 220
ターゲット側重複排除 220
ファイルライブラリデバイスについて 221
ディスクベースのデバイスの管理方法 221
ファイルデポ 221
ファイルデポの作成 221
ファイルデポ名 221
ファイルデポサイズ 222
ファイルデポのスペース消費 222
満杯ディスクの取り扱い 222
ディスク当たりのデバイス数 222
ファイルライブラリデバイスのプロパティを設定する 222
プロパティの初期設定 222
手順 222
デバイスプロパティを変更する 223
手順 223

ファイルライブラリデバイスを削除する 223
削除の段階 223
データ保護をチェックする 223
手順 223
ファイルデポをリサイクルする 224
手順 224
エクスポート済みのファイルデポのアイコンを削除する 224
手順 224
ファイルライブラリデバイスを削除する 224
手順 224
ジュークボックスデバイスについて 225
ジュークボックス物理デバイス 225
ジュークボックスファイルデバイス 225
WindowsとUnixにおける推奨スロットサイズ 225
ファイルジュークボックスデバイスのメンテナンス方法 226
ファイルジュークボックスデバイスを構成する 226
ファイルジュークボックスデバイスの構成 226
前提条件 226
手順 226
ファイルジュークボックスデバイス内のドライブの構成 227
手順 227
ファイルジュークボックスのスロットをリサイクルする 227
手順 227
スタンドアロンデバイスについて 228
スタンドアロン物理デバイス 228
スタンドアロンファイルデバイス 228
スタンドアロンファイルデバイスを構成する 229
前提条件 229
手順 229

第9章: メディア 230

メディア管理について 230

[デバイス/メディア]ビューをカスタマイズする 230
メディアプールについて 230
フリープール 231
デフォルトのメディアプール 231
フリープールの特性 231
フリープールのプロパティ 231
フリープールを使用するタイミング 231
メディア品質の計算 232
フリープールの制限事項 232
メディアプールのプロパティ 232
[メディアプールプロパティ - 一般] 232
メディアプールプロパティ - 割り当て 232
割り当て 232

メディアプールプロパティ - 状態 233
メディア状態要素 233
メディアプールプロパティ - 使用法 233
メディアプールの品質 233
デバイスエラーとメディア品質 234
メディアプールを作成する 234
手順 234
メディアプールを変更する 235
手順 235
メディアプールを削除する 235
手順 235
メディアのライフサイクル 236
メディアをバックアップ用に準備する 236
メディアのバックアップ用の使用 236
メディアを安全な場所に保管する 236
メディアの廃棄 236
メディアの種類 237
サポートされているメディアの種類 237
メディアの品質 237
デバイスエラーとメディア品質 237
バックアップ用メディアの選択方法 237
メディア割り当てポリシー 238
メディアの事前割り当て 238
メディアの状態 238
メディアの使用方法 238
制限事項 238
メディアの選択に影響する要因 239
各種メディアフォーマットの使用 239
制限事項 240
WORMメディア 240
Data ProtectorでWORMメディアを使用する方法 240
サポートされているWORMメディア 240
メディアのフォーマットについて 240
埋め込みブロックのフォーマット 241
メディアをフォーマットするタイミング 241
メディアラベル 241
認識可能なメディアの形式 241
Data Protectorのメディアフォーマットのカテゴリ 242
メディアをフォーマットする 242
手順 243
マガジン内のすべてのメディアをフォーマットする 243
前提条件 243
手順 243
マガジン内の単一のメディアをフォーマットする 244
前提条件 244
手順 244

ライブラリデバイス内のメディアをフォーマットする 244
手順 244
メディアのインポートについて 245
留意事項 245
メディアをインポートするタイミング 245
メディアをインポートする 245
手順 246
マガジン内のすべてのメディアをインポートする 246
前提条件 246
手順 246
マガジン内の単一のメディアをインポートする 246
前提条件 247
手順 247
ライブラリデバイス内のメディアをインポートする 247
手順 247
暗号化されたバックアップを含むメディアのエクスポートとインポート 248
CMMDBを含まないCell Manager環境またはMoM環境 248
手順 248
CMMDBを含むMoM環境 248
手順 248
メディアのコピーについて 249
前提条件 249
制限事項 249
メディアをコピーするタイミング 249
どのような結果が得られるか 250
コピーからの復元 250
メディアをコピーする 250
スタンドアロンデバイスのメディアをコピーする 250
手順 250
ライブラリデバイスのメディアをコピーする 251
メディアの自動コピー 251
制限事項 251
メディアの自動コピー 252
メディアの自動コピーの種類 252
ポストバックアップのメディアコピー 252
スケジュール設定されたメディアコピー 252
ポストバックアップのメディアコピーを構成する 253
制限事項 253
手順 253
スケジュール設定されたメディアコピーを構成する 253
制限事項 253
手順 253
デバイスをスキャンする 254
手順 254
ライブラリデバイス内のメディアをスキャンする 254
手順 254

ライブラリデバイス内のドライブをスキャンする 255
手順 255
バーコードリーダーサポートをアクティブ化する 255
手順 256
ライブラリデバイスをバーコードスキャンする 256
前提条件 256
手順 256
メディアを検索/選択する 256
メディアプール内のメディアを検索/選択する 256
手順 256
ライブラリデバイス内のメディアを検索/選択する 257
手順 257
[メディアのリスト]レポートを使ってメディアを検索する 257
手順 257
バックアップ用メディアの事前割り当てリスト 257
バックアップ用のメディアを事前に割り当てる 257
手順 258
メディアをリサイクルする 258
手順 258
メディアからカタログをインポートする 259
手順 259
メディアを検証する 259
スタンドアロンデバイスのメディアを検証する 260
手順 260
ライブラリデバイスのメディアを検証する 260
手順 260
メディアを移動する 260
手順 261
メディアをエクスポートする 261
手順 261
MCFファイルにカタログメディアデータをコピーする 262
制限事項 262
推奨事項 262
手順 262
MCFファイルからカタログメディアデータをインポートする 263
前提条件 263
制限事項 263
手順 263
メディアの説明を変更する 263
手順 264
メディアの収納場所情報を変更する 264
手順 264
収納場所のリストを作成する 264
手順 264
メディアの位置の優先順位を設定する 265
手順 265

メディアをボールティングする 265
前提条件 265
手順 266
メディアを消去する 266
手順 266
書き込み保護メディアの検出 266
マウント要求について 267
ライブラリ固有のメディア管理について 267
他のアプリケーションによるライブラリメディアの使用 267
ADIC/GRAU DASライブラリまたはSTK ACSライブラリを使用した場合のHPE Data Protectorの照会処理について 268
スロットを追加する 268
手順 268
スロットを削除する 269
手順 269
メディアを挿入する 269
手順 270
メディアを取り出す 270
メディアの一括取り出し 270
メディアの取り出しの事前定義 270
手順 270
ライブラリデバイス内のメディアを消去する 271
手順 271
VOLSERを手動で追加する 271
手順 271
ADIC/GRAU DASホストおよびStorageTek ACSLMホストを照会する 272
制限事項 272
手順 272

第10章: バックアップ 273

バックアップについて 273

バックアップビューを設定する 273
手順 273

バックアップの種類 274
フルバックアップ 274
増分バックアップ 274
増分バックアップの種類 274
拡張バックアップソリューション 275
フルバックアップと増分バックアップ 275
従来の増分バックアップ 275
従来の増分バックアップの仕組み 275
変更の検出 276
拡張増分バックアップ 276
拡張増分バックアップの利点 277
ディスクスペース消費に対する影響 277

制限事項 278
Change Log Providerを使用した増分バックアップ 278
前提条件 278
パフォーマンスとディスクスペース消費 279
考慮事項 279
制限事項 280
合成バックアップ 280
合成バックアップの実行方法 280
仮想フルバックアップ 281
標準バックアップ手順 281
前提条件 281
ファイルシステムのバックアップ 282
バックアップ仕様を作成する 282
制限事項 282
手順 282
バックアップ仕様を修正する 283
手順 284
バックアップをプレビューして開始する 284
制限事項 284
手順 284
バックアップを中止する 285
手順 285
失敗したバックアップを再開する 285
前提条件 285
考慮事項 285
制限事項 286
手順 286
バックアップ仕様をコピーする 286
手順 286
バックアップ仕様を削除する 287
手順 287
拡張バックアップタスク 287
前提条件 287
拡張バックアップタスクとは 287
バックアップ対象となるネットワーク共有ディスクを選択する 288
前提条件 288
Windows Vista、Windows 7、Windows 8、Windows Server 2008、および Windows Server 2012の場合 288
要件 288
制限事項 289
手順 289
条件に一致するファイルだけをバックアップ対象として選択する 290
手順 290
バックアップ対象から除外するファイルを指定する 291
手順 291
バックアップを開始するためのショートカットの位置を選択する 291

制限事項 291
手順 291
複数のDisk Agentを使用してバックアップを実行する 292
手順 292
小サイズの繰り返しバックアップを処理する 293
ディスクイメージバックアップ 293
どのような場合にディスクイメージバックアップを使用するか 294
ディスクイメージセクションの指定方法 294
UNIXシステムの場合 294
Windowsシステムの場合 294
ディスクイメージセクションの場所 294
UNIXシステムの場合 294
Windowsシステムの場合 294
ディスクディスカバリによるクライアントバックアップ 295
どのような場合にディスクディスカバリを使用するか 296
バックアップ仕様 296
Webサーバーのバックアップ 296
Wake ONLANサポートを有効にする 297
手順 297
バックアップテンプレートについて 297
バックアップテンプレートを新規作成する 298
手順 298
バックアップテンプレートを修正する 299
手順 299
バックアップテンプレートをコピーする 299
手順 299
バックアップテンプレートを削除する 299
手順 299
バックアップテンプレートをバックアップ仕様に適用する 300
手順 300
バックアップオプションについて 300
利用可能なバックアップオプション 301
バックアップ仕様オプション 301
ファイルシステムオプション 301
ディスクイメージオプション 301
デバイスオプション 302
スケジュール用オプション 302
使用頻度の高いオプション 302
対話式バックアップ 302
保存済みのバックアップ仕様によるバックアップ 302
スケジュールバックアップ 303
カタログ保護の期限切れ 303
カタログ保護とバックアップ 303
カタログ保護と復元 303
ロギングレベルとバックアップ速度 304
ロギングレベルと復元時のブラウズ 304

ロギングレベルと復元速度 304
バックアップセッションオーナーとは 305
なぜバックアップオーナーを変更するか 306
誰がプライベートオブジェクトを復元できるか 306
バックアップ仕様オプション 306
一般的なバックアップ仕様オプション 306
クラスター化に関するバックアップ仕様オプション 307
セッションの自動再起動 307
セッションパラメーターの破棄とIDパラメーターの破棄 307
EMC Symmetrixに関するバックアップ仕様オプション 307
クライアントシステム 307
ミラーの種類 307
EMC Symmetrixでの実行前と実行後の分割 307
EMC Symmetrixオプション 308
HPE P9000 XPディスクアレイファミリバックアップ仕様オプション 308
クライアントシステム 308
ミラーの種類 308
複製管理オプション 308
セッションの開始時 308
セッションの終了時 308
アプリケーションシステムオプション 308
バックアップシステムオプション 309
HPE P6000 EVAディスクアレイファミリバックアップ仕様オプション 309
クライアントシステム 309
複製モード 309
フェイルオーバーシナリオにおける複製処理 309
スナップショット管理オプション 309
ミラークローンの準備/同期 309
複製管理オプション 310
アプリケーションシステムオプション 310
バックアップシステムオプション 310
ファイルシステムオプション 310
ファイルシステムオプション 310
その他のファイルシステムオプション 311
WinFSファイルシステムオプション 311
ディスクイメージオプション 312
デバイスオプション 312
デバイスのプロパティ - 一般 312
スケジュール用オプション 313
セッションオプション 313
スプリットミラー/スナップショットのバックアップ 313
バックアップオプションの設定 313
手順 314
データ保護を指定する 314
バックアップ仕様レベルでデータ保護を指定する 314
手順 314

個々のバックアップオブジェクトに対してデータ保護を指定する 315
手順 315
スケジュールバックアップに対してデータ保護を指定する 315
CLIを通じてデータ保護を指定する 315
手順 315
特定のオブジェクトのオプションを変更する 316
手順 316
バックアップデバイスオプションを変更する 316
手順 317
スケジュールバックアップオプションを設定する 317
実行前/実行後コマンドについて 318
実行前/実行後コマンドとは 318
バックアップ用の実行前/実行後コマンドの構成 318
バックアップ仕様 318
バックアップオブジェクト 318
実行前/実行後コマンドの実行方法 318
バックアップ仕様を対象とする実行前/実行後コマンド 319
実行前/実行後コマンドの特徴 319
セキュリティを確保するためのコマンドの起動と場所 319
Windowsシステム 319
UNIXシステム 319
環境変数 320
SMEXIT値 320
実行前/実行後コマンドに関する留意事項 320
バックアップ仕様を対象とする実行前/実行後コマンドを指定する 322
特定のバックアップオブジェクトを対象とする実行前/実行後コマンド 322
コマンドの起動と場所 322
環境変数 323
実行前/実行後コマンドに関する留意事項 323
セキュリティの留意事項 324
バックアップオブジェクトを対象とする実行前/実行後コマンドを指定する 325
すべてのバックアップオブジェクトを対象とする実行前/実行後コマンドを指定する 325
個々のバックアップオブジェクトを対象とする実行前/実行後コマンドを指定する 325
統合ソフトウェアを対象とする実行前/実行後コマンドを指定する 326
バックアップスケジュールについて 326
複数のバックアップを連続して実行する 326
手順 326
バックアップ仕様グループについて 327
バックアップ仕様グループの例 327
バックアップ仕様グループを表示する 328
手順 328
バックアップ仕様グループを作成する 328
手順 328
バックアップ仕様をグループに保存する 328
手順 328
バックアップ仕様またはテンプレートをグループ間で移動する 329

手順 329
バックアップ仕様グループを削除する 329
手順 329
Windowsシステムのバックアップについて 330
制限事項 330
バックアップの対象となるデータ 330
Windows Server 2012 330
Windows固有の情報 330
バックアップの対象外のデータ 330
Windows Vista、Windows 7、Windows 8、Windows Server 2008、および Windows Server 2012の場合: 331
Windows Server 2012 331
その他のWindowsシステム 331
NTFS 3.1ファイルシステムの機能 331
再解析ポイント 332
スパースファイル 332
システムディスクをバックアップする際の注意事項 332
構成データのバックアップ(Windows) 333
制限事項 333
Windowsの構成オブジェクト 333
Active Directory 334
DFS 334
DHCPおよびWINS 334
プロファイル 334
リムーバブル記憶域の管理データベース 335
ターミナルサービスデータベース 335
Windowsサービス 335
システム状態データのバックアップ 335
リモートストレージサービス 336
リモートストレージサービス: 336
リモート記憶域データベース: 336
リムーバブル記憶域の管理データベース 337
ファイルシステム保護 337
UNIXシステムのバックアップについて 337
制限事項 337
バックアップの対象となるデータ 337
UNIXファイルシステムのバックアップから除外するべきデータ 338
NFSのバックアップ 338
どのような場合にNFSバックアップを使用するか 338
制限事項 338
前提条件 339
制限事項 339
バックアップの対象となるデータ 340
Novell Open Enterprise Server (OES)のバックアップについて 340
前提条件 340
制限事項 341

圧縮ファイルのバックアップおよび復元 341
バックアップの対象となるデータ 341
Novell OESを構成する 341
HPLOGINユーティリティを使用してユーザー名とパスワードを保存する 341
手順 341
ファイルシステム用Target Service Agent(TSAFS)をデュアルモードでロードする 341
手順 341
Novellディレクトリサービス用Target Service Agent(TSANDS)をロードする 342
手順 342
ファイルシステム用GroupWise Target Service Agent(TSAFSGW)をロードする 342
手順 343
バックアップのパフォーマンスについて 343
インフラストラクチャー 343
オブジェクトのミラーリングとバックアップパフォーマンス 344
デバイス以外の高パフォーマンスハードウェア 344
ハードウェアの並列処理 344
同時処理数 345
パフォーマンスへの影響 345
多重データストリーム 345
デバイスストリーミング 345
デバイスストリーミングの構成方法 346
ブロックサイズ 346
セグメントサイズ 346
Disk Agentのバッファー数 347
ソフトウェア圧縮 347
ハードウェア圧縮 348
ディスクイメージバックアップとファイルシステムバックアップ 348
メディアに対するオブジェクトの分配 349
ファイルシステムスキャン 349
パフォーマンスに関するさまざまなヒント 350

第11章: オブジェクト集約 351

オブジェクト集約について 351
オブジェクト集約の種類 351
ポストバックアップのオブジェクト集約 351
スケジュール済みのオブジェクト集約 351

オブジェクトの集約方法 351
デバイスの選択 351
オブジェクト集約のオプション 352
メディアセットの選択 352
集約されたオブジェクトの所有権 352

標準オブジェクト集約タスク 352
前提条件 352
制限事項 353

オブジェクトを対話型に集約する 353
手順 353
ポストバックアップのオブジェクト集約を構成する 354
手順 354
オブジェクト集約のスケジュールを設定する 355
手順 355
オブジェクト集約仕様をコピーする 356
手順 356

第12章: コピー 357
バックアップデータの複製について 357
オブジェクトコピーについて 358
オブジェクトコピーとは 358
オブジェクトの自動コピー 358
ポストバックアップのオブジェクトコピー 359
スケジュール設定されたオブジェクトコピー 359
オブジェクトのコピー方法 359
デバイスの選択 359
オブジェクトコピーのオプション 360
コピー元のメディアセットの選択 360
オブジェクトコピーの完了ステータス 360
オブジェクトのコピー 360
ソースオブジェクト 360
オブジェクトコピーの所有権 361
標準オブジェクトコピータスク 361
前提条件 361
制限事項 361
オブジェクトを対話式にコピーする 362
手順 362
ポストバックアップのオブジェクトコピーを構成する 363
手順 363
オブジェクトコピーのスケジュールを設定する 364
手順 364
失敗したオブジェクトコピーセッションを再開する 365
前提条件 365
制限事項 365
手順 365
オブジェクトコピー仕様をコピーする 366
手順 366
拡張オブジェクトコピータスク 366
メディアを解放する 367
手順 367
メディアを逆多重化する 367
制限事項 368

手順 368
復元チェーンを集約する 369
制限事項 369
手順 369
別のメディアの種類に移行する 370
手順 370
ディスクステージングについて 370
ディスクステージングとは 370
ディスクステージングを実行する理由 371
ディスクステージングと小規模バックアップの繰り返し 371
オブジェクト操作セッションのトラブルシューティング 371
オブジェクトコピーに関する問題 371
コピーされたオブジェクトの数が想定された数より少ない 371
選択したライブラリ内の一部のオブジェクトしかコピーされない 372
追加のメディアに対するマウント要求が発行される 372
オブジェクトコピーを作成したときに、保護の終了時間が延長される 372
複数のオブジェクトを含むセッションを複製すると、応答が停止する 373
データドメインブーストデバイス上の複製セッションが再試行期間中に中止操作に応答できない 373
オブジェクト集約に関する問題 374
多くの時点のオブジェクト集約を行うと、上限を超える数のファイルが開かれる 374
B2Dデバイスへのオブジェクト集約が2回目の試行で失敗した 374
複製について 375
自動複製 375
ポストバックアップ複製 375
スケジュール設定した複製 376
制限事項 376
考慮事項 376
複製を使用可能にする方法 376
自動複製同期 376
前提条件 376
考慮事項 377
制限事項 377
外部のCell Managerのインポート 377
オブジェクトコピーセッションの実行 378
オブジェクトのミラーリングについて 379
オブジェクトのミラーリングの利点 379
制限事項 379
オブジェクトのミラーリングの使用方法 379
メディアをコピーする 380
スタンドアロンデバイスのメディアをコピーする 380
手順 380
ライブラリデバイスのメディアをコピーする 380

第13章: オブジェクト検証 382

オブジェクト検証について 382
データ検証 382
ホストへの送信 382
オブジェクト検証セッションの種類 382
ポストバックアップのオブジェクト検証 382
スケジュールされたオブジェクト検証 382
オブジェクトの検証方法 383
オブジェクトの選択 383
自動処理 383
対話型操作 383
ソースデバイスの選択 383
ターゲットホストの選択 383
スケジュール設定 383
標準オブジェクト検証タスク 384
前提条件 384
制限事項 384
オブジェクトを対話型で検証する 384
手順 385
ポストバックアップのオブジェクト検証を構成する 386
手順 386
スケジュール済みのオブジェクト検証を構成する 387
手順 387
オブジェクト検証環境をカスタマイズする 388

第14章: 復元 389

復元について 389
標準復元手順 389
前提条件 389
復元対象のデータを選択する 389
前提条件 390
バックアップオブジェクトのリストからデータを選択する 390
手順 390
バックアップセッションのリストからデータを選択する 390
制限事項 390
手順 390
特定のバックアップバージョンを選択する 391
ファイルまたはディレクトリ別にバックアップバージョンを選択する 391
手順 391
複数のファイルまたはディレクトリで同時にバックアップバージョンを選択する 391
手順 391
ファイルの重複を処理する 392
手順 392
復元に使用するデバイスを選択する 392

手順 393
復元に必要なメディアを検索する 393
制限事項 393
手順 394
復元をプレビューして開始する 394
前提条件 394
制限事項 394
手順 394
復元を中止する 395
手順 395
復元先オプション 395
復元先を選択する 395
手順 395
個々のファイルとディレクトリに対して復元先を指定する 396
復元先を指定して復元 396
手順 396
別名で復元 396
手順 397
失敗したセッションの再開について 397
ファイルシステムのバックアップセッション 398
制限事項 398
ファイルシステムの復元セッション 398
機能の動作方法 399
考慮事項 399
制限事項 399
Data Protector Oracle Server統合バックアップおよび復元セッション 400
失敗したセッションを再開する 400
前提条件 400
手順 400
拡張復元タスク 400
前提条件 400
拡張復元タスク 401
復元対象から除外するファイルを指定する 401
手順 401
条件に一致するファイルだけを復元対象として選択する 402
手順 402
開いているファイルを復元対象に指定する 402
手順 402
復元中のファイルへのアクセスを拒否する 403
手順 403
復元対象のファイルを検索する 403
手順 403
Windowsの共有ディスクを復元対象に指定する 404
前提条件 404
手順 404
複数のオブジェクトを並行して復元する 405

前提条件 405
制限事項 405
手順 405
ディスクイメージの復元 405
前提条件 406
保管場所に移動したメディアからデータを復元する 406
Webサーバーの復元 406
ブラウズなしの復元 406
オブジェクト全体を復元して必要な部分を抽出する 407
前提条件 407
手順 407
[復元のみ]オプションを使ってバックアップオブジェクトの一部を復元する 407
前提条件 408
手順 408
ファイルまたはディレクトリを手作業で復元する 408
前提条件 408
手順 409
復元オプション 409
全般的な復元オプション 409
実行前/実行後コマンド 411
デバイスの選択 411
ファイルの重複を処理する 412
Active Directory固有のオプション 412
複製モード 412
復元オプションを設定する 412
手順 413
Windowsシステムの復元について 413
NTFS 3.1ファイルシステムの機能 413
共有ディスクとしてバックアップされたオブジェクトの復元 414
Windowsファイルシステムの復元に対する制限事項 414
構成データの復元 415
制限事項 415
Windowsの構成オブジェクト 415
Active Directory 416
DFS 417
プロファイル 417
レジストリ 418
リムーバブル記憶域マネージャー データベース 418
サーバー構成オブジェクト 418
SysVol 418
Windows TCP/IPサービス 418
システム状態データの復元 419
リモートストレージサービス 419
ファイルシステム保護 420
UNIXシステムの復元について 420
UNIXシステム固有の情報 420

HP OpenVMSシステムの復元について 420
制限事項 420
復元されるファイルシステム情報 421

第15章: モニター、レポート、通知、Data Protectorイベントログ 423
監視について 423
現在実行中のセッションを表示する 423
前提条件 423
手順 423
終了したセッションを表示する 424
前提条件 424
手順 424
実行中のセッションを中止する 424
前提条件 424
手順 425
レポートについて 425
機能 426
レポートの形式 426
レポートの種類 426
構成レポート 426
セル情報 426
クライアントバックアップ 427
Data Protector向けに構成されていないクライアント 428
Data Protectorが使用していない構成済みクライアント 428
Data Protectorが使用していない構成済みデバイス 428
ライセンス 429
スケジュールのチェック 429
IDBレポート 429
IDBサイズ 429
メディアとメディアプールに関するレポート 430
メディアの拡張リスト 430
メディアのリスト 430
プールのリスト 431
メディア統計 431
セッション仕様の使用法に関するレポート 432
バックアップオブジェクトの平均サイズ 432
バックアップに関して構成されていないファイルシステム 432
オブジェクトの最新バックアップ 433
バックアップを持たないオブジェクト 433
セッション仕様情報 434
セッション仕様スケジュール 434
バックアップ仕様のツリー 434
時間枠内のセッションに関するレポート 435
クライアント統計 435
デバイスフロー 435
使用メディアの拡張レポート 436

セッションのリスト 436
オブジェクトコピー 436
使用メディアに関するレポート 437
セッションエラー 437
セッションフロー 438
セッション統計 438
単一セッションレポート 438
セッションデバイス 439
セッションメディア 439
セッションオブジェクトコピー 439
セッションオブジェクト 440
クライアントごとのセッション 440
単一セッション 441
レポートの送信方法 441
ブロードキャストメッセージによる送信 441
電子メールによる送信 441
Windowsシステムの場合 442
UNIXシステムの場合 442
電子メール(SMTP)による送信 442
Windowsシステムの場合 442
UNIXシステムの場合 442
外部スクリプトによる送信 443
ログファイルによる送信 443
SNMPによる送信 443
Windowsシステムの場合 443
UNIXシステムの場合 443
HPE Data Protector GUIを使ってレポートグループを構成する 443
前提条件 444
構成の段階 444
レポートグループを構成する 444
手順 444
レポートをレポートグループに追加する 445
手順 445
HPE Data Protector GUIを使ってレポートグループを実行する 445
前提条件 445
手順 445
HPE Data Protector GUIを使って個々のレポートを実行する 446
前提条件 446
手順 446
HPE Data Protector CLIを使ってレポートおよびレポートグループを実行する 446
前提条件 446
手順 447
新しいメールプロファイルを作成する 447
手順 447
Windows SNMPトラップを構成する 447
手順 447

通知について 448
通知の種類 - 通知をトリガーするイベント 449
警告 449
期限切れ証明書 449
Csa Start Sessionの失敗 450
デバイスエラー 450
セッションの完了 450
ファイルライブラリのディスクの使用状況 450
健全性チェックの失敗 451
IDBのバックアップ必要 451
IDBの破損 451
IDBの制限 452
IDBの再構成必要 452
IDBのスペース不足 452
ライセンス警告 453
ライセンス期限切れ 453
メールスロット満量 453
マウント要求 454
フリーメディア不足 454
セッションエラー 454
セッションの開始 455
セッションが多すぎる 455
予期しないイベント 455
UNIX Media Agentのチェック 456
ユーザーチェックの失敗 456
通知の送信方法 456
ブロードキャストメッセージによる送信 456
電子メールによる送信 457
Windowsシステムの場合 457
UNIXシステムの場合 457
電子メール(SMTP)による送信 457
外部スクリプトによる送信 457
ログファイルによる送信 458
Data Protectorイベントログによる送信 458
SNMPによる送信 458
Windowsシステムの場合 458
UNIXシステムの場合 458
レポートグループによる送信 458
通知を構成する 459
前提条件 459
手順 459
HPE Data Protectorイベントログについて 459
処理によって発生するイベント 460
ユーザーが発生させるイベント 460
イベントログビューアーにアクセスする 460
前提条件 460

手順 461
イベントログビューアーの表示内容を削除する 461
前提条件 461
手順 461
監査について 461
監査レポートを生成する 461
手順 462
Data Protectorが正常に機能していることのチェック 462
Data Protectorが実行するチェック 462
保守タスク 462
チェック 463
ユーザーが実行するチェックについて 463
チェックを自動化する方法 465

HPE Data Protectorのドキュメント 466
ドキュメントマップ 466
略称 466
統合 469

フィードバックを送信 471

第1章: 概要

Data Protectorについて

HPE Data Protectorは、急速に増加するビジネスデータに対して信頼性の高いデータ保護と優れたアクセス容易性を提供する、バックアップソリューションです。Data Protectorは、特に全社レベルでの管理作業や分散環境に適した、包括的なバックアップ機能および復元機能を提供します。

Data Protectorの主な特長

- スケーラビリティと柔軟性に優れたアーキテクチャー
- 混在環境のサポート
- 集中管理の容易さ
- 高パフォーマンスのバックアップ
- 復元の容易さ
- データおよび制御通信のセキュリティ
- 高可用性のサポート
- 操作の自動化や無人化
- モニター、レポート、通知
- サービス管理
- オンラインデータベースアプリケーションとの統合
- 他の製品との統合

HPE Data Protectorアーキテクチャー

Data Protectorは、単一のシステムを使用する環境から、複数のサイト上に何千ものシステムが存在するような環境に至るまで、さまざまな状況で使用できます。Data Protectorセルが基本的な管理単位となります。

Data Protectorセルは、1つのCell Managerシステム、1つまたは複数のインストールサーバー、複数のクライアントとデバイスで構成されるネットワーク環境です。

Cell Managerとインストールサーバーは、デフォルトでは同じシステムにインストールされますが、必要に応じて別々のシステムにインストールすることもできます。

Cell Manager

Cell Managerは、Data Protectorセルを集中的に制御するメインシステムです。このシステムには、Data Protectorコアソフトウェアおよび IDBがインストールされます。Cell Managerでは、セッションマネージャーが実行されます。セッションマネージャーは、バックアップセッションおよび復元セッションを制御し、セッション情報をIDBに書

き込みます。IDBには、バックアップしたファイルに関する情報とData Protectorセルの構成に関する情報が記録されます。

インストールサーバー

インストールサーバーシステムは、Data Protectorソフトウェアレポジトリを維持するコンピューターです。UNIX環境とWindows環境の両方にネットワーク経由のリモートインストールを実行して、セル内のシステムにソフトウェアコンポーネントを配布するには、UNIX用とWindows用のインストールサーバーをそれぞれ1つ以上用意する必要があります。

クライアントシステム

Cell ManagerシステムにData Protectorソフトウェアをインストールし終えたら、セル内のすべてのシステムにData Protectorコンポーネントをインストールすることができます。これらのシステムは、Data Protectorクライアントとなります。各クライアントの役割は、そのクライアントにインストールしたData Protectorソフトウェアによって決まります。

バックアップ対象のシステム

バックアップ対象のクライアントシステムには、Data Protector Disk Agent (DA)をインストールしておく必要があります(DAは、バックアップエージェントとも呼ばれます)。Disk Agentは、システム上のディスクからデータを読み取ってMedia Agentに渡したり、Media Agentから受け取ったデータをディスクに書き込んだりする働きをします。Cell ManagerにもDisk Agentがインストールされます。これにより、Cell Manager上のデータ、Data Protector構成情報、およびIDBをバックアップできます。

バックアップデバイスが接続されているシステム

バックアップデバイスが接続されているクライアントシステムには、Data Protector Media Agent(MA)をインストールしておく必要があります。Media Agentは、デバイス内のメディアに対してデータの読み書きを行うか、またはDisk Agentからデータを受け取ります。バックアップデバイスは、Cell Managerだけではなく、任意のシステムに接続できます。バックアップデバイスが接続されているクライアントシステムは、ドライブサーバーとも呼ばれます。複数のバックアップデバイスが接続されているクライアントシステムは、マルチドライブサーバーと呼ばれます。

HPE Data Protectorセットアップ作業の概要

Data Protectorの構成は容易ですが、高度なプランニングを多少行えば、環境の構成とバックアップの最適化に役立ちます。このセクションでは、バックアップ環境をセットアップするためのグローバルタスクについて概説します。

環境の規模と複雑さによっては、以下の手順のすべてが必要とはならないことがあります。

手順

1. ネットワーク構造と編成構造を分析します。どのシステムのバックアップが必要であるかを判断します。詳細については、『*HPE Data Protectorコンセプトガイド*』を参照してください。
2. Microsoft Exchange Server、Microsoft SQL Server、Oracle Server、SAP R/3など、バックアップしたい具体的なアプリケーションやデータベースがあるかどうかをチェックします。Data Protectorには、これらの製品に特化した統合機能が備わっています。

   統合の構成方法については、『*HPE Data Protectorインテグレーションガイド*』を参照してください。
3. Data Protectorセルの構成について、以下のような点を決定します。
   - Cell Managerになるシステム
   - ユーザーインターフェイスのインストール先システム
   - ローカルバックアップまたはネットワークバックアップ
   - バックアップデバイスおよびライブラリを制御するシステム
   - LANとSANのいずれか一方または両方
4. 決定したセットアップ方法に合わせて、必要なData Protectorライセンスを購入します。この結果、インストールに必要なパスワードを取得できます。

   別のやり方として、一時パスワードを使用してData Protectorを操作することも可能です。ただし、このパスワードはインストール後60日間のみ有効です。『*HPE Data Protectorインストールガイド*』を参照してください。
5. セキュリティ面について考慮します。
   - セキュリティ留意事項を分析します。『*HPE Data Protectorインストールガイド*』を参照してください。
   - どのユーザーグループを構成する必要があるかを考慮します。
   - 暗号化形式のメディアにデータを書き込んでセキュリティを強化します。
6. バックアップの構造について決定します。
   - どのメディアプールをどのように使用するか。
   - どのデバイスをどのように使用するか。
   - 各バックアップデータのコピーはそれぞれいくつ必要か。
   - バックアップ仕様はいくつ必要で、それらをどのようにグループ化するか。
   - ディスクへのバックアップを計画している場合、合成バックアップやディスクステージングなどのアドバンストバックアップ戦略を検討する。
7. Data Protector Cell Managerとインストールサーバーをインストールします。次に、Data Protector GUIを使用して、他のシステムにData Protectorのエージェントを配布します。詳細については、『*HPE Data Protectorインストールガイド*』を参照してください。

8. バックアップデバイスを構成します。
9. メディアプールを構成し、メディアを用意します。
10. バックアップ仕様を作成します。IDB用のバックアップ仕様も必要です。
11. 必要に応じ、レポートを構成します。
12. ディザスタリカバリの準備をします。ディザスタリカバリの詳細については、『*HPE Data Protectorディザスタリカバリガイド*』を参照してください。
13. 次のような作業について、その方法を確認しておきます。
    - 失敗したバックアップの処理
    - 復元処理の実行
    - バックアップデータとメディアのボールティングを複製する
    - ディザスタリカバリをテストする
    - IDBの保守

HPE Data Protectorの操作

バックアップタスクと復元タスクは、セッション内で完了します。複数のセッションを同時に実行できます。同時に実行できるセッションの最大数は、Cell Managerの構成(プロセッサー速度、メインメモリサイズ、ディスクスペース)など、セル内のリソースによって異なります。

バックアップセッション

バックアップセッションは、データをクライアントシステムからメディアにバックアップするプロセスです。バックアップセッションは常にCell Managerシステム上で実行されます。バックアップセッションはバックアップ仕様に基づいて、オペレーターによって対話的に起動されるか、Data Protectorスケジューラーによって(無人で)起動されます。

復元セッション

復元セッションは、データを既存のバックアップからディスクに復元するプロセスです。復元セッションは、オペレーターがData Protectorユーザーインターフェイスを使って対話式に開始します。

実行前コマンドと実行後コマンド

実行前コマンドにより、バックアップまたは復元セッションの前に特定の処理を実行できます。実行後コマンドでは、バックアップセッションまたは復元セッションの完了後に特定の処理を実行できます。

実行前コマンドおよび実行後コマンドは、バックアップ仕様の一部として設定できます。この場合は、Cell Managerシステム上で実行されます。また、バックアップオブジェクトオプションとして指定することもできます。この場合は、Disk Agentが稼動しているクライアントシステム上で実行されます。

実行可能ファイルまたはバッチファイル(Windowsシステム)か、シェルスクリプト(UNIXシステム)を実行前コマンドおよび実行後スクリプトコマンドとして使用できます。Data Protectorには、このようなシェルスクリプトは用意されていません。バックアップオペレーターなどが自分でスクリプトを作成する必要があります。

オブジェクトコピー、オブジェクト集約、およびオブジェクト検証セッション

オブジェクトコピーセッションは、オブジェクトコピー仕様に基づきます。オブジェクト集約セッションは、オブジェクト集約仕様に基づきます。いずれのセッションも、対話形式で開始することも、自動的に開始させることもできます。

オブジェクト検証セッションは、オブジェクト検証仕様に基づきます。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のデータ整合性と、オブジェクトを必要な位置に配布する機能をチェックします。セッションは、対話形式で開始することも、自動的に開始することもできます。

ユーザーインターフェイス

Data Protectorには、グラフィカルユーザーインターフェイス(GUI)とコマンドラインインターフェイス(CLI)があります。

グラフィカルユーザーインターフェイス

Windowsシステム用のグラフィカルユーザーインターフェイスが用意されています。

Data Protectorのグラフィカルユーザーインターフェイスでは、単一のシステムからバックアップ環境全体を集中的に管理できます。複数のバックアップ環境を単一のシステムから管理することも可能です。このData Protectorアーキテクチャーにより、Data Protectorユーザーインターフェイスのインストールや使用に対する柔軟性が得られます。ユーザーインターフェイスは、Cell Managerシステムから使用する必要はありません。デスクトップシステム上にインストールすることができます。

GUIはさまざまなシステムにインストールできるので、複数の管理者が自分のローカルコンソールからData Protectorにアクセスすることが可能です。Data Protector GUIをクライアントシステム上で使用するには、そのシステムのユーザーをCell Manager上の適切なData Protectorユーザーグループに追加する必要があります。

ファイル名およびセッションメッセージに含まれている各国語文字を表示するには、特別なセットアップと構成を行う必要があります。

Data Protector 10.00 GUIの以前のバージョンは、Data Protector 10.00 Cell Managerとは互換性がありません。

コマンドラインインターフェイス

グラフィカルユーザーインターフェイスに加え、WindowsシステムおよびUNIXシステム用のコマンドラインインターフェイスが用意されています。コマンドラインインターフェイス(CLI)では、UNIX標準形式のコマンドおよ

びオプションを使って、Data Protectorの全機能にアクセスできます。これらのコマンドを使ってスクリプトを作成すれば、実行頻度の高いタスクを効率化できます。

omniintro manページには、サポートされているData Protectorコマンドすべて、およびUNIXプラットフォームとWindowsプラットフォームにおけるコマンドの違いが記載されています。詳細については、『*HPE Data Protector Command Line Interface Reference*』を参照してください。

GUIで言語設定をカスタマイズする

異種混合環境(1つのセルにロケールが異なる複数のオペレーティングシステムが含まれる環境)でのファイル名の扱いは、非常に複雑です。あるロケール設定でバックアップされたファイル名を別のロケール設定を使って表示または復元する場合、正しく表示するためには特別な設定を行う必要があります。

前提条件

GUIシステムには、次の前提条件が適用されます。

- 選択した文字コードセットに必要なフォントをData Protector GUIシステムにインストールします。たとえば、ヨーロッパ言語のシステムで稼動しているGUIに日本語文字を表示するには、日本語フォントをインストールします。

制限事項

- WindowsオペレーティングシステムとUNIXオペレーティングシステムでは、文字コード変換の実装が若干異なります。Data Protector GUIを実行しているプラットフォームと、構成中のクライアントのプラットフォームが異なると、一部の文字が正しくマッピングされないことがあります。ただし、正しく表示されない文字は少数なので、バックアップまたは復元には影響しません。

手順

1. コンテキストリストで、**[バックアップ]**、**[モニター]**、**[復元]**、**[レポート]**、または**[内部データベース]**をクリックします。
2. [表示]メニューの**[エンコード]**をクリックします。
3. バックアップファイルの作成元のシステムで使用されていた文字コードを選択します。

HPE Data Protector GUIを起動する

WindowsシステムでData Protector GUIを起動する手順は、次のとおりです。

[スタート] > **[プログラム]** > **[HPE Data Protector]** > **[Data Protector Manager]**

managerコマンドを実行する方法もあります。

接続するCell Managerを指定するには、次のコマンドを実行します。

```
manager -server Cell_ Manager_name
```

このコマンドのコンテキスト固有オプションにより、1つまたは複数のData Protectorコンテキストを起動することができます。Data Protector[バックアップ]コンテキストと[復元]コンテキストを起動するには、次のコマンドを実行します。

```
manager -backup -restore
```

これらのコマンドの詳細については、`omnigui` manページまたは『*HPE Data Protector Command Line Interface Reference*』を参照してください。

Microsoft管理コンソール(MMC)の使用法

Windowsシステムでは、Microsoft管理コンソールを使用して、Data Protectorのホームページにアクセスしたり、Data Protector GUIを起動したりできます。

Data Protectorのスナップイン`OB2_Snap`が、Data ProtectorとMMCの基本的統合を行います。このスナップインを使用する手順は、次のとおりです。

手順

1. Data Protectorプログラムグループで**[Data Protector MMC snap-in]**を選択します。
2. [Console Root]で[**HPE Data Protector**]を選択すると、オプションが表示されます。

Data ProtectorのGUIからHPEStorage Optimizerを起動する

次の手順を実行することで、Data Protector GUIからHPE Storage Optimizerを起動することができます。

1. Data Protectorの**グローバル**ファイル内に`StorageOptServer`変数を追加します。

   以下の形式で指定します。`StorageOptServer = <server name>` この手順は必ず実行します。
2. [バックアップ]コンテキストで、**[アクション]** > **[HPE Storage Optimizer]**に移動します。新しいWebブラウザウィンドウにStorage Optimizerが開きます。

第2章: 構成作業

システムのセキュリティ

Data Protector 10.00では、デフォルトで、すべての通信がTLS 1.2で行われます。クライアントとCell Managerの間の信頼を構成するには、インストール前に特定の前提条件が満たされている必要があります。Data Protector 10.00より前のバージョンでは、暗号制御通信(ECC)を有効にすることでCell Managerとクライアント間の通信を保護することができました。10.00より前のECCが有効になっているDAおよびMAクライアントは、引き続きData Protector 10.00でも機能します。

10.00では、すべてのコマンドおよびスクリプトが、Cell Managerを介して実行されます。集中型コマンド実行により、制御とデータの両方がセキュアTLSチャネルで送信されるため、データ整合性が保証されます。さらに、Data Protectorクライアントは、信頼済みで確認済みのCell Managerからの指示とスクリプトコマンドの実行のみをリッスンし、受け入れるようになったため、セキュリティブリーチのリスクが大幅に軽減されています。

セキュリティの詳細については、『*HPE Data Protectorインストールガイド*』を参照してください。

セキュアな通信のための証明書の構成

インストール時に、セキュアな通信のためにOpenSSLベースの自己署名証明書が使用され、指紋照合による信頼が確立されます。カスタムの証明書を使用する必要がある場合、Data Protectorのインストール後に、Data Protectorのインストール中に生成されたOpenSSL証明書をカスタム証明書で置き換えることができます。カスタム証明書の生成、証明書の再生成、および証明書の再配布のための手順は、以下のとおりです。

カスタム証明書の生成

カスタム証明書を生成し、その証明書ファイルを以下のパスにコピーすることができます。

Windowsの場合:

秘密キー: `<DP_HOME>\config\sscertificates\localhost_key.pem`

自己署名証明書: `<DP_HOME>\config\sscertificates\localhost_cert.pem`

UNIX:の場合:

秘密キー: `/etc/opt/omni/config/sscertificates/localhost_key.pem`

自己署名証明書: `/etc/opt/omni/config/sscertificates/localhost_cert.pem`

Data Protectorでの証明書の再生成

次のコマンドを実行して、Data Protectorで証明書を再生成します。

```
omnicc -secure_comm -regenerate_cert
```

証明書の再配布

カスタム証明書の使用中、または証明書を再生成する場合に、証明書の再配布が必要になります。

Cell Manager証明書の再配布

1. 次のコマンドを実行して、すべてのインストールサーバーサーバー(すべてWindowsおよびUnix)のCell Manager証明書を再構成します。

   ```
   omnicc -secure_comm -reconfigure_peer <CM hostname>
   ```

2. 再配布および再構成を行うには、次のコマンドをCMに対して実行する必要があります。

   ```
   omnicc -secure_comm -reconfigure_peer_all <input_file_path>
   ```

   パラメーター<input_file_path>は、省略可能です。このファイルには、セルを構成するすべてのクライアントの証明書が含まれている必要があります。

   ファイルの形式は次のとおりです。

   ```
   -host "linux_client_hostname" -user "<username>" -pass "password"
   -host "windows_client_hostname" -user "<Domain>\<username>" -pass "<password>"
   ```

   各行は1つのクライアントに対応していて、ユーザー名とパスワードは上記のように指定する必要があります。

   <input_file_path>を指定しない場合、omniccは、Cell Manager証明書の再配布および構成を試行するときに、クライアント証明書を求めるプロンプトを表示します。

   > **注:**
   > Windowsクライアントの場合、Domain名にプレフィックスを付加する必要があります。

クライアント証明書の再配布

クライアント証明書を再生成する場合は、その証明書をCell Managerに再配布する必要があります。次のコマンドを実行します。

```
omnicc -secure_comm -reconfigure_peer <client_host_name>
```

レポート

[レポート]コンテキストの下の[通知]セクションに、**WarnCertificateExpiry**通知が追加されています。

これを使用すると、期限切れが近づいている証明書に関する通知を生成することができます。

デフォルトでは、7日後に期限切れとなる証明書について通知が生成されます。**WarnCertificateExpiryBefore**グローバル変数の値を変更することで、もっと前に通知を生成することができます。

GUIからCell Manager/Jumpstation UIに接続する

Cell Consoleコンポーネントがインストールされているホストを使用して複数のCell Managerに接続している場合、CCコンポーネントがインストールされているホストを、接続するすべてのCell Managerに対してセキュリティで保護し、すべてのCMをCUIホストに対してセキュリティで保護する必要があります。

例:

ケース1:

Cell ManagerのhostCM1、hostCM2、hostCM3に接続するためにhostXが使用される場合、hostXで次のコマンドを実行します。

```
Omnicc –secure_comm –configure_peer <hostCM1>
Omnicc –secure_comm –configure_peer <hostCM2>
Omnicc –secure_comm –configure_peer <hostCM3>
```

上記のすべてのCell Managerで、次のコマンドを実行します。

```
Omnicc -secure_comm -configure_peer <hostX>
```

ケース2:

hostXが10.00より前のバージョンで、hostCM1、hostCM2、hostCM3が10.0以降の場合、3つのすべてのCell Managerで次のコマンドを実行します。

```
Omnicc -secure_comm -configure_for_gui <hostX>
```

ケース3:

CMが10.0より前のバージョンで、hostxが10.0以降の場合、hostXで次のコマンドを実行します。

```
Omnicc -secure_comm -configure_for_gui <hostCM1>
Omnicc -secure_comm -configure_for_gui <hostCM2>
Omnicc -secure_comm -configure_for_gui <hostCM3>
```

ケース4:

hostCM1が10.0より前のバージョンで、hostCM2、hostCM3、hostXが10.0以降の場合、hostXで、次のコマンドを実行します。

```
Omnicc -secure_comm -configure_for_gui <hostCM1>
Omnicc -secure_comm -configure_peer <hostCM2>
Omnicc -secure_comm -configure_peer <hostCM3>
```

hostCM2とhostCM3で次のコマンドを実行します。

```
Omnicc -secure_comm -configure_peer <hostX>
```

ユーザーのセキュリティ

Data Protectorユーザーは、セキュリティが重要なData Protector層の1つです。ユーザーの構成は、注意して計画およびテストする必要があります。

ユーザー権限

一部のユーザー権限は非常に強力なので、セキュリティの問題が発生する危険性を含んでいます。たとえば、[ユーザーの構成]と[クライアントの構成]のユーザー権限を持つユーザーは、セキュリティ設定を変更できます。

[別のクライアントへ復元]ユーザー権限も、特に**[ルートユーザーとしてバックアップ]**ユーザー権限または**[ルートユーザーとして復元]**ユーザー権限のいずれかと組み合わせた場合は非常に強力です。

あまり強力ではないユーザー権限でも、その権限に関連するリスクを内包しています。Data Protectorでは、特定のユーザー権限を制限して、このようなリスクを軽減するように構成できます。

[バックアップ仕様を開始]ユーザー権限

このユーザー権限を割り当てられているユーザーは、コマンドラインで`omnib`を`-datalist`オプションを指定して実行することによって、バックアップ仕様のバックアップセッションを開始することが許可されます。

[バックアップ仕様を開始]ユーザー権限と**[バックアップ開始]**ユーザー権限の両方が割り当てられているユーザーは、GUIで構成済みのバックアップ仕様を表示でき、バックアップ仕様または対話式バックアップのバックアップセッションを開始できます。

ユーザーには、必ずしも対話式バックアップの実行を許可する必要はありません。**[バックアップ仕様を保存]**権限を持つユーザーにのみ対話式バックアップを許可するには、`StrictSecurityFlags`グローバルオプションを`0x0200`に設定します。

バックアップ仕様の内容にアクセスできないようにする

セキュリティの高い環境では、保存されているバックアップ仕様の内容が重要な情報または機密情報として扱われることがあります。

Data Protectorは、**[バックアップ仕様を保存]**ユーザー権限を持つユーザーを除き、すべてのユーザーがバックアップ仕様の内容にアクセスできないように構成できます。これを行うには、`StrictSecurityFlags`グローバルオプションを`0x0400`に設定します。

ホストの信頼

ホストの信頼機能を使用すると、クライアント数が限られていて、あるクライアントから別のクライアントにデータを復元する必要だけがある場合は、ユーザーに**[別のクライアントへ復元]**ユーザー権限を付与しなくてすむことがあります。そのデータを使用する信頼関係のあるホストのグループを定義できます。

ホストの信頼は、通常、以下のような場合に使用します。

- クライアントがクラスター(ノードおよび仮想サーバー)内に存在する場合。
- クライアントのホスト名を変更した後、古いバックアップオブジェクトのデータを復元する必要が生じた場合。
- DNSの問題により、クライアントのホスト名とバックアップオブジェクトが一致していない場合。
- ユーザーが複数のクライアントを保有していて、あるクライアントから別のクライアントにデータを復元する必要がある場合。

ユーザーグループ

Data Protectorには、デフォルトで、いくつかの定義済みユーザーグループのみ用意されています。Data Protector環境のユーザーの種類ごとに特定のグループを定義して、最小限の権限だけをユーザーに割り当てるようにすることをお勧めします。

ユーザー制限

特定のユーザーグループを定義するほかに、ユーザーアクションをさらに制限してセルの特定のシステムでのみ実行されるようにすることができます。このような制限は、`user_ restrictions`ファイルを構成して適用します。この制限が適用されるのは、adminおよびoperator以外のData Protectorのユーザーグループです。

ユーザーのチェック

ユーザーの構成とユーザーのチェックは、密接な関係にあります。ユーザーのチェックを強化しても注意してユーザーを構成しないと意味がありません。反対に、細心の注意を払ってユーザーを構成してもユー

ザーのチェックを強化しないとうまくいきません。

Data Protectorのユーザーリストに"脆弱な"ユーザー仕様が存在しないようにすることが重要です。ユーザー仕様のクライアント部分は、(特にチェックを強化した場合)強度がある部分ですが、ユーザー部分とグループ部分は、確実にチェックすることができません。

強力なユーザー権限を持つユーザーは、そのユーザーがData Protectorの管理に使用する特定のクライアントに対して構成する必要があります。複数のクライアントを使用する場合は、そのユーザーを、`user`、`group`、`<Any>`として指定するのではなく、クライアントごとにエントリを追加するようにします。信頼されていないユーザーにはこれらのシステムへのログインを許可しないようにする必要があります。

厳密なホスト名チェック

デフォルトでは、Cell Managerによって、比較的簡単な方法を使ってユーザーのチェックが行われます。この方法では、ユーザーインターフェイスまたはApplication Agentを起動しているクライアントが認識できるホスト名が使用されます。この方法は、構成するのが簡単であり、セキュリティが「推奨」される(悪質な攻撃が予期されない)環境で妥当なレベルのセキュリティを確立します。

一方、厳密なホスト名チェックの設定を使用すると、ユーザーのチェックが強化されます。このチェックでは、Cell Managerで接続から取得したIPを基にDNS逆引きを行ってホスト名を解決し、そのホスト名を使用します。厳密なホスト名チェックを有効に設定するには、`StrictSecurityFlags`グローバルオプションを`0x0001`に設定します。

制限事項

- IPベースのユーザーチェックは、ネットワークのスプーフィング対策程度の強度しかありません。セキュリティ設計者は、特定のセキュリティ要件を満たすレベルのスプーフィング対策が既存のネットワークに施されているかどうかを確認する必要があります。スプーフィング対策は、ファイアウォール、ルーター、VPNなどを使ってネットワークをセグメント化することによって実現できます。
- 特定のクライアント内でユーザーを分離しても、クライアント間で分離した場合ほど強度はありません。セキュリティの高い環境では、通常のユーザーと高い権限を持つユーザーを同じクライアント内に混在させないようにする必要があります。
- ユーザー仕様内で使用されているホストは、固定IPが割り当てられていてDNSで構成されている場合を除き、DHCPを使用するように構成できません。

この設定で実現できる保護レベルを正しく評価するには、上記の制限事項に注意してください。

要件

チェックを強化した場合、一部の内部接続へのアクセス権が自動的に付与されません。そのため、このチェックを使用する場合は、以下について、新しいユーザーを追加する必要があります。

- Windowsクライアント上のApplication Agent (OB2BAR)。Application Agentがインストールされている各クライアントに、ユーザー`SYSTEM`、`NT AUTHORITY`、*`client`*を追加する必要があります。特定のアカウントを使用するようにクライアントのInetを構成する場合は、そのアカウントが既に構成されている必要があります。

ホスト名の解決

以下の場合、Data Protectorでチェックに使用されるホスト名が、デフォルトのユーザーチェックの場合とホスト名によるチェックの場合とで異なることがあります。

- DNS逆引きで別のホスト名が返される。これは、意図的に行うこともありますが、クライアントまたはDNS逆引き用テーブルのいずれかの構成が正しくないことを示していることもあります。
- クライアントがマルチホーム構成である(複数のネットワークアダプターや複数のIPアドレスを持つ)。マルチホームクライアントにこの留意事項が該当するかどうかは、そのクライアントのネットワーク内での役割やDNSでの構成方法によって異なります。
- クライアントがクラスター構成である。

この設定で有効になるチェックの特性により、Data Protectorユーザーを再構成する必要があることがあります。既存のData Protectorユーザーの仕様をチェックして、上記のいずれかの理由が影響するかどうかを確認する必要があります。状況によっては、既存の仕様を変更するか、新しい仕様を追加して、接続元になる可能性のあるすべてのIPを含める必要があることがあります。

なお、厳密なホスト名チェックを有効にするときにユーザー仕様を変更する必要があった場合は、デフォルトのユーザーチェックに戻すときにユーザーを再構成する必要があります。そのため、継続的に使用するユーザーチェックを事前に決定することをお勧めします。

信頼性の高いDNS逆引きを行うための前提条件は、保護されたDNSサーバーを使用することです。許可されていないユーザーからの物理アクセスやログオンを防ぐ必要があります。

(ホスト名の代わりに)IPを使ってチェックを行うと、DNS関連のチェック時に発生する可能性のある一部の問題を解決できますが、保守が大変になります。

セキュリティログ

Data Protector機能またはクライアントへのアクセスに問題がある場合は、ログファイルの情報を使用して問題を割り出すことができます。たとえば、ログに記録されたログが、誤って構成されたユーザーまたはクライアントの特定に役立つことがあります。

クライアントの保護イベント

クライアントのセキュリティイベントは、セル内の各クライアントのデフォルトのData Protectorログファイルディレクトリに存在する`inet.log`ファイルに記録されます。

これらのファイルは、クライアント上で最近実行されたData Protectorの処理のチェックに役立ちます。

Cell Managerのセキュリティイベント

Cell Managerのセキュリティイベントは、デフォルトのData Protectorサーバーログファイルディレクトリに存在する`security.log`ファイルに記録されます。

`security.log`ファイルは、初めてセキュリティイベントが発生したときに作成されます。

ホストの信頼を構成する

そのデータを使用する信頼関係のあるホストのグループを定義できます。

手順

1. Windows Cell Managerで、*Data_Protector_program_data*\Config\Server\cell\host_trustsファイルを作成します。

   UNIX Cell Managerで、/etc/opt/omni/server/cell/host_trustsファイルを作成します。
2. このファイルに、信頼済みホストのリストを作成します。

   例:

   ```
   GROUP="cluster.domain.com"
   {
   cluster.domain.com
   node1.domain.com
   node2.domain.com
   }
   GROUP="DFG"
   {
   computer.domain.com
   anothercomputer.domain.com
   }
   ```
3. ファイルを保存します。

暗号化

データの暗号化について

Data Protectorを使用すると、バックアップされたデータを暗号化して、保護することができます。データ暗号化方式には、ソフトウェアベース暗号化とドライブベース暗号化の2種類があります。

AES 256ビット暗号化と呼ばれるData Protectorのソフトウェア暗号化は、暗号化と復号化の両方に同じキーを使用するAES (Advanced Encryption Standard)という暗号化アルゴリズムに基づきます。データの暗号化は、データをネットワーク上で転送してメディアに書き込む前に行われます。

Data Protectorのドライブベースの暗号化では、ドライブの暗号化機能が使用されます。実際の実装と暗号化の強度は、ドライブのファームウェアによって異なります。Data Protectorは、その機能を有効にして、暗号化キーを管理するだけです。

暗号化を有効にした後は、どのような追加の構成も必要ありません。ただし、Data ProtectorのAES 256ビットの暗号化には、コマンドラインインターフェイス(CLI)を使用した暗号化キーの高度な手動の管理機能があります(キーの有効期限、再アクティベーション、エクスポート、インポート、削除など)。

Data Protector GUIまたはCLIを使用すると、どのバックアップオブジェクトが暗号化されているか、あるいはどのバックアップメディアに暗号化されたオブジェクトが含まれているかを知り、これらのオブジェクトの暗号化の詳細を入手できます。

AES 256ビット暗号化を有効化する

ソフトウェアベースのAES 256ビット暗号化は、新しいバックアップ仕様の作成時またはすでに構成されたバックアップ仕様の作成時に有効化できます。

前提条件

- 暗号化されたIDBバックアップを実行する前に、アクティブな暗号化キーが必要です。詳細については、`omnikeytool`のmanページまたは『*HPE Data Protector Command Line Interface Reference*』を参照してください。

制限事項

- AES 256ビット暗号化では、ファイル名、ファイルサイズなどのメタデータは暗号化されません。
- 暗号化は、ディスクへのZDBとディスク+テープへのZDBのディスクパートには適用されません。
- AES 256ビット暗号化を使用してバックアップされるオブジェクトは、集約できません。

ファイルシステムのバックアップ仕様で暗号化を有効化する

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで**[バックアップ仕様]**→**[ファイルシステム]**の順に展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 変更するバックアップ仕様をクリックします。
4. [オプション]プロパティページで、[ファイルシステムオプション]の**[拡張]**ボタンをクリックします。
5. [ファイルシステムオプション]ウィンドウで、**[その他]**タブをクリックします。**[データセキュリティ]**ドロップダウンリストで、**[AES 256ビット]**オプションを選択します。
6. **[OK]**をクリックし、**[適用]**をクリックして、変更内容を保存します。

> **ヒント:**
> 選択したバックアップオブジェクトのみを暗号化するには、**[バックアップオブジェクトのサマリー]**タブに移動し、オブジェクトのプロパティの**[AES 256ビット]**オプションを選択します。

ディスクイメージバックアップ仕様で暗号化を有効化する

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで**[バックアップ仕様]**→**[ファイルシステム]**の順に展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 変更するバックアップ仕様をクリックします。
4. [バックアップオブジェクトのサマリー]ページで**[プロパティ]**ボタンをクリックします。
5. [オブジェクトのプロパティ]ウィンドウで、**[その他]**タブをクリックします。**[データセキュリティ]**ドロップダウンリストで、**[AES 256ビット]**オプションを選択します。
6. **[OK]**をクリックし、**[適用]**をクリックして、変更内容を保存します。

内部データベースバックアップ仕様で暗号化を有効化する

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**、**[内部データベース]**を順に展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 変更するバックアップ仕様をクリックします。
4. [オプション]ページで、[共通アプリケーションオプション]の下の**[拡張]**ボタンをクリックします。
5. [共通アプリケーションオプション]ウィンドウで、**[その他]**タブをクリックします。**[データセキュリティ]**ドロップダウンリストから、**[AES 256ビット]**オプションを選択します。
6. **[OK]**をクリックし、**[適用]**をクリックして、変更内容を保存します。

アプリケーション統合バックアップ仕様で暗号化を有効化する

制限事項

- AES 256ビット暗号化をサポートするアプリケーション統合の最新リストは、https://softwaresupport.hpe.com/にある最新のサポート一覧を参照してください。
- Microsoft SQL Server用統合ソフトウェアの場合、オプション**[高速ダイレクトモード]**および**[AES 256ビット]**を組み合わせて使用することはできません。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[MS SQL Server]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 変更するバックアップ仕様をクリックします。
4. [オプション]プロパティページで、[共通アプリケーションオプション]の**[拡張]**ボタンをクリックします。
5. [共通アプリケーションオプション]ウィンドウで、**[その他]**タブをクリックします。**[データセキュリティ]**ドロップダウンリストで、**[AES 256ビット]**オプションを選択します。
6. **[OK]**をクリックし、**[適用]**をクリックして、変更内容を保存します。

暗号化されたバックアップを含むメディアのエクスポートとインポート

暗号化されたバックアップから別のData Protectorセルのクライアントにデータを復元するには、以下のセクションで説明するように、メディアと暗号化キーをあて先のCell Managerにインポートする必要があります。

> **注:**
> Data Protectorには、コマンドラインインターフェイス(CLI)を使用する暗号化キーの高度な手動の管理機能があります(キーの有効期限、再アクティベーション、エクスポート、インポート、削除など)。詳細については、`omnikeytool`のmanページまたは『*HPE Data Protector Command Line Interface Reference*』を参照してください。

CMMDBを含まないCell Manager環境またはMoM環境

Cell Manager環境またはローカルのMMDBを使用するMoM環境で以下の手順を実行し、暗号化されたバックアップを含むメディアをエクスポートおよびインポートします。

手順

1. 元のCell Managerで、IDBからメディアをエクスポートします。この操作では、キーストアから、暗号化キーがエクスポートされるデフォルトディレクトリの*mediumID*.csvファイルに関連暗号化キーもエクスポートします。
2. *mediumID*.csvファイルをエクスポート先のCell Managerに転送し、暗号化キーがインポートされるデフォルトディレクトリに配置します。
3. エクスポートしたメディアをあて先のCell Managerが使用するドライブに挿入します。
4. あて先のCell Managerで、メディアをインポートします。この操作によって、*mediumID*.csvファイルからキーもインポートされます。

> **注:**
> キーファイルがない場合にもメディアのインポートはできますが、復号化キーがないので、カタログインポートは中止されます。

CMMDBを含むMoM環境

CMMDBが使用されているMoM環境では、すべてのメディア情報がMoM Managerに保存されますが、メディアで使用される暗号化キーIDとCDBは、それぞれのCell Managerのローカルキーストアに保存されます。メディア管理のすべての操作は、MoM Cell Managerで実行する必要があることに注意してください。

CMMDBがMoM Managerにある場合に暗号化されたバックアップを含むメディアをエクスポートおよびインポートするには、以下の手順を実行します。

手順

1. CMMDBからメディアをエクスポートします。キーIDは、暗号化キーがエクスポートされるデフォルトディレクトリの*mediumID*.csvファイルにエクスポートされます。
2. *mediumID*.csvファイルをエクスポート先のCell Managerに転送し、暗号化キーがインポートされるデフォルトディレクトリに配置します。
3. MoM Managerで、ライブラリからメディアを取り出します。
4. メディアを元のメディアプールからあて先セルのドライブに関連付けられているメディアプールに移動します。この操作によって、カタログもインポートされます。
5. エクスポートしたメディアをあて先のCell Managerが使用するドライブに挿入します。
6. あて先のCell Managerで、メディアをインポートします。この操作によって、*mediumID*.csvファイルからキーもインポートされます。

ドライブベースの暗号化の有効化

ドライブベースの暗号化をサポートするデバイスの最新リストは、https://softwaresupport.hpe.com/にある最新のサポート一覧を参照してください。

ドライブベースの暗号化は、次の場合に有効化できます。

- ドライブを構成するか、または既に構成されているドライブを変更する場合。
- 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の仕様を構成するか、または既に構成されている仕様を変更する場合。
- 自動メディア操作を構成するか、または既に構成されている操作を変更する場合。

前提条件

- 暗号化されたIDBバックアップを実行する前に、アクティブな暗号化キーが必要です。詳細については、`omnikeytool`のmanページまたは『*HPE Data Protector Command Line Interface Reference*』を参照してください。

制限事項

- NDMPサーバーにより制御されるデバイスや、外部暗号化コントロール(HPE SKMコントロール下のESLライブラリなど)があるライブラリ内のドライブには、ドライブベースの暗号化を使用できません。

推奨事項

- パフォーマンスを最適化するために、使用するブロックサイズは、少なくとも256キロバイトにする必要があります。

> **注:**
> 暗号化されたバックアップと暗号化されていないバックアップの両方が含まれるメディアにバックアップすると、[`Drive-based decryption enabled`]メッセージが表示されます。これは、メディアでの前回のバックアップが暗号化されたものであり、新しいバックアップが追加される前にData Protectorにより確認できるように自動的に復号されたことを意味しています。

ドライブ構成でドライブベースの暗号化を有効化する

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[デバイス]**を展開し、次に目的のデバイスおよびそのドライブを展開します。
3. 目的のドライブを右クリックし、**[プロパティ]**をクリックします。
4. [設定]プロパティページで**[拡張]**をクリックします。
5. [拡張オプション]ウィンドウの**[設定]**タブで、**[ドライブベースの暗号化]**オプションを選択し、**[OK]**をクリックします。
6. **[適用]**をクリックして、変更内容を保存します。

バックアップ仕様でドライブベースの暗号化を有効化する

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 適切なバックアップ仕様をクリックします。

4. [あて先]ページで、バックアップ用に選択されているデバイスを右クリックして**[プロパティ]**をクリックします。
5. [デバイスプロパティ]ウィンドウで、**[ドライブベースの暗号化]**オプションを選択し、**[OK]**をクリックします。
6. **[適用]**をクリックして、変更内容を保存します。

> **ヒント:**
> オブジェクトコピーまたはオブジェクト集約の仕様を変更するには、**[オブジェクト操作]**コンテキストで仕様を開き、手順4～6を実行します。

自動メディア操作におけるドライブベースの暗号化を有効化する

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[自動操作]**を展開します。構成済みの自動操作がすべて表示されます。
3. ドライブベースの暗号化を有効にするメディア操作をクリックします。
4. [オプション]ページで、**[ドライブベースの暗号化]**オプションを選択し、**[適用]**をクリックします。

> **注:**
> **[ドライブベースの暗号化]**オプションは、自動メディア操作に関係するすべてのデバイスに適用されます。

ユーザー認証とLDAPについて

企業システムとしてのData Protectorは、認証と承認のために、エンタープライズユーザー管理インフラストラクチャーに接続する必要があります。この接続を行うことで、会社のユーザーディレクトリ内で構成したユーザーとグループに対して、Data Protectorサービスへのアクセスを許可できます。

セキュリティで保護された接続を介してユーザー認証が実施され、基盤となる技術としてLightweight Directory Access Protocol (LDAP)が使用されます。その後、ユーザーは会社の資格情報を使用してData Protectorサービスにアクセスできるようになるため、別途パスワードを管理する必要はありません。また、確立された認証および承認プロセスに従って、会社のディレクトリ内で管理者またはオペレーターをグループとして管理できます。

LDAP統合は、Java Authentication and Authorization Service (JAAS)ログインモジュールを使用して、Data Protectorの組み込みアプリケーションサーバー(WildFly)のセキュリティドメイン内に構成されます。LDAP認証と承認サービスは、オプションのLDAPログインモジュールによって提供され、必須のData Protectorログインモジュールによって Data Protector権限にマップされます。LDAP統合が構成されていない場合、Data Protectorは以前のリリースと同じ動作になります。

Data Protectorは、ユーザー認証にログインモジュールスタック内のログインモジュールを使用します。Data Protector GUIを使用してCell Managerに接続すると、ユーザー認証は以下のログインモジュールを使用して実行されます。

1. LDAPログインモジュール: 既存のLDAPサーバーに対して、ユーザー名とパスワードなどのユーザーの資格情報を認証します。「LDAPログインモジュールを初期化して構成する」を参照してください。
2. Data Protector ログインモジュール: Data Protectorユーザーリストと Webアクセスパスワードに対してユーザー資格情報を認証します。「Data Protectorの権限をLDAPユーザーまたはグループに付与する」を参照してください。

3. LDAPの初期化と構成に必要なすべての手順を実行すると、構成もチェックできます。「LDAP構成をチェックする」を参照してください。

> **注: 注記**: 従来の方法でCLIのアクセスを許可するようにData Protector内でユーザーまたはクライアントを構成すると、Data Protector GUIではLDAP機能を使用できなくなります。

LDAPログインモジュールを初期化して構成する

LDAPログインモジュールは、Data Protectorとともにインストールされるwildflyアプリケーションサーバーのセキュリティドメインに配置されます。LDAPセキュリティ機能をはじめて使用する場合は、事前にLDAPログインモジュールを初期化して構成する必要があります。

1. LDAPログインモジュールを初期化する。
2. LDAPログインモジュールを構成する。

LDAPログインモジュールを初期化する

LDAPログインモジュールを初期化するには、`jboss-cli` utilityユーティリティを使用します。このユーティリティはData Protectorとともにインストールされます。

1. `jboss-cli`ユーティリティは `%Data_Protector_home%/AppServer/bin`ディレクトリにあります。次のコマンドを実行します。
   - Windowsの場合: `jboss-cli.bat --file=ldapinit.cli`
   - UNIXの場合: `jboss-cli.sh --file=ldapinit.cli`

   このコマンドは、wildfly構成内にLDAPログインモジュールを作成し、この新しいログインモジュールにデフォルト値を設定します。このコマンドラインによって`standalone.xml`構成ファイル内に生成されるデフォルト値は次のとおりです。

```
<security-domain name="hpdp-domain">

<authentication>

<login-module code="LdapExtended" flag="optional">

<module-option name="java.naming.factory.initial"
value="com.sun.jndi.ldap.LdapCtxFactory"/>

<module-option name="java.naming.security.authentication" value="simple"/>

<module-option name="roleFilter" value="(member={1})"/>

<module-option name="roleAttributeID" value="memberOf"/>

<module-option name="roleNameAttributeID" value="distinguishedName"/>

<module-option name="roleAttributeIsDN" value="true"/>

<module-option name="searchScope" value="SUBTREE_SCOPE"/>

<module-option name="allowEmptyPasswords" value="true"/>

<module-option name="password-stacking" value="useFirstPass"/>
```

```
</login-module>
<login-module code="com.hp.im.dp.cell.auth.DpLoginModule" flag="required">
<module-option name="password-stacking" value="useFirstPass"/>
</login-module>
</authentication>
</security-domain>
```

> **注:**
> このコマンドラインによってstandalone.xml構成ファイル内に生成されるデフォルト値は、Cell ManagerがUNIX環境にインストールされLDAPを使用している場合は異なります。変更を以下に示します。
>
> ```
> <login-module code="LdapExtended" flag="optional">
> <module-option name="java.naming.factory.initial"
> value="com.sun.jndi.ldap.LdapCtxFactory"/>
> <module-option name="java.naming.security.authentication" value="simple"/>
> <module-option name="roleFilter" value="(member={1})"/>
> <module-option name="roleAttributeID" value="memberOf"/>
> <module-option name="roleNameAttributeID" value="distinguishedName"/>
> <module-option name="roleAttributeIsDN" value="true"/>
> <module-option name="searchScope" value="SUBTREE_SCOPE"/>
> <module-option name="allowEmptyPasswords" value="false"/>
> <module-option name="password-stacking" value="useFirstPass"/>
> <module-option name="java.naming.provider.url" value="ldap://<IP_of_
> Active_Directory_host>"/>
> <module-option name="baseCtxDN" value="OU=_Benutzer,DC=godyo,DC=int"/>
> <module-option name="rolesCtxDN" value="OU=_Gruppen,DC=godyo,DC=int"/>
> <module-option name="bindDN" value="CN=backup-service,OU=_Service_
> Accounts,DC=godyo,DC=int"/>
> <module-option name="bindCredential" value="password"/>
> <module-option name="baseFilter" value="(userPrincipalName={0})"/>
> </login-module>
> ```
>
> 構成パラメーターbaseCtxDNとrolesCtxDNは、主要なパラメーターです。組織単位(OU)パラメーターはUNIX Cell Managerの認証に使用します。

2. Cell Manager上に置かれているWildFly管理コンソールにリモートクライアントからアクセスするには、WildFly管理コンソールへのリモートアクセスを有効にする必要があります。これを行うには、テキストエディターを使用して、以下のようにstandalone.xmlファイルのインターフェイスセクション内の管理イ

ンターフェイスのバインドアドレスを127.0.0.1から0.0.0.0に変更します。

```
<interfaces>
<interface name="management">
<inet-address value="${jboss.bind.address.management:0.0.0.0}"/>
</interface>
<interface name="public">
<inet-address value="0.0.0.0"/>
</interface>
<interface name="unsecure">
<inet-address value="${jboss.bind.address.unsecure:127.0.0.1}"/>
</interface>
</interfaces>
```

3. 以下を使用してData Protectorサービスを再起動します。

```
omnisv stop
omnisv start
```

LDAPログインモジュールを構成する

LDAPログインモジュールを構成するには、WildFly Application ServerのWebベースの管理コンソールを使用します。このWebベースの管理コンソールはData Protectorとともにインストールされます。以下の手順を実行します。

1. WildFly管理コンソールにアクセスするには、WildFlyユーザーを作成します。WildFlyユーザーを作成するには、add-userユーティリティを実行します。
   - Windows: `add-user.bat`の場所: `%Data_Protector_home%/AppServer/bin`
   - UNIX: `add-user.sh`の場所: `/opt/omni/AppServer/bin`
2. 次のパラメーターを入力します。
   - **Type of user to add**: [Management User]を選択します。
   - **Realm**: ユーティリティによってデフォルト値のManagementRealmが選択されているため、このフィールドは空白のままにします。
   - **Username**: ユーザー名を追加します。
   - **Password**: パスワードを追加します。
   - **グループ**: なし。
3. WildFly管理コンソールにアクセスするには、ブラウザーで次のURLを開きます。<http://cell-manager-name:9990/console>

4. [認証]画面で、add-userユーティリティを使用して作成した**ユーザー名**と**パスワード**を指定します。
5. **[ログイン]**をクリックします。WildFlyアプリケーションサーバーの管理コンソールが表示されます。
6. WildFly管理コンソールで、**[プロファイル]**タブを選択します。
7. **[プロファイル]**タブで、**[セキュリティ]**ノードを展開し、**[セキュリティドメイン]**をクリックします。
8. 登録済みのセキュリティドメインのリストで、hpdp-domainの**[表示]**をクリックします。セキュリティドメインhpdp-domainに対して、次のログインモジュールが定義されています。
   - LdapExtended
   - Com.hp.im.dp.cell.auth.DpLoginModule
9. **LdapExtended**モジュールを選択します。
10. [詳細]セクションで、**[モジュールオプション]**タブをクリックします。構成済みのすべてのモジュールオプションが**[モジュールオプション]**タブに表示されます。
11. LDAPログインモジュールをカスタマイズして使用するには、他のモジュールオプションを追加する必要があります。**[追加]**をクリックして、各モジュールオプションの**[名前]**と**[値]**を指定します。詳細については、次の表を参照してください。

モジュールオプション	名前	値	説明
プロバイダーURL	`java.naming.provider.url`	LDAPサーバーのURLを次の形式で指定します。`ldap://<server>:<port>`	標準プロパティ名
基本コンテキスト識別名(DN)	`baseCtxDN`	ユーザーが格納されているLDAPの場所のDNを指定します。	ユーザー検索の開始場所となるコンテキストの固定DN
基本フィルター	`baseFilter`	ユーザーのログイン名に一致するLDAPセットアップの属性を次の形式で指定します。(`(<user-login-name-attribute>={0})`)。`<user-login-name-attribute>`は、対応するLDAP属性名に置き換える必要があります。	認証対象のユーザーのコンテキストを検索するために使用する検索フィルター
役割コンテキストDN	`rolesCtxDN`	ユーザーグループが格納されているLDAPの場所のDNを指定します。	ユーザーグループを検索するためのコンテキストの固定DN
バインドDN	`bindDN`	ログインモジュールが最初のLDAPバインドを実行するために使用するLDAPユーザーのDNを指定します。ユー	ユーザーと役割を問い合わせるためにLDAPサーバーに対してバインドするために使用さ

		ザーとグループのLDAP場所を検索してユーザーとユーザーグループを取得するために、必要な権限を持っている必要があります。これらの場所は、baseCtxDN と rolesCtxDN モジュールオプションで定義されます。	れるDN。これは、baseCtxDN と rolesCtxDN 値に対する読み取り/検索権限を持つDNです。
バインド資格情報	bindCredential	BindDNモジュールオプションで入力したLDAPユーザーのパスワードを指定します。	bindDNのパスワード。

その他のモジュールオプションの詳細については、次のURLにアクセスしてください。

- https://community.jboss.org/wiki/LdapExtLoginModule
- http://technet.microsoft.com/en-us/library/cc773354 (v=ws.10).aspx

12. 変更は、WildFly Application Serverの構成を再ロードしたときに有効になります。構成を再ロードするには、%Data_Protector_home%/AppServer/binにある jboss-cliユーティリティを使用します。
13. 次のコマンドを実行します。
    - Windowsの場合: jboss-cli.bat -c :reload
    - UNIXの場合: jboss-cli.sh -c :reload

> **注: 注記**: LDAPログインモジュールをMoM環境で構成するときには、必ずすべてのCell Manager上で上記の手順を実行してください。MoM環境内のすべてのCell Managerは、LDAPログインモジュールの構成と同じ構成にする必要があります。

HPE Data Protectorの権限をLDAPユーザーまたはグループに付与する

Cell Managerに接続できるのは、Data Protector権限を付与されたLDAPユーザーに限られます。LDAPログインモジュールを構成すると、LDAPユーザーに必要なData Protector権限を付与できます。

Data Protector権限を付与するには、以下の手順に従ってください。

1. Data Protector GUIを開始して、LDAPユーザーまたはグループにData Protector権限を付与します。
    - LDAPユーザーをData Protectorユーザーグループに追加します。
    - LDAPグループをData Protectorユーザーグループに追加します。
2. LDAP資格情報を使用してログインします。

LDAPユーザーをData Protectorユーザーグループに追加する

LDAPユーザーをData Protectorユーザーグループに追加するには、以下の手順に従ってください。

1. コンテキストリストで、**[ユーザー]**をクリックします。
2. Scopingペインで**[ユーザー]**を展開し、LDAPユーザーを追加するユーザーグループを右クリックします。
3. **[ユーザーの追加/削除]**をクリックして、ウィザードを起動します。
4. [ユーザーの追加/削除]ダイアログボックスの**[手動]**タブで、次の詳細を入力します。
   - **種類**: LDAPを選択します。
   - **名前**: LDAPユーザーをLDAPユーザープリンシパル名形式で指定します。
   - **エンティティ**: LDAPユーザーを入力します。
   - **説明**: これは省略可能です。
5. **[完了]**をクリックしてウィザードを終了します。

LDAPグループをData Protectorユーザーグループに追加する

LDAPグループをData Protectorユーザーグループに追加するには、以下の手順に従ってください。

1. コンテキストリストで、**[ユーザー]**をクリックします。
2. Scopingペインで**[ユーザー]**を展開し、LDAPグループを追加するユーザーグループを右クリックします。
3. **[ユーザーの追加/削除]**をクリックして、ウィザードを起動します。
4. [ユーザーの追加/削除]ダイアログボックスの**[手動]**タブで、次の詳細を入力します。
   - **種類**: LDAPを選択します。
   - **名前**: LDAPグループ名を識別名(DN)形式で指定します。
   - **エンティティ**: LDAPグループを入力します。
   - **説明**: これは省略可能です。
5. **[完了]**をクリックしてウィザードを終了します。

> **注:** LDAPユーザーには、このユーザーが所属しているLDAPグループと同じ権限レベルが自動的に付与されます。

LDAP資格情報を使用してログインする

LDAP資格情報を使用してログインするには、以下の手順に従ってください。

1. Data Protector GUIを起動してCell Managerに接続します。
2. [LDAP認証]画面で、Data ProtectorにアクセスするためのLDAP資格情報を入力します。LDAPユーザーは使用可能なData Protectorユーザーグループであればどのユーザーグループに所属していてもかまいません。

LDAP構成をチェックする

WebブラウザーからData Protectorログインプロバイダーサービス`getDpAcl`を照会して、特定のLDAPユーザーまたはグループに対してユーザー権限が正しく設定されているかどうかを確認するには、以下の手順を行います。

特定のユーザーのアクセス制御リスト(ACL)を取得するには、以下の手順に従ってください。

1. ブラウザーを使用してData ProtectorログインプロバイダーのWebサービスに接続します。
2. ブラウザー上にサーバー証明書の承認を求めるメッセージが表示される場合があります。**[承認]**をクリックして要求を確認します。
3. ログイン資格情報の入力を求めるダイアログボックスが表示されます。Data Protectorを使用して設定した有効なLDAPユーザー名とパスワードを入力します。
4. ブラウザーから次のACL (アクセス制御リスト)が返されます。`https://<server>:7116/dp-loginprovider/restws/dp-acl`
5. このACLを使用して、割り当てられている権限が、対応するData Protectorユーザーグループに指定されているData Protectorユーザー権限に一致しているかどうかを確認します。

ファイアウォールのサポート

ファイアウォールのサポートについて

Data Protectorは、Data Protectorプロセスがファイアウォールを経由して通信するような環境で構成することができます。Data Protector 9.09および10.00以降、ファイアウォールで開いておく必要があるポート数が少なくなりました。この変更は、セルのアップグレード後にのみ行われます。そのときまで、古いクライアントは、レガシーモードで作動し、以前のData Protectorバージョンと同じ、開いているポートを使用します。

OB2PORTRANGE変数とOB2PORTRANGESPEC変数をData Protectorプロセスのリスンポート用に設定する必要はありません。ただし、Data Protectorがホスト内で内部プロセス通信に使用するために、これらの変数を設定することは可能です。以下の例で、使用法について説明します。

例1:

HPE Data Protector 9.09 MAおよびHPE Data Protector 9.09 DAの旧バージョン

MAは、すべてのアドレスにバインドされたポートを開きます。MAが0.0.0.0:1234でリッスンしているため、これはnetstat出力に表示されます。

- 「1234」は例であり、実際のポートは、OB2PORTRANGE変数およびHPE Data Protector構成を使用して設定される動的ポート範囲によって決まります。
- 「0.0.0.0」は「すべてのアドレス」を表し、IPv6の[::]と同等です。これは、クライアントがどのルートを介しても接続可能であることを意味します。

同じホストの他のプロセスは、ポート1234を開くことができません。DAは、MAホスト1234に直接接続します。ポート1234は、ファイアウォールでを開いたままにしておく必要があります。

例2:

HPE Data Protector 9.09 MAおよびHPE Data Protector 9.09 DA:

- MAは、接続中のDAがHPE Data Protectorバージョン9.09以前であるかどうかを認識しないため、MAはポート0.0.0.0:1234を開いたままにします。
- ケース1と比較すると、HPE Data Protector 9.09クライアントのみが接続することが確実である場合は、ポート1234を開く必要はありません。これはホストをアップグレードする順序によって異なります。

例3:

HPE Data Protector 9.09 MA、HPE Data Protector 9.09 DA、およびHPE Data Protectorファイアウォールが MAホストで有効になっている

- MAは、ループバックインターフェイスのみにバインドされたポートを開きます。MAが127.0.0.1:1234(IPv6の場合は[::1]:1234)でリッスンしているため、これはnetstat出力に表示されます。
- リモートホストからポート1234にアクセスできないため、Windowsファイアウォールか他のファイアウォールに関わらず、古いDAは接続できません。

> **注:**
> ファイアウォールは、開いているポートからのプロセスを阻止せずに、リモートホストから開いているポートへの接続のみを阻止します。

HPE Data Protector 10.00でのポートの使用の詳細については、HPE Data Protector 9.09以降におけるポートの使用の表を参照してください。

Data Protector内の通信

Data Protectorの各種プロセスは、TCP/IP接続を通じて互いに通信します。Data Protectorは、以下のポートが必要です。

- すべてのData Protectorシステム上のInetポート(デフォルトは5555/5565)。

  > **注:**
  > Windows inetは、マルチスレッドです。

- Cell Managerシステム上のIDBサービスポート(デフォルトで7112)。
- Cell Managerシステム上のアプリケーションサーバーポート(デフォルトで7116)。
- StoreOnceSoftware.exeバイナリのルールは、インバウンドファイアウォール例外に残しておく必要があります。StoreOnceSoftware.exeは、(サードパーティのコードに基づく)単一ポート通過をサポートしていませんが、インバウンドポートを開いて通信を受け入れます。

これらのポートは、ファイアウォールで(リモートホストからアクセスできるように)開いておく必要があります。

さらに、Data Protectorは、いくつかの番号の動的ポートを開きます。これらのポートは、Data Protectorセルがアップグレードされるまで、ファイアウォールで開いたままにしておく必要があります。セルがData Protector 10.00以降にアップグレードされたら、これらのポートはプロセス(IPC)内で使用されるようになり、ファイアウォールの観点からは開いておく必要はありません。

動的ポートの範囲を構成するには、以下の変更が必要です。

- すべてのセルがアップグレードされるまで、ファイアウォールで開いておく必要があるポートを制限する。
- Data Protectorが、サードパーティアプリケーションで必要とされるポートを開かないようにする。
- Data Protectorが、独自のポートを開く必要があるData Protector以外のソフトウェアと通信可能である。

> **注:**
> インストール時に、以下のポートをInet用に開いておく必要があります。
> - Data Protectorのフレッシュインストール - 5565
> - Data Protectorのアップグレードインストール - 5555

構成メカニズム

ポート割り当て動作は、以下の2つのomnircオプションを使用して構成できます。

- OB2PORTRANGE
  このオプションは、Data Protectorのすべてのプロセスが動的ポートを開くポート範囲を設定します。
- OB2PORTRANGESPEC

Data Protector 10.00および9.09以前は、ポート範囲には以下の2つの目的がありました。

- セキュリティ: Data Protectorによって開かれるポートを制限して、ポートユーザーがファイアウォールでポートを開かなければならないようにします。
- 他のソフトウェアとの競合: Data Protector以外のソフトウェアはポート1000-2000を特定の用途のために必要とするため、OB2PORTRANGEを使用して、Data Protectorがこの範囲を使用しないようにします。これは、OB2PORTRANGEの場合に有効です。

> **注:**
> - デフォルトでは、動的ポートはオペレーティングシステムによって割り当てられます。
> - これらのオプションは、Inet(5555/5565)、IDBサービスポート(7112)およびアプリケーションサーバー(7116)用の固定ポートに影響を与えることはありません。
> - ポート範囲オプションは、Data Protectorのポート使用を制限します。これらのオプションは、Data Protector以外のアプリケーションに対しては、この範囲のポートの割り当てを制限できません。

通信に参加しているエージェントがアップグレードされると、ファイアウォールで開かれるポートの数が少なくなります。その時まで、Data Protectorは古い通信方法を使用します。古いDisk Agentは、新しいMedia Agentで機能します(その逆も同じ)。ユーザーは、すべてのセルホストがアップグレードされるまで、ポートを開いたままにする必要があります。

inetdが-p <proc_limit>オプションをサポートするプラットフォームでは、可能であれば、このオプションを使用しないでください。そうでない場合は、2200より大きいproc_limit値を使用することが推奨されています。

実際のファイアウォールを有効にする前に、Data Protectorファイアウォールが有効になっている環境でData Protectorをテストすることをお勧めします。

セル全体でData Protectorファイアウォールを有効にするには、以下のコマンドを実行します。

```
omnicc -firewall –all –enable_dp
```

一部のセルでData Protectorファイアウォールを有効にするには、-allではなく、個別のホストを指定します。

例えば、Disk AgentからMedia Agentへのファイアウォールを介した通信が可能かどうかをテストするには、以下のコマンドを使用してファイアウォールを終了します。

```
omnicc -firewall –host MAhost DAhost –enable_dp
```

-enable_dpオプションと一緒に-enable_osオプションを使用して、WindowsファイアウォールのData Protectorルールを無効にします。

これらのオプションを指定してテストを行った後で、ユーザーはサードパーティのファイアウォール(ルーターなど)の終了に進むことができます。

HPE Data Protector 9.09以降におけるポートの使用

以下の表は、Data Protector 9.09以降のさまざまなコンポーネントのポート要件についての情報を示しています。

Data Protectorホスト	ポート要件	アプリケーションホスト上のData Protectorのポート要件	アプリケーションのサードパーティ要件
インストールターゲットとして	Linux/Unix: • REXEC[1] (非セキュア):512 • RSH (非セキュア):514 • SSH:22 Windowsの場合: SMBサービス:445	なし	なし
Cell Managerとして	• Inet:5555/5565 • hpdp-as:7116 • IDBサービス:7112	なし	なし
HPE Data ProtectorDisk Agentとして	Inet:5555/5565	なし	なし
HPE Data Protector統合エージェントとして[4]	Inet:5555/5565	なし	なし
HPE Data ProtectorMedia AgentまたはNDMP Media Agentとして	Inet:5555/5565	なし	Store Once重複排除システム[2] • コマンドポート:9387 • データポート:9388 NDMPサーバー[2] • サーバー:10000 DDBoost[3]

			• NFS:2049 • 管理対象ファイル複製:2051 • NFSポートマッパー:111

[1] インストール方法に基づいて、REXEC/RSH/SSHDポートのいずれか1つのみが必要です。

[2] 開くことができる他のサードパーティポートの正確な情報については、サードパーティソフトウェアのドキュメントを参照してください。

[3] DDBoostポートの詳細については、『EMC® Data Domain® Boost for OpenStorage Administration Guide』を参照してください。

[4] Windows Hyper-Vサーバーでは、Hyper-vバックアップおよび復元を行う場合は、以下のポートを開く必要があります。

- **WMIインスタンス:135 (開始)**
- **Windowsリモート管理(HTTPS):5986**

[5] Windows Hyper-Vサーバーでは、Hyper-vバックアップおよび復元を行う場合は、以下のポートを開く必要があります。

ファイアウォールルールは、1番目の列のプロセスが、2番目の列のポートで、3番目の列のプロセスからの新しいTCP接続(SYNビットがオン)を受け付けるように作成する必要があります。

さらに、1番目の列のプロセスは、既存のTCP接続(SYNビットがオフ)上で3番目の列のプロセスに応答できなければなりません。

例えば、Media Agentシステム上のInetプロセスは、ポート5555/5565で、Cell Managerからの新しいTCP接続を受け入れることができなければなりません。Media Agentは、既存のTCP接続を使用して、Cell Managerに応答できなければなりません。Media AgentシステムからTCP接続を開く必要はありません。

制限事項

- この機能は、OpenVMSホストとSCOホストでは使用できません。これらのシステムでMedia Agent(またはポートを開くHPE Data Protectorコンポーネント)が実行されている場合、ユーザーはこれらのポートをファイアウォールで開く必要があります。

DMZ内のDisk Agent、Media Agent、およびApplication Agent

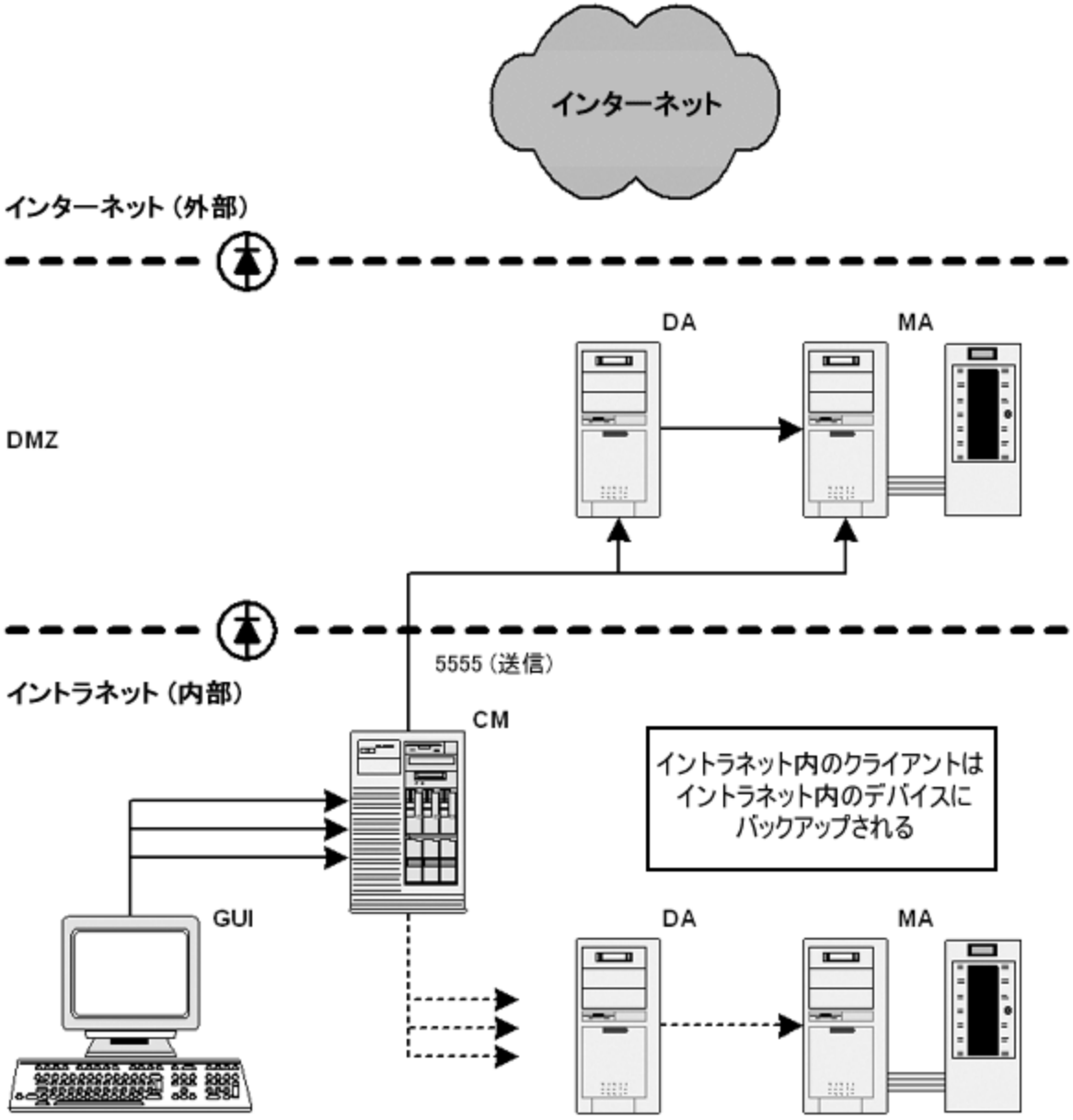
ここでは、Cell ManagerとGUIをイントラネット内に配置し、Disk Agent、Application AgentおよびMedia AgentをDMZ内に配置したバックアップ環境の構成について説明します。

構成図

ポートを開く

制限事項

構成図



ポートを開く

HPE Data Protectorは、構成用に以下のポートを開きます。

1. Disk AgentとMedia Agentは、セッションマネージャーからの接続をポート5555/5565で受け付ける必要があります。

- CMシステムからDAシステム上のポート5555/5565への接続を許可します。
- CMシステムからMAシステム上のポート5555/5565への接続を許可します。

2. **[切断された接続の再接続]**が有効になっている場合、MAおよびDAは、セッションマネージャーに接続します。
   - MAおよびDAシステムからCMシステム上のポート5555/5565への接続を許可します。
3. Application Agentは、セッションマネージャーとCRSに接続する必要があります。
   - アプリケーションサーバーシステムからCMシステム上のポート5555/5565への接続を許可します。

> **注:**
> 上記の項目2と3により、DMZからイントラネットへの接続が許可されるので、セキュリティ上のリスクが伴う可能性があります。

制限事項

- このセルでは、イントラネット内のクライアントと同様、DMZ内のクライアントもバックアップできます。ただし、クライアントの各グループは、ファイアウォールの同じ側にあるクライアント上で構成されているデバイスにバックアップする必要があります。

  お使いのファイアウォールが、イントラネットからDMZへの接続を制限していない場合は、イントラネット内のクライアントを、DMZエリア内のクライアント上で構成されているデバイスにバックアップすることもできます。ただし、イントラネットからDMZエリアにバックアップしたデータは外部からの攻撃を受けやすくなるため、この方法はお勧めできません。
- DMZ内のデバイスに別のクライアント上のロボティクスが構成されている場合、このクライアントもDMZ内に存在しなければなりません。

第3章: ユーザーとユーザーグループ

ユーザー管理について

Data Protectorユーザー管理機能には、許可されていないユーザーからのシステムやデータへのアクセスを防ぐセキュリティレイヤー機能があります。

セキュリティは、ユーザーに関連するセキュリティコンセプトに基づいています。Data Protectorユーザーとして構成されたユーザーだけがData Protectorを使用できます。ユーザーグループを作成し、さまざまなユーザー権限を適切に割り当てることで、実際のセキュリティ要件に応じたData Protectorユーザーの構成を柔軟に設定できます。

デフォルトでは、バックアップしたデータにはバックアップのオーナーのみアクセスでき、他のユーザーに対しては不可視となります。他のユーザーに対しては、データがバックアップされているという事実さえも知らされません。他のユーザーに対してデータを可視にするには、適切なユーザー権限を使用します。

ユーザー

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。つまり、Data Protectorを使用するには、Data Protectorユーザーアカウントが必要です。小規模な環境では、1人でも十分にバックアップタスクを実行できます。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のユーザーインターフェイスを起動するか、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。

各ユーザーは、1つのユーザーグループのみに所属します。それによって、ユーザーのユーザー権限が定義されます。

UNIXユーザーとWindowsユーザーの両方を構成できます。

UNIX

ユーザーは、ログオン名、UNIXユーザーグループ、およびログオン元のシステムによって定義されます。ワイルドカード文字を使用できます。

Windows

ユーザーは、ログイン名、Windowsドメインまたはワークグループ、およびログオン元のシステムによって定義されます。ワイルドカード文字を使用できます。

定義済みユーザー

インストール直後の初期状態では、`admin`グループを除く、どのユーザーグループにもメンバーが含まれていません。`admin` Data Protectorグループには次のユーザーが追加されています。

Cell Manager	ユーザーアカウント	備考
UNIX Cell Manager	Cell Manager上のrootユーザー(root、*any group*、*Cell Manager host*)。	このユーザーアカウントは、変更しないでください。Cell Manager上のCRSデーモンなどのプロセスが正しく動作するために必要なアカウントです。 初期時にセルの管理が許されているのは、このユーザーのみです。他のクライアントからセルを管理するには、新しいユーザーを追加します。
Windows Cell Manager	Data Protectorのインストール時に指定されたCRSサービスアカウント(Cell Managerホストに限定)	CRSサービスのログインパラメーターを変更した場合を除き、CRSサービスアカウントは変更しないようにします。Cell Manager上のCRSデーモンなどのプロセスが正しく動作するために必要なアカウントです。
	Cell Managerをインストールしたユーザー(初期セル管理者)	このユーザーは初期セル管理者として構成され、どのクライアントからでもセルの管理を行えます。Data Protectorのインストールが終了した時点で、このユーザーアカウントを変更することをお勧めします。どのホストからでもアクセスできるようにするのではなく、セルの管理を行う特定のクライアントを指定してください。他のアカウントを使用する場合は、そのアカウントを追加し、その後、初期セル管理者を削除するか、または初期管理者にCell Managerからのアクセスのみを許可します。
	Cell Manager上のローカルシステムアカウント(SYSTEM、NT AUTHORITY、*Cell Manager host*)。	ローカルシステムアカウントとしてログインするようCRSサービスが構成された場合に備えて用意されるアカウントです。

環境内のユーザーの種類ごとに特定のグループを定義して、最小限の権限のみをユーザーに割り当てるようにすることをお勧めします。

javaユーザーの詳細については、『*HPE Data Protectorインストールガイド*』を参照してください。

> **重要:**
> Adminグループには、非常に強力な権限が与えられています。Data Protectorのadminユーザーグループのメンバーは、セル全体にわたってシステム管理者権限を持ちます。セキュリティの詳細については、『*HPE Data Protectorインストールガイド*』を参照してください。

ユーザーグループ

ユーザーグループは、同じ権限を持つユーザーの集まりです。管理者は、個々のユーザーを各自のアクセスの必要に応じてグループ化することで、ユーザーの構成を簡単にします。つまり管理者は、同じ権限を必要とするユーザーを1つのグループにまとめます。ユーザーが必要とする権限としては、セル内セッションの監視、バックアップの構成、ファイルの復元などがあります。

Data Protectorでは、デフォルトでユーザーグループがいくつか用意されています。これをそのまま利用することも、変更または新規に作成することもできます。

定義済みのユーザーグループ

Data Protectorには、構成作業を簡単に実施できるように、以下のユーザー権限を持つ3つの定義済みユーザーグループが用意されています。

ユーザー権限	管理者	オペレーター	ユーザー
クライアントの構成	✓		
ユーザーの構成	✓		
デバイスの構成	✓		
メディアの構成	✓	✓	
レポートと通知	✓		
バックアップ開始	✓	✓	
バックアップ仕様を開始	✓	✓	
バックアップ仕様を保存	✓		
ルートユーザーとしてバックアップ	✓		
セッションの所有権を切り替え	✓	✓	
モニター	✓	✓	
中止	✓	✓	
マウント要求	✓	✓	
復元の開始	✓	✓	✓
別のクライアントへ復元	✓		
別のユーザーから復元	✓	✓	
ルートユーザーとして復元	✓		
プライベートオブジェクトを表示	✓	✓	

インストール直後の初期状態では、どの定義済みユーザーグループにもメンバーがまだ含まれていません。ただし、adminユーザーグループは例外です。

> **重要:**
> 管理者には、非常に強力な権限が与えられています。Data Protector adminのユーザーグループのメンバーは、セル全体にわたってシステム管理者権限を持ちます。

Cell Managerで設定するユーザー権限によって、Cell Managerに接続するコンピューターからData Protector Cell Manager GUIまたはGUIコンテキストを使用できるかどうかが決まります。たとえば復元の開始ユーザー権限だけが設定されている場合、ユーザーインターフェイスコンポーネントをインストールしたときに利用できるのは[復元]コンテキストだけとなります。

利用可能なユーザー権限

Data Protectorには、さまざまなユーザー権限が用意されており、これらを適切に組み合わせることで高度なセキュリティを実現できます。ユーザー権限の詳細については、HPE Data Protectorヘルプを参照してください。

ユーザーへのWebサービスアクセスの提供

HPE Data Protectorは、Webサービスを使用して内部の通信と管理を行います。これらのWebサービスにアクセスするために、GUIなどの特定のHPE Data Protectorモジュールがデフォルトで構成されています。ただし、拡張GRE WebプラグインおよびREST APIなどの特定のモジュールの場合、ユーザーにWebサービスアクセスを明示的に提供する必要があります。

HPE Data ProtectorまたはCLIのいずれかを使用してWebサービスアクセスを提供できます。

> **注:**
> Webアクセスは、Data Protector**ユーザー**クラスのメンバーに対して有効にすることはできません。

HPE Data Protector GUIの使用

以下の手順を実行します。

1. コンテキストリストで、**[ユーザー]**をクリックします。
2. Scopingペインで**[ユーザー]**を展開し、Webサービスへのアクセスを提供するユーザーを選択します。
3. [HPE Data Protector ユーザー]ダイアログボックスの[プロパティ]の[一般]タブで、**[Webアクセス]**チェックボックスを有効にします。認証ウィンドウが開きます。
4. [パスワード]テキストボックスにパスワードを入力して、**[OK]**をクリックします。
5. **[適用]**をクリックします。

CLIの使用

新しいユーザーを作成するかまたは既存のユーザーのプロパティを更新するかによって、次のコマンドのいずれかを実行します。

- Webサービスへのアクセス権を持つ新しいユーザーを作成する場合:
  `omniusers -add -type {U | W} -name <UserName> -webaccess enable -passwd <Password>`
- 既存のユーザーを更新する場合:
  `omniusers -webaccess enable -name UserName -passwd Password -group GroupOrDomainName -client ClientName`

詳細については、`omniusers`*HPE Data Protector Command Line Interface Reference*を参照してください。

ユーザーの構成

ユーザーを追加する

あるユーザーがData Protectorを使用できるようにするには、そのユーザーを既存のユーザーグループに追加します。

前提条件

ユーザーを追加するには、[ユーザーの構成]権限が必要です。

手順

1. コンテキストリストで、**[ユーザー]**をクリックします。
2. Scopingペインで**[ユーザー]**を展開します。
3. ユーザーの追加先となるユーザーグループを右クリックします。
4. **[ユーザーの追加/削除]**をクリックして、ウィザードを起動します。
5. [ユーザーの追加/削除]ダイアログに特定のユーザープロパティを入力します。**[名前]**および**[グループ/ドメイン]**または**[UNIXグループ]**に情報を入力するときは、ネットワーク上の既存のユーザーに関する情報を入力する必要があります。
6. **[>>]**をクリックしてユーザーをユーザーリストに追加します。

   > **ヒント:**
   > ユーザーリストからユーザーを選択し、**[<<]**をクリックすると、ユーザーを削除できます。

7. **[完了]**をクリックしてウィザードを終了します。

指定したユーザーがユーザーグループに追加されます。このユーザーには、追加先のグループに割り当てられているユーザー権限が付与されます。

ユーザーを表示する

このプロセスを使って、特定のユーザーのプロパティを表示させます。

前提条件

操作を行うユーザーがすでにData Protectorユーザーになっていること。

手順

1. コンテキストリストで、**[ユーザー]**をクリックします。
2. Scopingペインで**[ユーザー]**を展開します。
3. ユーザーが所属しているユーザーグループをクリックします。
4. [結果エリア]で、表示対象のユーザーをダブルクリックします。

指定したユーザーのプロパティが[結果エリア]に表示されます。

ユーザープロパティを変更する

Data Protectorユーザーの構成時に指定したユーザープロパティは、後から変更できます。ただし、ユーザーのユーザー権限を変更するには、ユーザーを他のグループに移動する必要があります。

前提条件

ユーザープロパティを変更するには、[ユーザーの構成]権限が必要です。

手順

1. コンテキストリストで、**[ユーザー]**をクリックします。
2. Scopingペインで**[ユーザー]**を展開します。
3. ユーザーが所属しているユーザーグループをクリックします。
4. [結果エリア]で、変更対象のユーザーを右クリックします。
5. **[プロパティ]**をクリックします。
6. プロパティの設定を変更します。**[名前]**および**[グループ/ドメイン]**または**[UNIXグループ]**の情報を変更するときは、ネットワーク上の既存のユーザーに関する情報を入力する必要があります。
7. **[適用]**をクリックします。

他のユーザーグループにユーザーを移動する

特定のユーザーのユーザー権限を変更するには、そのユーザーを別のユーザーグループに移動します。

前提条件

ユーザーを移動するには、[ユーザーの構成]権限が必要です。

手順

1. コンテキストリストで、**[ユーザー]**をクリックします。
2. Scopingペインで**[ユーザー]**を展開します。
3. ユーザーが所属しているユーザーグループをクリックします。
4. [結果エリア]で、移動対象のユーザーを右クリックします。
5. **[移動]**をクリックします。
6. [ターゲットグループ]リストで、適切なユーザーグループ名を選択して**[OK]**をクリックします。

指定したユーザーが元のユーザーグループから削除され、指定したユーザーグループに追加されます。このユーザーには、移動先のユーザーグループの権限が適用されます。

ユーザーを削除する

ここでは、ユーザーが現在構成されているユーザーグループからユーザーを削除する手順を示します。

前提条件

ユーザーを削除するには、[ユーザーの構成]権限が必要です。

手順

1. コンテキストリストで、**[ユーザー]**をクリックします。
2. Scopingペインで**[ユーザー]**を展開します。
3. ユーザーが所属しているユーザーグループをクリックします。
4. [結果エリア]で、削除対象のユーザーを右クリックし、**[削除]**をクリックします。
5. 確認メッセージが表示されたら、操作を続行してよいことを確認してください。

指定したユーザーがユーザーグループから削除されます。そのユーザーは、Data Protectorを使用できなくなります。

> **ヒント:**
> [ユーザーの追加/削除]ダイアログでもユーザーを削除できます。

ユーザーグループの構成

ユーザーグループを追加する

通常は、デフォルトのData Protectorユーザーグループで十分です。独自のユーザーグループを定義して、ニーズに合わせてData Protector環境で権限の割り当てを制御することができます。ただし、既存のグループを変更するだけでニーズを満たせる可能性もあります。既存のグループを変更するだけではニーズを満たせない場合にのみ、新しいグループを追加するようにしてください。

前提条件

[ユーザーの構成]権限が付与されたアカウントを使用する必要があります。

手順

1. コンテキストリストで、**[ユーザー]**をクリックします。
2. Scopingペインで**[ユーザー]**を右クリックします。
3. **[ユーザーグループの追加]**をクリックして、ウィザードを起動します。
4. 新しいグループの名前と説明を入力します。
5. **[次へ]**をクリックします。
6. 新しいグループに適用するユーザー権限を設定します。
7. **[完了]**をクリックしてウィザードを終了します。

新しいユーザーグループがData Protectorに追加されます。このグループには、まだメンバーが登録されていません。

ユーザーグループを表示する

このプロセスを使って、特定のユーザーグループのプロパティを表示させます。

前提条件

操作を行うユーザーがすでにData Protectorユーザーになっていること。

手順

1. コンテキストリストで、**[ユーザー]**をクリックします。
2. Scopingペインで**[ユーザー]**を展開します。
3. ユーザーグループを右クリックします。
4. **[プロパティ]**をクリックします。

指定したユーザーグループのプロパティが[結果エリア]に表示されます。

ユーザー権限を変更する

(adminユーザーグループ以外の)任意のユーザーグループに割り当てられているユーザー権限は、実際のニーズに応じて変更できます。ユーザーグループには、少なくとも1つのユーザー権限を割り当てる必要があります。また、グループ内の各ユーザーのプロパティ(ユーザーが属するドメイン、ユーザーの本名、およびユーザーのユーザーグループなど)を変更することもできます。ユーザーがまったく属していないグループを選択すると、そのグループのプロパティが[結果エリア]に表示されます。ユーザーが属しているグループを選択すると、それらのユーザーのリストが[結果エリア]に表示されます。変更したいプロパティを持つユーザーをクリックすることによっても、ユーザーグループ内の各ユーザーのプロパティを変更することができます。

前提条件

- ユーザーグループがadminユーザーグループでないこと。
- User configuration権限を持つこと。

手順

1. コンテキストリストで、**[ユーザー]**をクリックします。
2. Scopingペインで**[ユーザー]**を展開します。
3. 変更対象のユーザーグループを右クリックします。
4. **[プロパティ]**をクリックし、**[ユーザー権限]**タブをクリックします。
5. 権限を必要に応じて変更します。すべてのユーザー権限をユーザーグループに割り当てるには、**[すべてを選択]**をクリックします。多数のユーザー権限を変更する必要がある場合は、**[すべてを解除]**をクリックしてユーザーグループからすべての権限を削除した後、少なくとも1つの権限をグループに追加します。
6. **[適用]**をクリックします。

指定したユーザー権限がユーザーグループに割り当てられ、そのグループに所属しているすべてのユーザーに適用されます。

ユーザーグループを削除する

不要になったユーザーグループ(adminグループ以外)は削除できます。

前提条件

- ユーザーグループがadminユーザーグループでないこと。
- User configuration権限を持つこと。

手順

1. コンテキストリストで、**[ユーザー]**をクリックします。
2. Scopingペインで**[ユーザー]**を展開します。
3. 削除対象のユーザーグループを右クリックします。
4. **[削除]**をクリックします。

指定したユーザーグループがData Protectorから削除されます。このとき、グループに所属しているユーザーはすべて削除されます。

第4章: 内部データベース

IDBについて

内部データベース(IDB)とは、Cell Manager上に配置される、Data Protectorの内部データベースです。バックアップ対象のデータとバックアップデータの格納先メディアのほか、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、メディア管理の各セッションの結果や、構成済みのデバイスとライブラリなどに関する情報を保持します。

IDBを使用する理由

IDBに保存された情報を利用することで、以下のことが可能になります。

- 復元手順の効率化

  復元対象のファイルとディレクトリをブラウズできます。復元に必要なメディアをすばやく検索できるので、復元をすばやく実行できます。

- バックアップ管理

  バックアップセッションの結果を確認できます。

- メディア管理

  バックアップ、オブジェクトコピー、およびオブジェクト集約のセッション中にメディアを割り当てたり、メディア管理操作およびメディア属性を追跡したり、メディアを異なるメディアプールにグループ化して、テープライブラリ中のメディア位置を追跡したりすることができます。

- 暗号化/復号化管理: IDBに保存されている情報によって、Data Protectorが暗号化されたバックアップまたはコピーセッション用に暗号化キーを割り当て、暗号化されたバックアップオブジェクトの復元に必要な復号キーを提供することが可能になります。

IDBのサイズと増大に関する考慮事項

IDBのサイズが非常に大きくなることがあり、バックアップのパフォーマンスとCell Managerシステムの動作に大きく影響する可能性があります。Data Protector管理者は、IDBについて十分理解し、どの情報をどのくらいの期間にわたってIDBに維持するかを決定する必要があります。復元時間および機能性の側面とIDBのサイズと増加の側面のバランスを取るのは、管理者の役目です。Data Protectorでは、これらのバランスをとる上で特に重要なパラメーターとして、ロギングレベルとカタログ保護の2つがあります。

IDBの定期的バックアップ

HPEIDBを定期的にバックアップすることを強くお勧めします。詳細については、「IDBバックアップの構成」を参照してください。

IDBアーキテクチャー

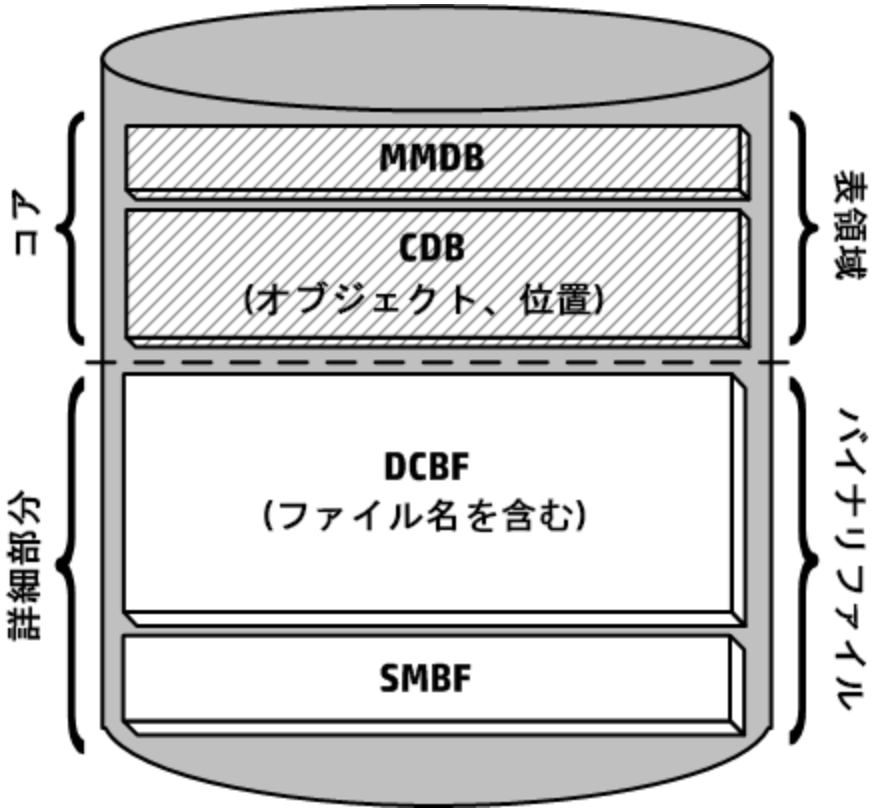
内部データベース(IDB)は、以下の部分からなります。

- メディア管理データベース(MMDB)
- カタログデータベース(CDB)
- 詳細カタログバイナリファイル(DCBF)
- セッション メッセージ バイナリ ファイル(SMBF)
- 暗号化キーストアとカタログファイル

IDBの各部分は、特定のData Protector情報(レコード)を格納し、IDBのサイズと増加にさまざまな影響を与えます。各部分はCell Manager上の個別のディレクトリに置かれます。

IDBの構成要素

データベースアーキテクチャー



MMDBとCDBの各部分は、テーブルスペースを含む組み込みデータベースを使って実装されています。このデータベースは、`hpdp-idb`、`hpdp-idb-cp`、および`hpdp-as`プロセスにより制御されます。CDB(オブジェクトと位置)およびMMDBは、IDBのコア部分となります。

IDBのDCBFおよびSMBFの各部分はバイナリファイルで構成されています。更新は、トランザクションログを経由せず、直接行われます。

Manager-of-Managers(MoM)環境では、MMDBをセントラルシステムに移動することで、集中メディア管理データベース(CMMDB)を構築できます。

メディア管理データベース(MMDB)

MMDBレコード

メディア管理データベースには、以下の項目に関する情報が格納されます。

- 構成されているデバイス、ライブラリ、ライブラリドライブ、スロット
- Data Protectorメディア
- 構成されているメディアプールとメディアマガジン

MMDBのサイズと増加

MMDBのサイズはそれほど大きくなりません。MMDBの大部分は、Data Protectorメディアに関する情報が占めるのが普通です。

MMDBの位置

MMDBは、以下のディレクトリに格納されます。

Windowsシステムの場合: *Data_Protector_program_data*\server\db80\idb

UNIXシステムの場合: /var/opt/omni/server/db80/idb

カタログデータベース(CDB)

CDBレコード

カタログデータベースには、以下の項目に関する情報が格納されます。

- 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各セッションに関する情報。これは、Data Protectorモニターウィンドウに送信された情報のコピーです。
- バックアップされたオブジェクトとそのバージョン、およびオブジェクトコピーに関する情報。暗号化されたオブジェクトバージョンの場合、キーID(KeyID-StoreID)も格納されます。
- バックアップしたオブジェクトのメディア上の位置。Data Protectorは、各バックアップオブジェクトについて、バックアップに使用するメディアやデータセグメントの情報を保存します。オブジェクトコピーとオブジェクトのミラーリングについても同様です。

CDB(オブジェクトと位置)のサイズと増加

CDBレコードは、IDBのうち、ごく一部のスペースを占有します。

CDBの位置

CDBは、以下のディレクトリに格納されます。

Windowsシステムの場合: *Data_Protector_program_data*\server\db80\idb

UNIXシステムの場合: /var/opt/omni/server/db80/idb

詳細カタログバイナリファイル(DCBF)

DCBF情報

詳細カタログバイナリファイル部分には以下の項目に関する情報が格納されます。

- バックアップファイルのパス名(ファイル名)とクライアントシステム名に関する情報。バックアップとバックアップの間に作成されたファイルのファイル名はDCBFに追加されます。
- ファイルメタデータ。これは、バックアップされたファイルバージョン、そのファイルサイズ、変更時刻、属性/保護、およびバックアップメディア上のバックアップコピーの場所に関する情報です。

バックアップに使用した各Data Protectorメディアにつき、DC(詳細カタログ)バイナリファイルが1つずつ作成されます。メディアが上書きされると、古いバイナリファイルが削除され、新しいバイナリファイルが作成されます。

DCBFのサイズと増加

[すべてログに記録]オプションを使用してファイルシステムのバックアップを行うのが一般的な環境では、DCBFはIDBで最も大きな割合を占めます。ロギングレベルとカタログ保護を使うと、IDB内に実際にどのようなデータをどれくらいの期間保存するかを指定できます。

デフォルトでは、DCバイナリファイル用にDCディレクトリが5つ構成されます。バックアップメディア数、またはDCバイナリファイル数が極めて大きい場合、またはディスク容量に問題がある場合、さらにDCディレクトリを作成して、IDBサイズを拡張できます。

DCBFのうち、サイズとその増加率が最も大きいのはファイル名部分です。

ファイル名部分のサイズの増大は、バックアップの数と同様に、バックアップ環境のサイズの増大と変動率に比例します。

IDB内のファイルまたはディレクトリは約100バイトを占めます。

DCBFの位置

デフォルトでは、DCBFは以下のディレクトリの、dcbf0～dcbf4というサブディレクトリに格納されます。

Windowsシステムの場合: *Data_Protector_program_data*\server\db80\dcbf

UNIXシステムの場合: /var/opt/omni/server/db80/dcbf

Cell Manager上のディスクスペースを考慮し、必要に応じてDCディレクトリの位置を変更してください。DCディレクトリを他に作成して、異なるディスクに置くこともできます。

セッション メッセージ バイナリファイル(SMBF)

SMBFレコード

セッションメッセージバイナリファイル(SMBF)部分には、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各セッションで生成されたセッションメッセージが保存されます。バイナリファイルは、セッションごとに1つずつ生成されます。バイナリファイルは、年と月に基づいて分類されます。

SMBFのサイズと増加

SMBFのサイズは、以下の要因に依存します。

- 実行されたセッションの数。
- セッション中のメッセージ数。1つのセッションメッセージは約200バイトを占めます。バックアップ、復元、およびメディア管理の実行中に表示されるメッセージの量は、[レポートレベル]オプションを通じて変更できます。これは、IDBに保存されるメッセージの量に影響します。

SMBFの位置

SMBFは、以下のディレクトリに格納されます。

Windowsシステムの場合: *Data_Protector_program_data*\server\db80\msg

UNIXシステムの場合: /var/opt/omni/server/db80/msg

SessionMessageDirグローバルオプションを編集してディレクトリの場所を変更することもできます。

暗号化キーストアとカタログファイル

暗号化されたバックアップ中に手動または自動で作成されたすべてのキーは、キーストアに保存されます。キーは、オブジェクトコピー、オブジェクト検証、および復元の各セッションにも使用できます。ハードウェア暗号化の場合、これらのキーはオブジェクト集約セッションにも使用できます。

ソフトウェア暗号化の場合、キーID(各キーIDはkeyIDとStoreIDで構成される)は、暗号化されたオブジェクトバージョンにマップされます。このマッピングはカタログデータベースに格納されます。メディア内の異なるオブジェクトに、異なる(ソフトウェア)暗号化キーを設定できます。

ハードウェア暗号化の場合、キーIDがメディアIDにマップされ、これらのマッピングはカタログファイルに保存されます。このファイルは、暗号化メディアを別のセルにエクスポートするのに必要な情報を含みます。

キーストアの位置

キーストアは、以下のディレクトリに格納されます。

Windowsシステムの場合: *Data_Protector_program_data*\server\db80\keystore

UNIXシステムの場合: /var/opt/omni/server/db80/keystore

カタログファイルの位置

カタログファイルは、以下のディレクトリに格納されます。

Windowsシステムの場合: *Data_Protector_program_data*\server\db80\keystore\catalog

UNIXシステムの場合: /var/opt/omni/server/db80/keystore/catalog

IDBの操作

ここでは、以下のData Protector操作時におけるIDBの動作について説明します。

- バックアップ
- 復元
- オブジェクトコピーおよびオブジェクト集約
- オブジェクト検証
- メディアのエクスポート
- 詳細カタログの削除

バックアップ

バックアップセッションが開始されると、IDBにセッションレコードが作成されます。また、セッションの各オブジェクトについて、オブジェクトバージョンレコードが作成されます。どちらのレコードもCDB部分に保存され、いくつかの属性を持ちます。バックアップ中にバックアップセッションマネージャーがメディアを更新します。すべてのメディアレコードはMMDB部分に保存され、ポリシーに従ってバックアップに割り当てられます。

データセグメント(およびそれに続くカタログセグメント)がテープに書き込まれると、そのデータセグメントに含まれているオブジェクトバージョンのそれぞれについて、メディア位置レコードがCDBに書き込まれます。また、カタログが詳細カタログ(DC)バイナリファイルに保存されます。Data Protectorメディア1つにつき、1つのDCバイナリファイルが保持されます。DCバイナリファイル名は、*MediumID_TimeStamp*.datです。この名前は、バックアップが同じメディアに追記されても変更されません。バックアップ中にメディアが上書きされると、そのメディアのDCバイナリファイルが削除され、新しいDCバイナリファイルが作成されます。

バックアップ中に生成されたすべてのセッションメッセージは、セッションメッセージバイナリファイル(SMBF部分)に保存されます。

IDBバックアップとアーカイブログファイル

内部データベースバックアップの仕様の構成に応じて、IDBバックアッププロセスは、古いアーカイブログファイルを削除し、IDB回復に必要な新しいアーカイブログファイルの作成を開始できます。

復元

復元の構成時に、Data Protectorはユーザーがバックアップデータの仮想ファイルシステムをブラウズできるように、CDB部分およびDCBF部分に対する一連の照会を実行します。これらのブラウズ照会は、2段

階で行われます。最初の段階では、特定のオブジェクト(ファイルシステムまたは論理ドライブ)を選択します。そのオブジェクトに多数のバックアップバージョンが保存されている場合、Data ProtectorはDCBFをスキャンしてブラウズ用のルックアップキャッシュを作成するので、多少時間がかかることがあります。第2段階では、ディレクトリをブラウズします。

特定のファイルバージョンを選択すると、Data Protectorが必要なメディアを特定し、選択したファイルに使用されているメディア位置レコードを検索します。これらのメディアはMedia Agentから読み込まれ、選択したファイルを復元するDisk Agentに詳細が送信されます。

オブジェクトコピーおよびオブジェクト集約

オブジェクトコピーセッションやオブジェクト集約セッションでは、バックアップセッション時および復元セッション時に実行される処理と同じ処理が実行されます。基本的には、データは復元されるときと同様にソースメディアから読み取られ、バックアップされるときと同様にターゲットメディアに書き込まれます。IDBの操作という点では、オブジェクトコピーセッションまたはオブジェクト集約セッションで行われることと、バックアップと復元で行われることは同じです。詳細については、以下の説明を参照してください。

オブジェクト検証

オブジェクト検証セッション中に、復元セッション中と同じデータベースプロセスが実行されます。基本的に、データは復元している場合のようにソースメディアから読み込まれ、確認を実行するホストDisk Agentに送信されます。IDB操作という点では、オブジェクト検証セッションで行われることと、復元セッションで行われることは同じです。詳細については、上記の「復元」セクションを参照してください。

検証セッション中に生成されるすべてのセッションメッセージは、セッションメッセージのバイナリファイルに保存されます。

メディアのエクスポート

メディアのエクスポート時には、以下の項目が削除されます。

- メディアのすべてのメディア位置レコードがCDB部分から削除されます。
- 他のメディア上に配置されていないオブジェクトがすべてCDB部分から削除されます。
- 古いセッション(メディアが上書きまたはエクスポートされているセッション)が削除されます。また、このようなセッションのセッションメッセージも削除されます。
- MMDB部分からメディアレコードが削除され、そのメディアのDCバイナリファイルがDCBF部分から削除されます。

詳細カタログの削除

特定のメディアから詳細カタログを削除すると、対応するDCバイナリファイルが削除されます。メディア上のすべてのオブジェクトバージョンに対するカタログ保護を削除した場合も同じ結果になります(バイナリファイルは、DCバイナリファイルに対して次に行う日常の保守作業で削除されます)。その他のすべてのレコードは、CDB部分およびMMDB部分に保持され、これらのメディアから復元を行えます(ただし、ブラウズはできません)。

内部データベースの構成

IDBの構成

内部データベース(IDB)を構成することにより、以下の項目が管理しやすくなります。

- IDBのサイズと利用可能なディスクスペース
- IDBディレクトリの位置
- IDB自体のバックアップ(IDBの破損/障害時に必要)
- IDBレポートおよび通知の構成

任意の時点でIDBを回復できるようにするため、あらかじめ準備をしておく必要があります。IDBの回復により、IDBに格納されている情報が復元されます。IDBの回復は、Cell Managerが障害発生によって影響を受けたときにバックアップされているデータの復元にとって不可欠です。IDBの回復準備作業は以下のとおりです。

- 堅牢性に関する考慮事項の確認
- IDBディレクトリの再配置
- IDBバックアップの構成
- IDBの定期的なバックアップ

IDBを構成し終えれば、保守の必要性が最小限になり、通知やレポートがあったときの対処が主な保守タスクとなります。

IDB用のディスクスペースの割り当て

時間とともに、内部データベース(IDB)が、Cell Manager上のディスクスペースのうちかなりの部分を占有する可能性があります。IDB用のディスクスペース割り当ては、今後のニーズを十分に見据えて計画しておく必要があります。

前提条件

- ファイル数、ファイルの変動率、環境規模の拡張など、IDBのサイズ増加に影響を及ぼす主な要因について理解しておく必要があります。
- 環境の要件と使用可能なディスクスペースに応じて、ロギングレベルとカタログ保護ポリシーを設定する必要があります。
- 今後のIDBのサイズ(IDBの今後のニーズを満たすために必要なディスクスペース)を見積もる必要があります。

ディスクスペースの必要量

IDBに必要となるディスクスペースは、バックアップの定義と実行に関するさまざまな構成条件とポリシーによって大きく異なります。

ここでは、3か月後に約900MBのディスクスペースが必要になり、それ以降のサイズ増加がごくわずかにとどまる環境の場合のシナリオを簡略化して示します。

- バックアップ対象となるシステムは、100台(10000ファイル/システム、メールサーバーなし)
- 総データ量は350GB。
- 典型的な変動率(1か月あたりの新ファイル3%)でのファイルシステムバックアップ。
- 1週間あたり1回のフルバックアップと4回の増分バックアップを計画。
- ロギングレベルを[すべてログに記録]に設定(復元前にファイル名を容易に参照できるようにするため)。これはディスクスペースを最も消費するログオプションです。
- カタログ保護は、フルバックアップに対しては3か月、増分バックアップに対しては2週間に設定。

> **注:**
> 構成規模が大きい場合や、IDB内のカタログの保護期間が長い場合は、IDB用スペースが20GB以上必要になる可能性があります。

事前に計画しておくべきこと

IDBのサイズは、特に使用開始直後(カタログの維持期限に達するまでの間)急速に増加するのが普通です。その後のサイズ増加率は、1か月あたりの新規ファイル数の割合が高いシステムの変動率や、環境規模の拡大(バックアップ対象のシステムの追加)などの要因によって決まります。

IDBのサイズ増加要因の違いを理解しておくことが重要です。

- IDBのファイル名とファイルメタデータを含む部分のサイズは、バックアップ数、セル内のバックアップファイル数、およびカタログ保護の期間に比例して増加します。
- アーカイブログファイルが占めるストレージ容量の予測は容易ではありません。バックアップ対象の新しいファイル名の数やIDBバックアップ間の総体的なバックアップアクティビティ(スケジュール済みバックアップが主体の場合は、週数)が主なサイズ増加要因となります。

IDBディレクトリの位置

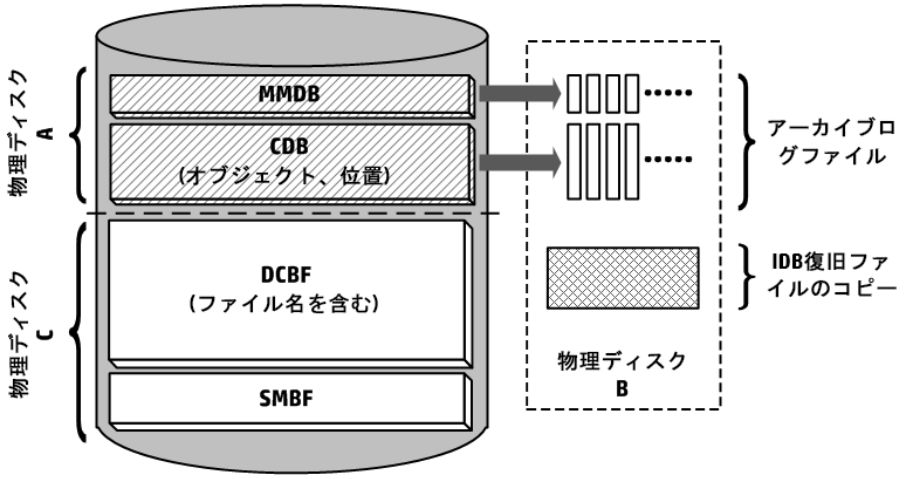
内部データベース(IDB)は、Cell Manager上に置かれます一部のIDBディレクトリを別の場所に移動して推奨条件を満たすことで、堅牢性を強化することができます。

制限事項

- IDBファイルは、ローカルに接続されている(NFSを使ってマウントされたり、ネットワーク共有フォルダーとしてマップされていない)ディスク上のボリュームにのみ保存できます。
- IDBをクラスター内にインストールする場合は、クラスターグループ(Microsoftサーバークラスター)またはクラスターパッケージ(HPE Serviceguard)内のボリュームにインストールする必要があります。
- IDBをクラスター内にインストールする場合は、クラスターグループ(Microsoftサーバークラスター)、クラスターパッケージ(HPE Serviceguard)またはクラスターサービスグループ(Symantec Veritasクラスターサーバー)内のボリュームにインストールする必要があります。

IDBディレクトリの推奨位置

IDB	Windowsシステムにおける位置	UNIXシステムにおける位置	位置変更の可否
表領域 (CDB、MMDB)	*Data_Protector_program_data*\server\db80\idb *Data_Protector_program_data*\server\db80\jce *Data_Protector_program_data*\server\db80\pg	/var/opt/omni/server/db80/idb /var/opt/omni/server/db80/jce /var/opt/omni/server/db80/pg	ディレクトリパスは固定されていますが、異なるボリュームのマウントは可能です。
バイナリファイル (DCBF、SMBF)	*Data_Protector_program_data*\server\db80\dcbf *Data_Protector_program_data*\server\db80\msg *Data_Protector_program_data*\server\db80\meta	/var/opt/omni/server/db80/dcbf /var/opt/omni/server/db80/msg /var/opt/omni/server/db80/meta	ディレクトリパスは変更可能です。また、別のボリュームもマウントできます。
アーカイブログファイル	*Data_Protector_program_data* \server\db80\pg\pg_xlog_archive	/var/opt/omni/server/db80/pg/pg_xlog_archive	ディレクトリパスは固定されていますが、異なるボリュームのマウントは可能です。
IDB復旧ファイル	*Data_Protector_program_data* \server\db80\logfiles\rlog	/var/opt/omni/server/db80/logfiles/rlog	ファイルのコピーは、任意の場所に置くことができます。



堅牢性に関する留意事項

- IDBのコア部分であるCDB(オブジェクト、位置)およびMMDBは、Data Protectorの運用に不可欠です。
- バックアップと復元など、Data Protectorの基本操作は、IDBのDCBF部分とSMBF部分が存在しなくても実行可能です。しかし、これらが存在しない場合は、復元対象のファイル名をブラウズできず、またセッションメッセージが失われます。
- IDB復旧ファイルおよびアーカイブログファイルが失われた場合、通常の操作には支障をきたしませんが、IDBの復元がかなり困難になり、前回のIDBバックアップ以降に生成されたIDBデータを再生できなくなります。代わりに、使用したメディアの再インポートが必要になります。

IDBバックアップの構成

HPE Data Protectorのセルの管理では、IDB自体のバックアップを構成することが非常に重要です。障害への準備において最も重要なタスクは、IDBバックアップを定期的に行うことです。Cell Managerに障害が発生した場合、IDBのオフライン復旧はその他のバックアップデータの復元に不可欠です。

IDB用のバックアップ仕様を作成するには、バックアップコンテキストのScopingペインで**内部データベース**を選択して、標準バックアップ手順に従います。詳細については、バックアップ仕様を作成するを参照してください。

IDBのバックアップ仕様の準備と実行に関するヒント

IDBバックアップの構成時には、次の点に注意してください。

- IDBバックアップを少なくとも1日1回実行するようにスケジュールを設定します。これにより、最新のIDBバックアップが常に維持されます。スケジュールは、Cell Managerの負荷が少ない時刻に設定します。

> **注意:**
> IDB構成になんらかの変更(内部データベースサービスとアプリケーションサーバーユーザーアカウントのパスワードの変更など)を行った場合、内部データベースを常にバックアップします。これを

> 怠ると、オンラインIDB復元とオフラインIDB復旧が正常に実行できなくなる場合があります。

- IDBバックアップに使用するデバイスおよびメディアの種類によって、障害発生後のIDBの復元の容易さ(難しさ)や可能性が大きく変わります。
  - 自動構成で構成できるデバイスを使用すると、非常に簡単にデバイスを構成できます。
  - ファイルジュークボックスデバイスを使用する場合は、IDBのあるドライブとは別のディスクドライブ上のジュークボックスを必ず使用してください。
  - 可能な限り、Cell Managerにローカルに接続されたデバイスを使用してください。
  - ファイルライブラリは、ファイルライブラリメディアをインポートできないため使用しないでください。
  - StoreOnceソフトウェア(SOS)メディアのインポートは複雑なこともあるため、SOSメディアのインポート手順が記述されており、検証が済んでいる場合は、SOSデバイスのみをIDBバックアップに使用してください。IDBバックアップは、別個のメディアプールを使用し、別個のバックアップメディア上で、専用のバックアップデバイスに行ってください。
  - どのメディアをIDBバックアップに使用するかを確認しておきます。**[セッションメディアレポート]**を構成しておくと、バックアップに使用するメディアに関する情報を確認できます。これにより、復元手順が大幅に効率化されます。
- データとカタログの保護を設定し、ビジネスニーズを十分に満たすIDBバックアップのコピーが存在するようにしてください。
- IDBの自動整合性チェックは、やむを得ない場合を除き無効にしないでください。整合性チェックを制御する[内部データベースのチェック]バックアップオプションは、デフォルトでオンです。
- IDBバックアップを暗号化すると、データの機密性を高めることができます。IDBバックアップにはキーストアが含めます。

> **注:**
> IDBバックアップ中に新しいキーを作成することはできないため、暗号化されたIDBバックアップを開始する前に、アクティブな暗号化キーが必要です。
> 暗号化されたIDBバックアップ時、暗号化キーは、`IDBClientName-keys.csv`ファイルに自動的にエクスポートされます。このファイルは、暗号化キーがエクスポートされるデフォルトのHPE Data Protectorディレクトリにあります。
> バックアップ後のキーの取り扱いには細心の注意を払ってください。障害発生時には、このキーが復元に必要です。暗号化されたIDBバックアップを実行した後は、対応するキーを安全な場所にコピーしてください。

- IDBバックアップに使用するデバイスおよびメディアの種類によって、障害発生後のIDBの復元の容易さ(難しさ)や可能性が大きく変わります。StoreOnceソフトウェア(SOS)メディアのインポートは複雑なこともあるため、SOSメディアのインポート手順が記述されており、検証が済んでいる場合は、SOSデバイスのみをIDBバックアップに使用してください。IDBバックアップは、別個のメディアプールを使用し、別個のバックアップメディア上で、専用のバックアップデバイスに行ってください。

> **注: 注**: ディザスタリカバリ後にインポートされたStoreOnceソフトウェア(SOS)メディアへのIDBバックアップはサポートされていません。

- DP IDBの復元については、手順を文書化し、検証することを強くお勧めします。

内部データベースの保守

IDBの保守について

内部データベース(IDB)の通知とレポートが構成済みであれば、保守作業を実行する必要が生じたときに通知が行われます。どの保守タスクを実行すべきかは、現在のIDBの状況によって異なります。

状況	* 通知/レポート[1]	保守タスク
IDBのスペースが不足している場合	[IDBのスペース不足]通知	IDBサイズを拡張する IDBのサイズ増加率を減らす IDBの現在のサイズを縮小する
IDBのサイズをチェックしたい場合	IDBサイズのレポート	IDBのサイズをチェックする
IDBが正しく動作しない(破損の可能性がある)場合	[IDBの破損]通知	IDBの整合性をチェックする

[1] 通知およびレポートは、事前に構成しておかないと出力されません。

> **注:**
> HPEでは、Data Protectorイベントログを定期的にチェックし、起こりうるIDBイベントを確認することをお勧めします。管理者は、通知に対してすばやく対応できるように、電子メールによる通知の送信を検討してみてください。

内部データベースのサイズ増加とパフォーマンス

IDBのサイズ増加とパフォーマンスについて

内部データベース(IDB)の構成と保守にあたっては、IDBのサイズ増加とパフォーマンスに影響する主な要因とパラメーターについて理解しておく必要があります。

ここでは、ファイルシステムバックアップにおける最悪のケース(IDBサイズが上限に達したか、または急激に増加している場合)を示します。ディスクイメージバックアップ、アプリケーション統合バックアップ、またはNDMPバックアップを実行する場合、IDBに格納されるデータはごく少量です。

IDBの主なサイズ増加要因

IDBのサイズ増加は、環境によって異なり、Data Protectorがファイルのブラウズおよび検索用に保持する履歴および詳細を定義するData Protector設定値にも依存します。

主な要因	IDBのサイズ増加に与える影響

環境のファイルとサイズに関する詳細	Data Protectorでは、各ファイルバージョンを追跡できます。このために、バックアップのたびに、1個のファイル名レコード(約100バイト)が、バックアップされた各ファイルのDCBF部に格納されます。
(フル)バックアップの頻度	バックアップの実行頻度が高いほど、IDB内に格納される情報が増えます。ファイルシステムの変動率が低い場合、DCBF部のサイズだけが増加します。
オブジェクトコピーの数	作成するオブジェクトコピーおよびオブジェクトミラーの数が多いほど、IDBに格納される情報量が増えます。オブジェクトコピーとオブジェクトミラーについても、バックアップされたオブジェクトと同じ情報がIDBに格納されます。

IDBの主なパフォーマンス要因

主な要因	バックアップ中のIDB負荷とパフォーマンスへの影響
並行ドライブの数	並行して動作するドライブ(テープ)の数は、IDB上の負荷に影響します。たとえば、10件のバックアップセッションで10基のドライブが並行して動作する場合や、5件のセッションで10基のドライブが動作している場合、データベースに対する負荷はほとんど同じです。新しいドライブが増えるたびに、データベースに格納しなければならないファイルカタログが増えます。
平均ファイルサイズ	バックアップするファイルのサイズが小さいほど、ファイルカタログが急速に生成されるので、IDBへの負荷が高くなります。
IDBのディスクパフォーマンス	バックアップ中にData Protectorが行う処理は、ディスクに対するデータの読み書きが中心です。したがって、IDBに使用されているCell Manager上のディスク(サブシステム)の速度が、パフォーマンスの決定要因となります。

IDBのサイズ増加とパフォーマンスに関する主なパラメーター

主なパラメーター	IDBのサイズ増加に与える影響	IDBのパフォーマンスに与える影響
ロギングレベル	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に書き込むか、および必要なストレージ容量を定義します。	復元するデータのブラウズのしやすさに影響します。
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。 カタログ保護が期限切れになっても、即座にデータがIDBから削除されるわけではありません。メディア全体のすべてのデータのカタログ保護が切れた時点で削除されます。	ありません。

実際のIDBのサイズ増加は、設定されるカタログ保護の期間(比較的短い期間、データ保護と同じ期間など)および有効なロギングレベルにより異なります。カタログ保護が終了するまで、IDBは高い増加率で増加します。それ以降は、バックアップ環境に応じた最小限の増加率になります。

ロギングレベルがIDBに及ぼす影響

ロギングレベルの設定の違いにより、内部データベースのサイズ増加率や復元対象ファイルシステムのブラウズのしやすさが影響されます。また、バックアップのパフォーマンスも稀に影響を受けます。

ここでは、ファイルシステムバックアップの場合のシナリオを示します。ディスクイメージバックアップ、オンラインデータベースバックアップ、またはNDMPバックアップを実行する場合、IDBに格納されるデータはごく少量です。

記録しない	一般に、ファイルシステムオブジェクトあたり2 kBのスペースを消費します。
ディレクトリレベルまでログに記録	**[記録しない]**の場合に保存されるデータに加え、バックアップディレクトリあたり30バイトのデータが保存されます。
ログファイル	**[ディレクトリレベルまでログに記録]**の場合に保存されるデータに加え、バックアップファイルあたり12バイトのデータが保存されます。
すべてログに記録	**[ファイルレベルまでログに記録]**の場合に保存されるデータに加え、バックアップファイルあたり18バイトのデータが保存されます。

カタログ保護がIDBに及ぼす影響

内部データベースの大部分のサイズは、カタログ保護の期間と選択したロギングレベルに比例します。カタログ保護期間中に実行するバックアップの回数が多いほど、IDBに蓄積されるデータが増えます。つまり、カタログ保護期間中にバックアップするファイル数に、各ファイルの必要データ量を乗算したデータが格納されることになります。

カタログ保護期限が過ぎても、情報はすぐにIDBからは削除されません。Data Protectorは一日に一度自動的に削除作業を実行します。IDB内の情報はメディア別に編成されているので、各メディアに関する情報はメディア上のすべてのオブジェクトのカタログ保護期限が切れない限り削除されません。削除時には、特定のDCバイナリファイルに占有されていたスペース全体が解放されます。

少なくとも最新のフルバックアップがカタログ保護に含まれるように設定することをお勧めします。たとえば、フルバックアップのカタログ保護を8週間に設定し、増分バックアップのカタログ保護を1週間に設定します。

IDBのサイズの見積もり

主にファイルシステムバックアップを実行する場合、状況によっては内部データベースがかなり大きいサイズ(数テラバイト)まで増加することがあります。ディスクイメージバックアップまたはオンラインデータベースバックアップを実行する場合には、IDBのサイズが数GBを超える可能性はほとんどありません。

DCディレクトリの保守

IDBでは、IDBの詳細カタログバイナリファイル(DCBF)部分を保存するディレクトリを複数登録できます。これにより、DCバイナリファイルを複数のディスクやボリュームに分散できます。デフォルトでは、

dcbf0～dcbf4という名前の5つのディレクトリが使用されます。

各DCBFディレクトリにはいくつかの構成パラメーターがあります。

- 割り当て順
- パス
- 最大サイズ
- 最大ファイル数
- 小容量

  構成パラメーターの詳細については、『HPE Data Protectorヘルプ』を参照してください。

新しいバイナリファイルを作成する必要がある場合、Data Protectorは次の"DCBF割り当て手順"を実行します。

1. 可能なすべてのDCディレクトリのリストから、Data Protectorは非アクティブ化されているものと存在しないものを除外します。DCディレクトリが存在しない場合は、IDBCorruptedイベントが生成されます。

   一杯になっているDCディレクトリは考慮されません。DCディレクトリが一杯になっていると見なされるのは、次の条件のうち少なくとも1つが満たされる場合です。

   ```
   Maximum size - Current size < Low space
   Free disk space < Low space
   Maximum files <= Current files
   ```

2. ユーザー選択可能なアルゴリズムのセット(グローバルオプションのDCDirAllocation)によって、実際のDCディレクトリが選択されます。

   - Fill in sequence

     Data Protectorは、構成されたシーケンスに基づき、最初の空きDCディレクトリに新しいDCバイナリファイルを作成します。

   - Balance size

     Data Protectorは、(合計サイズに基づく実効的な上限に比例して)DCBFデータ量が最も少ないDCディレクトリを選択します。次の値が最小になるように選択されます。

     ```
     (Maximum size - Current size - Low space) / (Maximum size - Low space)
     ```

   - Balance number

     Data Protectorは、(ファイル数に基づく実効的な上限に比例して)DCバイナリファイル数が最も少ないDCディレクトリを選択します。次の値が最小になるように選択されます。

     ```
     Current files / Maximum files
     ```

DCBF動作に影響するグローバルオプションとして、DCDirAllocationとMaxDCDirsを参照してください。

IDBのサイズをチェックする

内部データベース(IDB)の現在のサイズは、Data Protector GUIを使ってチェックできます。

また、[IDBサイズのレポート]および[IDBのスペース不足]の各通知を通じて、IDBのサイズに関する情報を取得することもできます(これらを事前に構成しておいた場合)。

手順

1. コンテキストリストで**[内部データベース]**をクリックします。
2. Scopingペインで、**[使用状況]**項目を展開します。[カタログデータベース]、[メディア管理データベース]、[詳細カタログバイナリファイル]、[セッションメッセージバイナリファイル]、[サーバーレス統合バイナリファイル]の各IDB項目が表示されます。

   項目「サーバーレス統合バイナリファイル」は、インストールされたHPE Data Protectorバージョンではサポートされなくなった機能に関連します。
3. IDBの各部分のプロパティとそれらのレコードを表示して、IDBのサイズをチェックします。
   - IDB項目のいずれか(**[カタログデータベース]**など)を右クリックし、**[プロパティ]**をクリックして、IDBの該当部分の[ディスクの使用状況]を表示します。[ディスクの使用状況]には、IDBの該当部分が現在占有しているディスクスペースの量が表示されます。**[レコード統計]**タブをクリックすると、該当部分に含まれているすべてのレコードの統計情報が表示されます。
   - DCディレクトリのディスクの使用状況をチェックするには、**[詳細カタログバイナリファイル]**を展開し、DCディレクトリをダブルクリックして、**[ディスクの使用状況]**タブをクリックします。

IDBのサイズ増加率を減らす

内部データベース(IDB)のサイズ増加率を抑えるには、バックアップ仕様、オブジェクトコピー仕様、オブジェクト集約仕様のロギングレベルおよびカタログ保護の設定値を抑制するようにします。これらを下げると、今後のサイズ増加が抑えられますが、IDBの現在のサイズは変更されません。

ロギングレベルを下げると、復元時のブラウズが制限されます。

カタログ保護期間を短縮すると、バックアップの復元時にブラウズ機能を利用できなくなることがあります。カタログ保護期間を超過したバックアップはブラウズできません。

以下の手順は、バックアップ仕様内のこれらの設定を変更する方法を示しています。

ロギングレベルを下げる

バックアップ仕様のロギングレベル設定を下げることにより、IDBに保存されるデータ(ファイル/ディレクトリ)の量を削減します。ロギングレベルは、高い順に、**[すべてログに記録]** → **[ファイルレベルまでログに記録]** → **[ディレクトリレベルまでログに記録]** → **[記録しない]**となります。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. ロギングレベルを変更するバックアップ仕様をダブルクリックして、**[オプション]**タブをクリックします。
4. [オプション]プロパティページの**[ファイルシステムオプション]**で、適切な**[拡張]**ボタンをクリックします。
5. **[その他]**タブをクリックし、**[ロギング]**でロギングレベルを変更します。
6. **[OK]**をクリックして変更内容を適用します。

カタログ保護期間を短縮する

カタログ保護期間を短縮すると、IDB内の情報(復元時のブラウズ用情報)に対してのみ保護期間が短縮されます。メディア上の情報は影響されません。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. カタログ保護を変更するバックアップ仕様をダブルクリックして、**[オプション]**タブをクリックします。
4. [オプション]プロパティページの**[ファイルシステムオプション]**で、適切な**[拡張]**ボタンをクリックします。
5. **[オプション]**タブをクリックし、**[カタログ保護]**で、カタログ保護を変更します。
6. **[OK]**をクリックして変更内容を適用します。

IDBの現在のサイズを縮小する

内部データベース(IDB)の現在のサイズを縮小するには、カタログ保護設定を変更します。この場合、完全バックアップ、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(セッション内のすべてのオブジェクト)を対象とすることも、特定のオブジェクトのみを対象とすることもできます。

カタログ保護期間を短縮すると、バックアップの復元時にブラウズ機能を利用できなくなることがあります。カタログ保護期間を超過したバックアップはブラウズできません。

この操作は、IDBの今後のサイズ増加には影響しません。

変更内容は、以下のタイミングで適用されます。

- メディア上のすべてのオブジェクトからカタログ保護が削除されたとき。
- 古くなったデータが1日1回(デフォルトでは正午)Data Protectorにより自動的にIDBから削除されるとき。時刻は、グローバルオプションの`DailyMaintenanceTime` を使って指定できます。時刻は24時間制で指定してください。

  `omnidbutil -purge -dcbf`コマンドを実行すると、削除を即時に開始することができます。他の古い項目をIDBから削除する方法については、`omnidbutil` manページまたは『*HPE Data Protector Command Line Interface Reference*』を参照してください。

カタログ保護を変更すると、IDB内の復元時のブラウズ情報に対してのみ保護が変更されます。メディア上の情報は影響されません。そのため、メディアをエクスポートしてから再度インポートする場合、Data Protectorでは、そのメディアからカタログ保護に関する情報が再度読み込まれます。

セッションのカタログ保護を変更する

バックアップセッションの保護を変更すると、そのセッションでバックアップしたすべてのオブジェクトに対して保護が変更されます。

手順

1. コンテキストリストで**[内部データベース]**をクリックします。
2. Scopingペインで、**[セッション]**項目を展開します。
3. 保護を変更するセッションを右クリックし、**[カタログ保護の変更]**をクリックします。
4. セッションに適用する新しいカタログ保護を指定し、**[完了]**をクリックして変更内容を適用します。

オブジェクトのカタログ保護を変更する

特定のオブジェクトの保護を変更すると、そのオブジェクトのバックアップ時のセッションからは独立して、そのオブジェクトの保護が変更されます。

手順

1. コンテキストリストで**[内部データベース]**をクリックします。
2. Scopingペインで、**[オブジェクト]**項目を展開します。
3. 保護を変更するオブジェクトを右クリックし、**[カタログ保護の変更]**をクリックします。
4. オブジェクトに適用する新しいカタログ保護を指定し、**[完了]**をクリックして変更内容を適用します。

IDBサイズを拡張する

IDBの詳細部分(バックアップ対象オブジェクトの名前、バージョン、およびメタデータ)に対する空きディスク容量の不足により、内部データベースの拡張が必要となる場合があります。拡張するには、新しいDCディレクトリを作成するか、既存のDCディレクトリをより大きな容量に再構成します。

DCディレクトリをより大きな容量に再構成する

[割り当て順]、[最大サイズ]、[最大ファイル数]、または[小容量]オプションを変更することにより、既存のDCディレクトリを再構成できます。選択されたDCディレクトリ内のファイルの個数と現在の合計サイズにより、調整範囲は限定される場合があります。

手順

1. コンテキストリストで**[内部データベース]**をクリックします。
2. Scopingペインで、**[使用状況]**と**[詳細カタログバイナリファイル]**を順に展開します。
3. 選択されたDCディレクトリのパスを右クリックし、**[プロパティ]**をクリックします。
4. [結果エリア]で利用可能なオプションを適切に変更します。
5. **[完了]**をクリックして変更を適用します。

IDBの整合性チェック

内部データベース(IDB)の内容は、論理的に正確でなければなりません。つまり、IDBの各部の整合がとれており、正しい順序になっている必要があります。IDB全体に対しても、またIDBの特定の部分に対しても、整合性チェックを手動で実行できます。

Data Protectorのデフォルト動作では、IDBのバックアップ前にIDBの整合性が自動的にチェックされます(クイックチェック)。これは、障害発生時にCell ManagerでIDBとバックアップデータを復旧する上で非常に重要です。

IDBチェックのタイプ	チェック対象	コマンド
IDBのクイックチェック	コア部分(MMDBおよびCDB)とファイル名のチェック、およびDCBF部分の簡易チェック。	`omnidbcheck -quick`
DCBF部分の簡易チェック	DCバイナリファイルの有無とそのサイズ。	`omnidbcheck -bf`
DCBF部分の完全チェック	メディア位置およびDCバイナリファイルの整合性。	`omnidbcheck -dc`
SMBF部分のチェック	セッションメッセージバイナリファイルの有無。	`omnidbcheck -smbf`
メディアの整合性チェック	メディアの整合性。メディアの整合性に問題がある場合には、不整合なメディアの名前の一覧も表示します。	`omnidbcheck -media_consistency`
スキーマの整合性チェック	スキーマの整合性。Data Protectorインストール中にスキーマが初めて作成されて以降に行われたスキーマのすべての変更も検出します。	`omnidbcheck -schema_consistency`
データベースの整合性チェック	データベースの整合性。データベースの整合性に問題がある場合には、エラーの一覧も表示します。	`omnidbcheck -database_consistency`
IDBの拡張	SMBFを除くすべてのチェックが実行されます。	`omnidbcheck -extended`

他のCell ManagerにIDBを移動する

内部データベース(IDB)は、同じオペレーティングシステムで実行されている別のCell Managerに移動できます。

最初のシナリオでは、以下の手順に従って、Data Protectorクライアントのバックアップデバイスから IDBの復元を実行します。

手順

1. Data Protectorクライアントの*client.company.com* で、バックアップデバイス*PreparedDevice*を準備します。
2. バックアップデバイス*PreparedDevice* を使用して、IDBバックアップを実行します。
3. ホスト*cmb.company.com* 上に、新しいData Protector Cell Managerを準備します(クリーンインストール)。
4. ホスト*cma.company.com* のCell Managerからクライアント*client.company.com* をエクスポートします。
5. ホスト*cmb.company.com* の新しいCell Managerにクライアント*client.company.com* をインポートします。
6. 新しいCell Managerにバックアップデバイス*PreparedDevice* をインポートします。
7. バックアップデバイス*PreparedDevice* から、IDB復元を実行します。
8. HPE Data Protectorサービスを停止します。
9. `standalone.xml`構成ファイルに格納されているすべてのパスワード(`keystore-password`、`truststore-password`、`ssl password`、`ca-certificate-password`)について、`webservice.properties`構成ファイルの`KeystorePassword`を使用します。

   これらの構成ファイルは以下の場所から利用できます。

   Windowsの場合:

   - `ProgramData\OmniBack\Config\client\components\webservice.properties`
   - `ProgramData\OmniBack\Config\server\AppServer\standalone.xml`

   UNIXの場合 :

   - `/etc/opt/omni/client/components/webservice.properties`
   - `/etc/opt/omni/server/AppServer/standalone.xml`
10. HPE Data Protectorサービスを開始します。
11. 元のCell Managerから新しいCell Managerにクライアントをインポートします。

    > **重要:**
    > 各クライアントは、元のCell Managerから事前にエクスポートしておく必要があります。

12. 新しいCell ManagerにGUIを再接続します。

2番目のシナリオでは、以下の手順に従って、元のCell Managerのバックアップデバイスから**IDB**の復元を実行します。

手順

1. 元のCell Managerのバックアップデバイス*PreparedDevice* を準備します。
2. バックアップデバイス*PreparedDevice* を使用して、IDBバックアップを実行します。
3. ホスト*cmb.company.com* 上に、新しいData Protector Cell Managerを準備します(クリーンインストール)。

4. 元のCell Managerから*バックアップデバイスPreparedDevice*をエクスポートします。
5. ホスト*cmb.company.com*の新しいCell Managerに*バックアップデバイスPreparedDevice*をインポートします。
6. *バックアップデバイス*PreparedDeviceから、I*DB復元を実行します。*
7. HPE Data Protectorサービスを停止します。
8. `standalone.xml`構成ファイルに格納されているすべてのパスワード(`keystore-password`、`truststore-password`、`ssl password`、`ca-certificate-password`)について、`webservice.properties`構成ファイルの`KeystorePassword`を使用します。

   これらの構成ファイルは以下の場所から利用できます。

   Windowsの場合:

   - `ProgramData\OmniBack\Config\client\components\webservice.properties`
   - `ProgramData\OmniBack\Config\server\AppServer\standalone.xml`

   UNIXの場合 :

   - `/etc/opt/omni/client/components/webservice.properties`
   - `/etc/opt/omni/server/AppServer/standalone.xml`
9. HPE Data Protectorサービスを開始します。
10. 元のCell Managerから新しいCell Managerにクライアントをインポートします。

    > **重要:**
    > 各クライアントは、元のCell Managerから事前にエクスポートしておく必要があります。

11. 新しいCell ManagerにGUIを再接続します。

Data Protectorのグローバルオプションをカスタマイズする

Data Protectorグローバルオプションファイルでは、グローバルオプションの値を変更したり、新しいオプションを追加できます。

前提条件

- ユーザーアカウントはData Protector `Admin`ユーザーグループに所属する必要があります。

GUI使用によるグローバルオプション設定

手順

GUIを使用してグローバルオプションを設定するには、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**[内部データベース]**をクリックします。
2. Scopingペインで**[内部データベース]**の**[グローバルオプション]**をクリックします。

[結果エリア]に**Data Protectorグローバルオプション**テーブルが表示されます。このテーブルには、次の6つの列があります。

- [グループ] - オプションが属するコンテキストセクションを表します。
- [使用中] - オプションのステータスを示します。オンになっているオプションはアクティブです。チェックボックスが空白の場合は、グローバルオプションファイルでコメントアウトされている非アクティブなオプションです。
- 名前
- [元] - オプションのロード元のファイルを示します。
- [値] - オプションに現在設定されている値を示します。
- [説明] - オプションの使用方法が示されます。

3. オプションを変更するには、[結果エリア]の[値]列で、変更する値をクリックし、[編集]アイコンをクリックして新しい値を入力します。**[保存]**をクリックして変更内容を適用します。

   オプションを追加するには、[追加]アイコンをクリックし、ダイアログボックスにオプションパラメーターを入力して**[追加]**をクリックします。

4. [結果エリア]の一番上にある[保存]アイコンをクリックします。

保存する前に複数の行を変更することもできます。

テーブルの表示を変更するには、テーブル見出しのフィルターを使用します。

保存プロセスでエラーが発生した場合は、元のグローバルオプションファイルのコピーが`global.old`という名前で、グローバルオプションフォルダーに作成されます。

グローバルファイルの編集によるオプションのカスタマイズ

GUIの使用以外にも、テキストエディターで`global`ファイルを編集して、Data Protectorグローバルオプションを設定することができます。

> **注意:**
> HPEでは、GUIを使用してグローバルオプションを設定することを推奨します。保存時に変更内容が検証されるため、範囲外または無効な設定、誤った削除、タイポまたはスペルミスが原因の問題が発生する可能性を減らせるためです。

手順

1. テキストエディターを開きます
2. テキストエディターで、デフォルトのData Protectorサーバー構成ディレクトリの`options`サブディレクトリにある`global`ファイルを開きます。
3. オプションをアクティブにするには、名前の前の#記号を削除して、目的の値に設定します。
4. ファイルをUnicode形式で保存します。

IDBレポートの構成

内部データベース(IDB)のレポートを構成すると、IDBサイズの拡張やIDBのサイズ増加の軽減など、IDBに対する保守タスクの実施が必要になったときに通知されるようになります。

IDBレポート

レポート	どのような場合に通知されるか
IDBサイズのレポート	... IDBの各部分のサイズに関する情報

IDB通知の構成

内部データベース(IDB)の通知を構成すると、IDBのサイズの拡張、IDBの整合性チェックなど、IDBに対する保守タスクの実施が必要になったときに通知されるようになります。

IDB通知

通知	どのような場合に通知されるか
IDBのスペース不足	... IDBのスペースが不足している場合
IDBの制限	... MMDBまたはCDB部分が上限に達した場合
IDBのバックアップ必要	... IDBバックアップが頻繁に行われない場合、または次の増分IDBバックアップが多すぎる場合

IDBを復元する

内部データベース(IDB)は、標準IDBバックアップ手順で作成したバックアップイメージから復元できます。この復元手順は、IDBが破損していると使用できません。IDBが破損している場合は、IDB回復方法のいずれかを実行する必要があります。

内部データベースを復元するには、以下の手順を実行します。

- IDBを復元する

暗号化されたIDBバックアップから復元する場合、実際の復元の前に次の追加の手順が必要です。

- 暗号化されたバックアップからのIDB復元の準備

IDBを復元する

内部データベースのオンライン復元中には、IDBの基本部分(CDB、MMDB、SMBF)は元の場所とは異なる場所にのみ復元できます。その一方で、Cell Manager構成データとIDBの詳細カタログバイナリファイル(DCBF)部分は、元の場所にも異なる場所にも復元できます。

前提条件

- 内部データベースのバックアップイメージのサイズに応じて、Cell Managerに十分なディスクの空き容量があることを確認します。

制限事項

[復元したデータベースを新しい内部データベースとして使用する]オプションを介して、復元したIDBを新しいIDBとして使用することは、SGクラスターセットアップではサポートされていません。omnirc変数OB2SGENABLEDを設定できます。この変数は、セッションレポートで、復元したIDBを新しいIDBとして使用する手順を提供します。omnirc変数を設定すると、セッションレポートに以下のメッセージが表示されます。

```
[Warning] From: OB2BAR_POSTGRES_BAR@<host name> "DPIDB"  Time: <date time>

[175:316]Automatic replacement of the Internal Database on cluster environment not
supported.
```

メッセージ内のエラー番号をクリックし、復元したIDBを新しいIDBとして使用する場合に従う必要がある手順の詳細を確認します。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインで、**[復元オブジェクト]**項目、**[内部データベース]**項目を順に展開します。
3. IDBのバックアップ元で[Cell Manager]を展開し、**[内部データベース]**をクリックします。
4. 内部データベースの基本部分を復元するため、[内部データベース]プロパティページの**[内部データベースの復元]**オプションを選択したままにします。IDBの基本部分は、カタログデータベース(CDB)、メディア管理データベース(MMDB)、およびセッションメッセージバイナリファイル(SMBF)です。復元中に使用する内部データベースサービス用一時ポートと、IDB基本部分の復元先となる場所を指定します。

   さらに、アーカイブログファイルを使用して内部データベース回復を実行するかどうか、および復元されたIDBをセルの新しい内部データベースとして使用すべきかどうかを決定します。
5. IDBのDCBF部分を復元するには、**[カタログバイナリファイルの復元]**を選択し、その復元場所(元の場所かカスタムの場所か)を選択します。
6. Data Protectorが、最新のIDBバックアップイメージが作成されたのとは異なる特定の時点にIDBを復元すべきかどうかを指定します。この場合、内部データベースの基本部分は、指定された時刻以前の最新のバックアップ状態に復元されます。
7. **[構成ファイル]**プロパティページで、Cell Manager構成データの復元に関する選択を行います。構成データを復元対象として選択する場合、構成データのバックアップオブジェクトバージョンと復元場所も指定し、Data Protectorが元の場所に存在する構成ファイルをどのように処理するのかを決定する必要があります。
8. **[オプション]**プロパティページで、復元セッションで使用する、実行前および実行後コマンドを指定します(省略可能)。
9. **[デバイス]**プロパティページで、セッションで使用するデバイスを選択します。

10. **[メディア]**プロパティページで、IDBの復元に使用されるバックアップメディアを確認します。セッション中、Data Protectorが参照するバックアップメディアの優先順位を調節します(省略可能)。
11. [アクション]メニューの**[復元の開始]**、または[結果エリア]の**[復元]**を選択します。
12. **[完了]**をクリックします。

> **重要:**
> ポイントインタイムIDB復元セッション後、auditing_*IDBRestoreSessionID_NNNNNNNNNN*ディレクトリから元のauditingディレクトリに特定ファイルをコピーします。これにより、監査情報が復元されたIDBの状態と整合するようになります。以下の監査ログをコピーする必要があります。
>
> *YYYY_MM_DD*.med
>
> *YYYY_MM_DD*.obj
>
> *YYYY_MM_DD*.ses
>
> 上記のファイル名の*YYYY*、*MM*、および*DD*文字列は、[内部データベース]プロパティページの**[復元の期限]**オプションで指定した日付に対応します。

> **注:**
> 復元後、IDBの整合性をチェックできます。

暗号化されたバックアップからのIDB復元の準備

暗号化されたIDBバックアップ時、暗号化キーは、IDB-*ClientName*-keys.csvファイルに自動的にエクスポートされます。このファイルは、暗号化キーがエクスポートされるデフォルトのData Protectorディレクトリにあります。

IDBを復元する前に、次の手順に従います。

手順

1. IDB復元を実行するCell ManagerにIDB-ClientName-keys.csvファイルを転送します。
2. 次のコマンドを実行してキーをインポートします。

   ```
   omnikeytool -import CSVFile
   ```

Cell Managerは、オンラインKMSからこのキーを使用して、IDBバックアップが含まれるメディアでデータを復号化します。

IDBの回復について

一部またはすべてのIDBファイルが利用不能になった場合や破損した場合は、内部データベース(IDB)の回復が必要になります。

IDBに関する問題には、3つのレベルがあり、それぞれ対処の方法が異なります。

- ファイルシステムがマウントされていないことやネームサービスの障害など、オペレーティングシステムの構成に原因があってIDBに発生した問題に対しては、トラブルシューティングを行います。
- IDBのうち、コア以外の部分(バイナリファイル)に問題がある場合は、それらを除外または削除します。このように処置できるのは、IDBの破損レベルが[警戒域]と特定された場合(つまり、IDBのコア部分が

破損していない場合)だけです。

- 前回のIDBバックアップ以降の変更内容のIDB復元とIDB更新からなる完全回復を実行します。IDBの破損レベルが[危険域]と特定された場合(コア部分が破損している場合)には、この処置が必須です。

完全回復(前回のIDBバックアップ以降の変更内容の復元と更新)

完全回復は、以下の2段階からなります。

1. IDBを復元して、IDBを最後の(利用可能な)整合状態に戻します。
2. IDBを最後の整合状態からIDBがまだ稼動していた最後の瞬間の状態まで更新します。

復元の手順は、問題が発生する前にIDB回復にどの程度まで備えていたか(IDB復旧ファイル、IDBバックアップイメージ、元のバックアップデバイス、およびアーカイブログファイルが利用可能かどうか)によって異なります。これがすべて利用可能であれば、ガイド式自動回復機能を使ってIDBを簡単に回復できます。

IDB回復方法の概要

内部データベース(IDB)を回復するには、何通りかの方法があります。破損のレベルや必要条件によって、また、IDB復旧ファイル、元のバックアップデバイス、アーカイブログファイルが利用可能かどうかによって、回復の手順は異なります。

最も効率的な完全回復

この回復方法では、画面に表示される指示に従って、アーカイブログファイルを再生しながらIDBの復元処理を進めることができます。アーカイブログファイルが利用できない場合でも、前回のIDBバックアップ以降のメディアをすべてインポートすると、IDBを更新できます。

破損レベル	問題の種類	現在の状況	回復手順
危険域	IDBが完全に失われたか、またはコア部分が破損している。	IDB復旧ファイルおよびIDBバックアップ作成時の元のデバイスが利用できない。	可能であれば、ガイド式自動回復(IDBの復元とアーカイブログファイルの再生)を実行します。これを実行できない場合は、「その他の回復方法」に示す方法のいずれかを使用してください。

IDBの破損部分の除外(削除)

破損レベルが[警戒域]の場合(コア部分が破損していない場合)は、IDBを完全に回復する代わりに、IDBのうち、紛失または破損した部分を除外(削除)することもできます。

破損レベル	問題の種類	回復手順

警戒域	DCバイナリファイルが紛失または破損している。	IDBのDCBF部分の[警戒域]レベルの破損に対処する

その他の回復方法

ここでは、特定の状況下での回復手順を示します。IDBを完全に回復したいが、何らかの理由でガイド式自動回復機能を実行できない場合には、これらの手順で対処できます。復旧では、IDBの復元と更新を行います。

復元

現在の状況	備考	回復手順(IDBの復元)
IDB復旧ファイルは利用できるが、IDBのバックアップに使用した元のデバイスが変更されている。	この方法は、基本的にガイド式自動回復と同じですが、ガイド内容が少なく手順が複雑になっており時間もかかります。	IDB復旧ファイルと新しいデバイスを使ってIDBを復元する
IDB復旧ファイルが利用できない。	この方法は、基本的にガイド式自動回復と同じですが、ガイド内容が少なく手順が複雑になっており時間もかかります。	IDB復旧ファイルを使わずにIDBを復元する
特定のIDBバックアップ(最新ではないバックアップ)からIDBを回復したい。	この方法では、IDBが最新の状態に復元されません。	特定のIDBセッションからIDBを復元する

IDBを更新する(前回のIDBバックアップ以降の変更内容を反映させる)

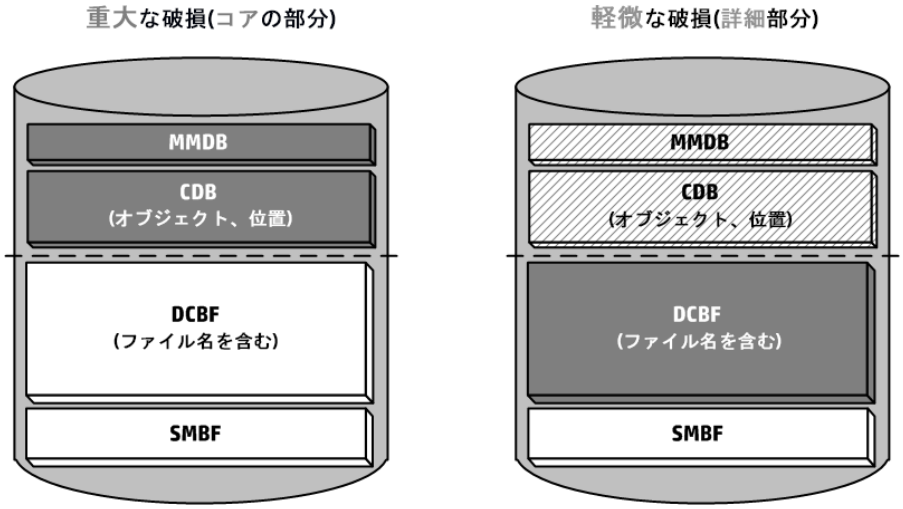
現在の状況	回復手順(IDBの更新)
アーカイブログファイルが利用可能ではない。	メディアをインポートしてIDBを更新する

IDB破損レベル

内部データベースの破損レベルは、[危険域]と[警戒域]の2つです。このレベルは破損がIDBのどこで発生したかによって決まります。

IDB整合性チェックを実行すると、IDBのどの部分が破損しているかを確認できます。

IDBの回復手順は、破損レベルによって異なります。



IDBの破損レベルを特定する

内部データベース(IDB)を適切な方法で回復するには、破損レベルを特定する必要があります。

手順

1. `omnidbcheck -extended`コマンドを使って、破損レベルを特定します。

   > **注:**
   > 上記のコマンドで拡張チェックを行うとかなりの時間がかかることがありますが、`omnidbcheck`コマンドの一部を実行することもできます。たとえば、`omnidbcheck -connection`コマンドを実行すると、IDBとの接続が機能しているかどうかを特定できます。

破損のレベルと特定したら、適切な方法で回復を実行します。

ガイド式自動回復(IDBの復元とアーカイブログファイルの再生)を実行する

ガイド式自動回復は、内部データベース(IDB)を最も効率的に回復する方法です。IDBバックアップメディアの他に、IDBバックアップに使用したIDB復旧ファイルとオリジナルのデバイスが揃っていれば、ガイド式自動回復を実行できます。

この方法により、前回のIDBバックアップ以降のアーカイブログファイルを再生しながら復元処理を進めることができます。アーカイブログファイルが利用できない場合でも、メディアをインポートすると前回のIDBバックアップ以降からIDBを更新できます。

トランザクションでは、IDBのコア部分の更新が再生されます。ただし、バイナリファイルは更新されないので、バイナリファイルの変更内容は失われます。前回のIDBバックアップからIDB破損までの間に実行されたバックアップについては、以下の項目が利用できなくなります。

- セッションメッセージ。
- ファイルバージョンのブラウズ(オブジェクト全体の復元は可能です)。バックアップに使用したメディアに対

してカタログのインポートを実行すると、変更内容を回復できます。

前提条件

- 内部データベースのバックアップイメージのサイズに応じて、Cell Managerに十分なディスクの空き容量があることを確認します。
- 『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』のCell Managerのインストール要件に記載されている通り、Data Protector Cell Managerに合計RAMの2倍の容量があることを確認します。Cell ManagerがUNIXシステムの場合、カーネルパラメーター`shmmax`に、同じセクションに記載されている必要な値の2倍の値を設定するようにしてください。
- IDBのバックアップ時と同じディレクトリ(Windowsでは、同じドライブ文字を指定すること)で、障害発生前と同じサイズのディスクをマウントします。これが確かでない場合は、IDBを別のディスク/ボリュームレイアウトに復元する手順に従ってください。`omniofflr`コマンドの`-preview`オプションを使うと、ファイルの復元先を事前に確認できます。
- Data ProtectorをCell Manager上にインストールし、その後、デバイス(なるべくIDBバックアップに使用したデバイス)が接続されているシステムにインストールします。
- IDBがHPE Serviceguard上にインストールされている場合、ガイド式自動回復を実行する前に、アクティブノード上で以下のコマンドを実行する必要があります。
  1. `cmhaltpkg` *`PackageName`*(ここで、*`PackageName`*はData Protectorクラスターパッケージの名前)。このコマンドにより、Data Protectorパッケージが停止され、Data Protector共有ボリュームグループがアンマウントされます。
  2. `vgchange -a e /dev/`*`vg_name`*(ここで、*`vg_name`*はData Protector共有ボリュームグループの名前)。このコマンドにより、Data Protector共有ボリュームグループがアクティブ化されます。システム上のボリュームグループのリストを表示するには、`ll /dev/*/group`を実行します。
  3. `mount /dev/`*`vg_name`*`/`*`lv_name`*`/`*`MountPoint`*(ここで、*`MountPoint`*はData Protector共有ボリュームグループのマウントポイントの名前)。このコマンドにより、Data Protector共有ボリュームグループがマウントされます。

  ガイド式自動回復が完了したら、アクティブノード上で`cmrunpkg` *`PackageName`*コマンドを実行して、Data Protectorパッケージを開始します。
- IDBがSymantec Veritas Cluster Server上にインストールされている場合、ガイド式自動回復を実行する前に、アクティブノード上でData Protectorアプリケーションリソースをオフラインで取り込みます。

  ガイド式自動回復が完了したら、アクティブノード上でData Protectorアプリケーションリソースをオンラインにして、Data Protectorサービスを開始します。
- IDBがMicrosoft Cluster Server上にインストールされている場合は、ガイド式自動回復を実行する前に、アクティブノード上でクラスターアドミニストレーターユーティリティを使って、`OOBVS_HPDP_AS`, `OBVS_HPDP_IDB`, および`OBVS_HPDP_IDB_CP`クラスターグループをオフラインにし、`Inet`サービスを停止します。ガイド式自動回復が完了したら、クラスターアドミニストレーターユーティリティを使って`OBVS_HPDP_AS`, `OBVS_HPDP_IDB`, `OBVS_HPDP_IDB_CP`,および`OBVS_MCRS`クラスターグループをオンラインにし、`Inet`サービスを再起動します。

手順

1. `omniofflr -idb -autorecover`コマンドを実行します。

このコマンドでは、IDB復旧ファイルが読み取られます。このファイルにIDBバックアップが記録されていれば、サービスが停止され、IDBが元の位置に復元されます。すべてのオプションは、IDB復旧ファイルのデータに従って自動的に設定されます。

復元が完了すると、omniofflrコマンドによって再生可能なアーカイブログファイルの有無がチェックされます。ログファイルが存在していれば、それらのログを再生するかどうかを確認するメッセージが表示されます。この手順を取り消した場合およびアーカイブログファイルが存在しない場合は、前回のIDBバックアップ以降の更新内容をIDBに適用する方法を示すメッセージが表示されます。この場合は、以下の操作を手動で実行する必要があります。

- メディアをインポートする。
- アーカイブログファイルを検索して、後で再生する。

ログファイルを再生するか、またはメディアをインポートしてIDBを更新し終えると、IDBが完全に回復されるはずです。

IDBのDCBF部分の[警戒域]レベルの破損に対処する

内部データベース(IDB)に重大度が[警戒域]の破損が検出された場合は、一部のDCバイナリファイルが紛失または破損していることを意味します。IDBを完全に回復する必要はありません。バイナリファイルは、メディアからカタログをインポートすることで簡単に再作成できます。破損の種類に応じた回復手順を選択してください。

DCバイナリファイル喪失時の回復

DCバイナリファイルは、メディアごとに1つずつ作成されます。一部のDCバイナリファイルが紛失している場合は、一部のメディアのメディア位置が存在しないファイルを参照しています。この場合、対応するファイルシステムをブラウズすると、エラーメッセージが表示されます。

手順

1. omnidbcheck -bfコマンドの出力から、紛失しているバイナリファイルのメディアIDを特定します。また、omnimm -media_info *medium-id*コマンドを実行すると、その他のメディア属性(メディアラベルやメディアプールなど)を確認できます。
2. メディア位置(mpos)とバイナリファイルの間の整合性を確保するには、omnidbutil -fixmposコマンドを実行します。
3. メディアからカタログをインポートしてバイナリファイルを再作成します。

DCバイナリファイル破損時の回復

一部のDCバイナリファイルが破損している場合は、DCバイナリファイルをいったん削除してから、適切なロギングレベルのメディアをインポートして再作成することで対処できます。ファイルを削除すると、一部のメディア位置が存在しないバイナリファイルを参照することになるため、対応するファイルシステムのブラウズ時にエラーメッセージが表示されますが、それ以外の影響はありません。

手順

1. omnidbcheck -dcコマンドの出力から、破損したDCバイナリファイルのメディアIDを特定します。また、omnimm -media_info *medium-id*コマンドを実行すると、その他のメディア属性(メディアラベルやメディアプールなど)を確認できます。
2. 破損したメディアに対応するDCバイナリファイル特定します。DCバイナリファイル名は、*MediumID_TimeStamp*.datとなります(MediumIDに含まれるコロン":"は、アンダースコア"_"に置換されます)。
3. 破損したDCバイナリファイルを削除します。
4. メディア位置(mpos)とバイナリファイルの間の整合性を確保するには、omnidbutil -fixmposコマンドを実行します。
5. メディアからカタログをインポートしてバイナリファイルを再作成します。

IDB復旧ファイルと新しいデバイスを使ってIDBを復元する

ここでは、IDB復旧ファイルが利用可能で、しかしIDBバックアップに使用されたオリジナルのデバイスが回復に使用するデバイスと異なるか、またはメディアが別のスロットに格納されている場合に、この手順で内部データベース(IDB)を復元できます。

前提条件

- IDBのバックアップ時と同じディレクトリ(Windowsでは、同じドライブ文字を指定すること)で、障害発生前と同じサイズのディスクをマウントします。これが確かでない場合は、IDBを別のディスク/ボリュームレイアウトに復元する手順に従ってください。omniofflrコマンドの-previewオプションを使うと、ファイルの復元先を事前に確認できます。
- 可能であれば、既存のmedia.logファイルを安全な場所に移動しておきます。このファイルには、前回のIDBバックアップ以降に使用されたメディアに関する情報が含まれています。アーカイブログファイルが利用できない場合は、このファイルがIDBの更新に非常に役立ちます。
- Data ProtectorをCell Manager上にインストールし、その後、デバイス(なるべくIDBバックアップに使用したデバイス)が接続されているシステムにインストールします。
- IDBがHPE Serviceguard上にインストールされている場合、ガイド式自動回復を実行する前に、アクティブノード上で以下のコマンドを実行する必要があります。
  1. cmhaltpkg *PackageName*(ここで、*PackageName*はData Protectorクラスターパッケージの名前)。このコマンドにより、Data Protectorパッケージが停止され、Data Protector共有ボリュームグループがアンマウントされます。
  2. vgchange -a e /dev/*vg_name*(ここで、*vg_name*はData Protector共有ボリュームグループの名前)。このコマンドにより、Data Protector共有ボリュームグループがアクティブ化されます。システム上のボリュームグループのリストを表示するには、ll /dev/*/groupを実行します。
  3. mount /dev/*vg_name*/*lv_name*/*MountPoint*(ここで、*MountPoint*はData Protector共有ボリュームグループのマウントポイントの名前)。このコマンドにより、Data Protector共有ボリュームグループがマウントされます。

  ガイド式自動回復が完了したら、アクティブノード上でcmrunpkg *PackageName*コマンドを実行して、Data Protectorパッケージを開始します。
- IDBがSymantec Veritas Cluster Server上にインストールされている場合、ガイド式自動回復を実行

する前に、アクティブノード上でData Protectorアプリケーションリソースをオフラインで取り込みます。

ガイド式自動回復が完了したら、アクティブノード上でData Protectorアプリケーションリソースをオンラインにして、Data Protectorサービスを開始します。

- IDBがMicrosoft Cluster Server上にインストールされている場合は、ガイド式自動回復を実行する前に、アクティブノード上でクラスターアドミニストレーターユーティリティを使って、OBVS_HPDP_AS, OBVS_HPDP_IDB, およびOBVS_HPDP_IDB_CPクラスターグループをオフラインにし、Inetサービスを停止します。ガイド式自動回復が完了したら、クラスターアドミニストレーターユーティリティを使ってOBVS_HPDP_AS, OBVS_HPDP_IDB, OBVS_HPDP_IDB_CP,およびOBVS_MCRSクラスターグループをオンラインにし、Inetサービスを再起動します。

手順

1. 次のコマンドを実行して、復元ジョブオプションを設定するとともにテキストファイルを作成します。

   ```
   omniofflr -idb -autorecover -save C:\TEMP\restjob.txt -skiprestore -logview
   ```

   -logviewオプションを指定しているので、セッションIDの隣に最初のアーカイブログファイルのリストが表示されます。復元対象のセッションの最初のアーカイブログファイルは復元後にIDBを更新するときに必要になるので、この情報を忘れずにメモしておいてください。たとえば、出力内容が2013/02/09-2 AAAAAAHであれば、■を復元するために必要な最初のアーカイブログファイルはAAAAAAHです。2013/02/09-2 session.

   作成したrestjob.txtファイルには、オリジナルのデバイスに関する情報と、IDBバックアップ時にメディアが格納されていたスロットに関する情報が含まれています。
2. restjob.txtファイルを編集して、現在のデバイスを指定するか、またはメディアが現在格納されているスロットを指定します。
3. omniofflr -idb -read C:\TEMP\restjob.txtコマンドで復元を実行します。

このコマンドの実行後、画面に表示される指示に従うと、前回のIDBバックアップ以降のアーカイブログファイルを再生しながら復元処理を進めることができます。アーカイブログファイルが利用できない場合でも、前回のIDBバックアップ以降に使用されたメディアをすべてインポートすると、IDBを更新できます。

IDB復旧ファイルを使わずにIDBを復元する

ここでは、IDB復旧ファイルが使用できない場合に内部データベース(IDB)を復元する手順を示します。

前提条件

- IDBのバックアップ時と同じディレクトリ(Windowsでは、同じドライブ文字を指定すること)で、障害発生前と同じサイズのディスクをマウントします。これが確かでない場合は、IDBを別のディスク/ボリュームレイアウトに復元する手順に従ってください。omniofflrコマンドの-previewオプションを使うと、ファイルの復元先を事前に確認できます。
- 可能であれば、既存のmedia.logファイルを安全な場所に移動しておきます。このファイルには、前回のIDBバックアップ以降に使用されたメディアに関する情報が含まれています。アーカイブログファイルが利用できない場合は、このファイルがIDBの更新に非常に役立ちます。
- Data ProtectorをCell Manager上にインストールし、その後、デバイス(なるべくIDBバックアップに使用したデバイス)が接続されているシステムにインストールします。

- IDBがHPE Serviceguard上にインストールされている場合、ガイド式自動回復を実行する前に、アクティブノード上で以下のコマンドを実行する必要があります。
  1. `cmhaltpkg PackageName`(ここで、*PackageName*はData Protectorクラスターパッケージの名前)。このコマンドにより、Data Protectorパッケージが停止され、Data Protector共有ボリュームグループがアンマウントされます。
  2. `vgchange -a e /dev/vg_name`(ここで、*vg_name*はData Protector共有ボリュームグループの名前)。このコマンドにより、Data Protector共有ボリュームグループがアクティブ化されます。システム上のボリュームグループのリストを表示するには、`ll /dev/*/group`を実行します。
  3. `mount /dev/vg_name/lv_name/MountPoint`(ここで、*MountPoint*はData Protector共有ボリュームグループのマウントポイントの名前)。このコマンドにより、Data Protector共有ボリュームグループがマウントされます。

  ガイド式自動回復が完了したら、アクティブノード上で`cmrunpkg PackageName`コマンドを実行して、Data Protectorパッケージを開始します。
- IDBがSymantec Veritas Cluster Server上にインストールされている場合、ガイド式自動回復を実行する前に、アクティブノード上でData Protectorアプリケーションリソースをオフラインで取り込みます。

  ガイド式自動回復が完了したら、アクティブノード上でData Protectorアプリケーションリソースをオンラインにして、Data Protectorサービスを開始します。
- IDBがMicrosoft Cluster Server上にインストールされている場合は、ガイド式自動回復を実行する前に、アクティブノード上でクラスターアドミニストレーターユーティリティを使って、`OBVS_HPDP_AS`, `OBVS_HPDP_IDB`, および`OBVS_HPDP_IDB_CP`クラスターグループをオフラインにし、`Inet`サービスを停止します。ガイド式自動回復が完了したら、クラスターアドミニストレーターユーティリティを使って`OBVS_HPDP_AS`, `OBVS_HPDP_IDB`, `OBVS_HPDP_IDB_CP`,および`OBVS_MCRS`クラスターグループをオンラインにし、`Inet`サービスを再起動します。

手順

1. Data Protector GUIを使ってデバイスを構成します。
2. 最新のIDBバックアップが含まれているメディアを見つけます。
3. メディアをデバイスに挿入し、次のコマンドを使ってメディアの内容を表示します。

   `omnimlist -dev device_name`

   IDBを復元するには、復元対象のバックアップセッションのメディアIDとDisk Agent IDが必要です。
4. 次のコマンドを使って、デバイス構成に関する情報を表示します。

   `omnidownload -dev device_name`

   IDBを復元するには、以下の情報が必要です。
   - Mahost (Media Agentホスト)
   - ポリシー(番号): ポリシー番号は次のように割り当てられています。スタンドアロンデバイスは1、スタッカーデバイスは3、ジュークボックスデバイスは5、外部制御デバイスは6、GRAU DASライブラリは8、StorageTek ACSライブラリは9、SCSIライブラリは10です。
   - メディアの種類(番号): メディアの種類番号は、`scsitab`ファイルでメディアクラスとして定義されます。場所については、「新しいデバイスのサポート」を参照してください。

- SCSIアドレス
- ロボティクスのSCSIアドレス。エクスチェンジライブラリデバイスを使用する場合のみ必要です。

5. 取得した情報を使用して`omniofflr`コマンドを実行します。

   ```
   omniofflr -idb -policy PolicyNumber -type MediaTypeNumber [-ioctl
   RoboticsSCSIAddress] -dev SCSIAddress -mahost MAClientName -maid MediumID -daid
   DiskAgentID
   ```

   次の例では、メディアIDとして`0100007f:3a486bd7:0410:0001`、Disk Agent IDとして`977824764`、接続先システムとして`company.dot.com`、およびSCSIアドレスとして`scsi0:1:2:0`を指定し、DLTのスタンドアロンデバイスを使用して、バックアップセッションからIDBを復元します。

   ```
   omniofflr -idb -policy 1 -type 10 -dev scsi0:1:2:0 -mahost company.dot.com -
   maid 0100007f:3a486bd7:0410:0001 -daid 977824764
   ```

このコマンドの実行後、画面に表示される指示に従うと、前回のIDBバックアップ以降のアーカイブログファイルを再生しながら復元処理を進めることができます。ログファイルが利用できない場合でも、前回のIDBバックアップ以降に使用されたメディアをすべてインポートすると、IDBを更新できます。

特定のIDBセッションからIDBを復元する

ここでは、最新でないバックアップから内部データベース(IDB)を復元する手順を示します。これは、IDB復旧ファイルが利用可能であることを前提としています。

前提条件

- IDBのバックアップ時と同じディレクトリ(Windowsでは、同じドライブ文字を指定すること)で、障害発生前と同じサイズのディスクをマウントします。これが確かでない場合は、IDBを別のディスク/ボリュームレイアウトに復元する手順に従ってください。`omniofflr`コマンドの`-preview`オプションを使うと、ファイルの復元先を事前に確認できます。
- 可能であれば、既存の`media.log`ファイルを安全な場所に保存しておきます。このファイルには、前回のIDBバックアップ以降に使用されたメディアに関する情報が含まれています。アーカイブログファイルが利用できない場合は、このファイルがIDBの更新に非常に役立ちます。
- Data ProtectorをCell Manager上にインストールし、その後、デバイス(なるべくIDBバックアップに使用したデバイス)が接続されているシステムにインストールします。
- IDBがHPE Serviceguard上にインストールされている場合、ガイド式自動回復を実行する前に、アクティブノード上で以下のコマンドを実行する必要があります。
  1. `cmhaltpkg PackageName`(ここで、*PackageName*はData Protectorクラスターパッケージの名前)。このコマンドにより、Data Protectorパッケージが停止され、Data Protector共有ボリュームグループがアンマウントされます。
  2. `vgchange -a e /dev/vg_name`(ここで、*vg_name*はData Protector共有ボリュームグループの名前)。このコマンドにより、Data Protector共有ボリュームグループがアクティブ化されます。システム上のボリュームグループのリストを表示するには、`ll /dev/*/group`を実行します。
  3. `mount /dev/vg_name/lv_name/MountPoint`(ここで、*MountPoint*はData Protector共有ボリュームグループのマウントポイントの名前)。このコマンドにより、Data Protector共有ボリュームグループがマウントされます。

ガイド式自動回復が完了したら、アクティブノード上で`cmrunpkg PackageName`コマンドを実行して、Data Protectorパッケージを開始します。

- IDBがSymantec Veritas Cluster Server上にインストールされている場合、ガイド式自動回復を実行する前に、アクティブノード上でHPE Data Protectorアプリケーションリソースをオフラインで取り込みます。

  ガイド式自動回復が完了したら、アクティブノード上でHPE Data Protectorアプリケーションリソースをオンラインにして、HPE Data Protectorサービスを開始します。
- IDBがMicrosoft Cluster Server上にインストールされている場合は、ガイド式自動回復を実行する前に、アクティブノード上でクラスターアドミニストレーターユーティリティを使って、`OBVS_HPDP_AS`, `OBVS_HPDP_IDB`, および`OBVS_HPDP_IDB_CP`クラスターグループをオフラインにし、`Inet`サービスを停止します。ガイド式自動回復が完了したら、クラスターアドミニストレーターユーティリティを使って`OBVS_HPDP_AS`, `OBVS_HPDP_IDB`, `OBVS_HPDP_IDB_CP`,および`OBVS_MCRS`クラスターグループをオンラインにし、`Inet`サービスを再起動し、`omnidbutil -fixmpos`コマンドを実行します。

手順

1. 次のコマンドを使って、すべてのバックアップをチェックします。

   ```
   omniofflr -idb -autorecover -logview -skiprestore
   ```
2. どのバックアップセッションのデータを復元するかを選択し、次のコマンドを実行してIDB復元を実行します。

   ```
   omniofflr -idb -autorecover -session SessionID
   ```

このコマンドの実行後、画面に表示される指示に従うと、前回のIDBバックアップ以降のアーカイブログファイルを再生しながら復元処理を進めることができます。アーカイブログファイルが利用できない場合でも、前回のIDBバックアップ以降に使用されたメディアをすべてインポートすると、IDBを更新できます。

異なるCell Managerホスト上でIDBデータベースを復元する

異なるCell Managerホスト上でIDBデータベースを復旧するには、以下の手順を実行します。

1. 新しいCell ManagerホストにData Protectorをインストールし、古いCell ManagerホストのIDBバックアップが格納されているデバイスをインポートします。
2. 構成ファイルのみを新しいディレクトリに復元します。例: `/tmp/idb/config`。
3. 元のファイル`/etc/opt/omni/server/cell/cell_info`のコピーを作成します。
4. IDBデータベース全体を新しいディレクトリに復元します。例: `/tmp/idb/newidb`。
   - データベースファイルの復元には、オプション**StartDatabaseServer**および**UseRestoredDatabaseAsNewDatabase**を選択します。
   - カタログバイナリファイルの復元先として、[元の位置に復元]を選択します。
   - 構成ファイルの復元先として**[元の位置に復元]**を選択し、ファイル重複時の処理として**[上書き]**を選択します。
5. 復元がエラーなく完了した場合、(万一に備えて)次の元のファイルのコピーを作成します。
   - `/etc/opt/omni/server/AppServer/standalone.xml`
   - `/etc/opt/omni/server/idb/idb.config`

- /etc/opt/omni/server/idb/ulist

6. 次のコマンドを実行して、Data Protectorサービスを停止します。/opt/omni/sbin/omnisv stop
7. 手順3で作成したファイルのコピーを使用して、/etc/opt/omni/server/cell/cell_infoファイルに上書きします。
8. 任意のエディターで/etc/opt/omni/server/AppServer/standalone.xml ファイルを開き、keystore-passwordとtruststore-passwordを見つけ、記録しておきます。これらは通常同じです。
9. 任意のエディターで/etc/opt/omni/client/components/webservice.propertiesファイルを開き、keystore-passwordと truststore-passwordをstandalone.xmlファイルの値に変更し、ファイルを保存して閉じます。

   注: クラスター環境では、クラスターのすべてのノードにあるwebservice.propertiesファイルを編集する必要があります。

10. 次のコマンドを実行して、証明書を再生成します。/opt/omni/bin/perl /opt/omni/sbin/omnigencert.pl -server_id *<hostname>* -user_id hpdp -store_password *<your keystore password>*
11. 次のファイルに古いCell Managerのホスト名が含まれていないことを確認します。
    - /etc/opt/omni/client/components/dp-jobexecutionengine-backup\webservice.properties /etc/opt/omni/client/components/dp-jobexecutionengine-consolidation\webservice.properties
    - /etc/opt/omni/client/components/dp-jobexecutionengine-copy\webservice.properties
    - /etc/opt/omni/client/components/dp-jobexecutionengine-verification\webservice.properties
    - /etc/opt/omni/client/components/dp-loginprovider\webservice.properties
    - /etc/opt/omni/client/components/dp-Scheduler-gui\webservice.properties
    - /etc/opt/omni/client/components/dp-webservice-server\webservice.properties
    - /etc/opt/omni/client/components/jce-dispatcher\webservice.properties
    - /etc/opt/omni/client/components/jce-serviceregistry\webservice.properties
    - /etc/opt/omni/client/components/webservice.properties
12. omnircファイルに次の変数を追加します: /opt/omni/.omnirc: OB2_CERT_VERIFYHOST=0。omnircファイルがない場合、空のテキストファイルを作成し、.omnircという名前を指定するか、.omnirc.TMPLを.omnircという名前に変更します。.omnirc
13. 次のコマンドを実行して、Data Protectorサービスを開始します。/opt/omni/sbin/omnisv start
14. 次のコマンドを実行して、Data Protectorファイルの所有権を変更します。/opt/omni/sbin/omnidbutil -change_cell_name *<old_cm_hostname>*
15. 次のコマンドを実行して、実行中のセッションをクリアします。/opt/omni/sbin/omnidbutil -clear

16. Windows GUIクライアントで、古い証明書のあるフォルダーを削除します。Data Protectorサービスを開始すると、Cell Managerにある新しい証明書がData Protector GUIにインポートされます。古い証明書は次のパスにあります。`C:\Users\<USERNAME>\AppData\Local\Hewlett-Packard\Data Protector\ca\<NEW_CM_HOSTNAME>"`
17. 必要に応じて以下の手順を実行します。
    a. 次のコマンドを実行して、IDBが新しいディレクトリのファイルを使用していることを確認します(DCBFが元のフォルダーにある場合、テーブルスペースファイルと先書きログは新しいディレクトリにあります)。`/opt/omni/sbin/omnidbutil -show_db_files`
    b. 古いCell Managerのホスト名を含んでいるファイル(通常は、ユーザーリスト、バーリスト、構成ファイル)を更新します。これらのファイルを見つけるには、次のコマンドを実行します。`grep -rnw /etc/opt/omni -e <OLD_CM_HOSTNAME>`
    c. 新しいCell Managerを使用するためにデバイスを再構成します。

メディアをインポートしてIDBを更新する

アーカイブログファイルを使用できない場合、前回のIDBバックアップ以降に使用されたすべてのメディアをインポートして内部データベースを更新します。この操作は、IDB復元の完了後に実行します。

手順

1. Data Protectorのプロセスとサービスを開始します
2. セッションカウンターの値を増やします。IDBを初期化して復元した場合、このカウンターは`0`に設定されています。したがって、新規セッションのセッションIDは、同じ日にすでに開始済みのセッションのIDと同じになってしまいます。

   次のコマンドでは、セッションカウンターを`200`に設定しています。ほとんどの場合は、これで十分です。

   ```
   omnidbutil -set_session_counter 200
   ```

   必要であれば、この時点でバックアップを開始できます。
3. 前回のIDBバックアップが含まれているメディアをエクスポートおよびインポートします。これにより、前回のIDBバックアップに関する一貫した情報が作成されます。
4. 前回のバックアップ以降、IDB復元までに使用されたメディアをインポートします(IDBにすでに含まれている場合はエクスポートします)。使用されたメディアのリストについては、デフォルトのData Protectorサーバーログファイルの場所にある`media.log`ファイルを参照してください。
5. `omnidbcheck`コマンドを実行します。

IDB全体が正常に回復されます。

> **注:**
> CMMDBまたはリモートMMDBが含まれているIDBを新しいディスクレイアウトに回復する場合は、IDBの更新後に`omnidbutil -cdbsync`コマンドを実行します。

第5章: Manager-of-Managers環境

MoM環境について

Data ProtectorのManager-of-Managers概念により、エンタープライズバックアップ環境とも呼ばれる、複数のData Protectorセルを有する大規模な環境を、管理者は一点から集中管理することができます。

この方法により、バックアップ環境の規模拡大にほぼ無限に対応でき、

各MoMクライアントとMoM Managerは、同じバージョンのData Protectorを実行する必要があります。

Manager-of-Managersは、以下の機能を提供します。

- すべてのタスクの集中管理

  Data Protectorでは、エンタープライズバックアップ環境の構成、管理、制御を一点から行うことができます。具体的には、バックアップ、復元、メディア管理、監視、バックアップ環境全体の状態のレポートの構成を行うことができます。

- メディア集中管理データベース(CMMDB)

  環境内のセルすべてに1つの共通の中央データベースを共有させ、それによって企業内のデバイスとメディアを管理することもできます。CMMDBにより、ハイエンドデバイスやメディアをMoM環境内の複数のセルで共有できます。これにより、CMMDBを使用する1つのセルのすべてのデバイスが、CMMDBを使用する他のセルでも利用可能になります。

- 集中型ライセンス

  Data Protectorでは、MoM環境全体のライセンスを集中管理できます。すべてのData Protectorライセンスは、MoM Managerにインストールして保存します。必要に応じて、ライセンスを特定のセルに割り当てます。

CMMDBについて

ハイエンドバックアップデバイスを備えたマルチセル環境においては、複数のセルでデバイスやメディアを共有したい場合があります。これを実現するには、すべてのセルに対して中央MMDBを1つ設定し、各セルに対して個別のCDBを設定します。これにより、マルチセル構造のセキュリティ機能を保全しながら、メディアおよびデバイスを共有できます。

メディアの共有方法

CMMDBでは、メディアに最初にバックアップを実行したData Protectorセルだけが、そのメディアを所有できます。メディアのオーナーはメディアビューに表示されます。メディアが保護されている間は、そのセルからのバックアップデータしかメディアに追加できません。保護データが入ったメディアには、どのセルが現在データを所有しているかを示す情報があります。保護期限が終了したメディアは、再び他のセルからも使用できるようになります。

メディアの初期化方法

1つのセルによって初期化されたテープは、保護されたデータを含んでいない限り、他のセルから使用できます。ライブラリにロードされたテープがまだ初期化されていない場合、[緩和]ポリシーが設定されていて、他に利用可能なテープがないときには、どのセルでもテープを初期化できます。メディアの割り当てルールは、共有テープにも同様に適用されます。ただし、追加可能メディアの場合は、そのメディアを所有するセルだけがデータを追加できます。

> **重要:**
> 以下の点に注意してください。
>
> - MMDBを集中管理すると、ライセンスに大きな影響があります。MMDBをローカルからリモートに変更したら、すぐに、ライブラリとデバイスに関するすべてのライセンスをMoM Managerから取得(確認)し、クライアントセルからは削除する必要があります。
> - エンタープライズ環境におけるセルがバックアップを行うには、CMMDBにアクセスできる必要があります。たとえば、セルとMoMセルとの間にネットワーク障害が発生すると、問題となります。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環境の構成手順

前提条件

- MoM Managerに使用するシステムを選択する必要があります。信頼性の高いシステム(ソフトウェアがインストールされたData Protector Cell Manager)を選択する必要があります。
- MoMセルと、MoMクライアントセルになると予想されるすべてのセルに必要なライセンスをインストールします。

MoM環境の構成手順

MoM環境を構成するには、以下の作業を実施します。

1. MoM Managerを設定します。
2. Data ProtectorセルをMoM環境にインポートします。
3. MoM管理者としての役割を果たすData Protectorユーザーを、MoM環境のすべてのセル上の`admin`ユーザーグループに作成します。
4. Data Protectorのサービスを再起動します。

メディア集中管理データベースを構成し、集中型ライセンスを構成して、MoM構成を配布することもできます。

MoM Managerを設定する

エンタープライズ環境を設定するには、いずれかのCell ManagerをMoM Managerとして構成します。

手順

1. コンテキストリストで**[クライアント]**をクリックします。
2. [アクション]メニューで、**[CMをData Protector Manager-of-Managersサーバーとして構成]**をクリックします。
3. Data Protectorサービスを再起動します。
4. Data Protectorプログラムグループの**Data Protector Manager-of-Managers**を選択してMoMユーザーインターフェイスを起動します。

   または、*Data_Protector_home*\binディレクトリから、momコマンドを実行します。momコマンドの詳細については、omnigui manページまたは『*HPE Data Protector Command Line Interface Reference*』を参照してください。

MoMの管理者をセルに追加する

MoMの管理者は、エンタープライズ環境のすべてのセルで、管理作業を行うことができます。

前提条件

MoM環境では、どのCell Manager上のadminユーザーグループにも登録されている特定のユーザーが必要になります。たとえば、「MoM_Admin」などの名前のユーザーを構成します。このユーザーがMoMの管理者となります。

手順

1. Data Protector Managerを使用して、MoM環境内の各Cell Managerにadminユーザーグループのメンバーとして接続します([User configuration]ユーザー権限が必要です)。
2. MoMの管理者となるユーザーをData Protectorのadminユーザーグループに追加します。

セルをインポートする

MoM環境にセルをインポートすると、MoM Managerを使用してセルを集中管理できます。

MoM Managerは、クラスタークライアントを仮想サーバー名で識別します。MoM環境にクラスターをインポートする場合、そのクラスターの仮想サーバー名以外は使用しないでください。

前提条件

- アクティブなユーザーは、インポート対象のセルのCell Manager上のAdminユーザーグループのメンバーでなければなりません。

手順

1. Data Protector Manager-of-Managersで、コンテキストリストの**[クライアント]**をクリックします。
2. **[エンタープライズクライアント]**を右クリックし、**[Cell Managerのインポート]**をクリックします。
3. インポートするCell Managerを選択し、**[完了]**をクリックします。

MoMでのHPE Data Protectorサービスを再起動する

MoM環境の構成後、Data Protectorのサービスを再起動するように促すメッセージが表示されます。

`Windows Service Control Manager`を使ってCell Managerのサービスの停止と開始を行うと、現在と前回のデータベースログのコピーだけが保存されます。`omnisv`コマンドを使うと、以前のすべてのデータベースログが保存されます。

Data Protectorのサービスを停止する

非クラスター環境のCell Managerの場合

次のコマンドを実行します。`omnisv -stop.`

HPE Serviceguard上のCell Managerの場合

次のコマンドを実行します。`cmhaltpkg` *`PackageName`*(ここで、*`PackageName`*はData Protectorクラスターパッケージの名前)。

このコマンドにより、Data Protectorパッケージが停止され、Data Protector共有ボリュームグループがアンマウントされます。

Symantec Veritas Cluster Server上のCell Managerの場合

HPE Data Protectorアプリケーションリソースをオフラインにします。

Microsoft Cluster Server上のCell Managerの場合

`OBVS_HPDP_AS`, `OBVS_HPDP_IDB`, 、`OBVS_HPDP_IDB_CP`クラスターグループをオフラインにします(アクティブノード上で、`Cluster Administrator`ユーティリティを実行)。

Data Protectorのサービスを開始する

非クラスター環境のCell Managerの場合

次のコマンドを実行します。`omnisv -start`

HPE Serviceguard上のCell Managerの場合

`cmrunpkg -n NodeName PackageName`コマンドを使用してData Protectorパッケージを再起動します。

Symantec Veritas Cluster Server上のCell Managerの場合

HPE Data Protectorアプリケーションリソースをオンラインにします。

Microsoft Cluster Server上のCell Managerの場合

`Cluster Administrator`ユーティリティを使用して、`OBVS_HPDP_AS, OBVS_HPDP_IDB, OBVS_HPDP_IDB_CP, and OBVS_MCRS`クラスターグループをオンラインにします。

CMMDBを構成する

メディア集中管理を行う場合は、CMMDBを設定します。CMMDBを設定しなかった場合には、各セルがIDBを持つことになります。

構成時に選択した場合、ローカルのメディア管理データベースがCMMDBとマージされます。CMMDBを使用するか、それとも専用のローカルMMDBを持たせるかを、セルごとに指定できます。

> **重要:**
> CMMDBを構成しその使用を開始してから、ローカルMMDBに分割して戻すことはできません。MMDBの以前の状態を復元するのではなく、最初からMMDBを作成しなおしてください。

必要な作業

新しいセルを構成する場合(そしてデバイスやメディアをまだ構成していない場合)は、データベースをマージする必要がありません。デバイスやメディアが既に構成されているCMMDBにセルをマージするだけです。

前提条件

- すべてのセルのData Protector Cell Managerで、同じバージョンのData Protectorがインストールされて実行されていることを確認してください。
- CMMDBに追加されるどのセル上でも、バックアップ、復元、メディア管理セッションが実行されていないことを確認してください。

クライアントセルでCMMDBを構成する

手順

1. `admin`ユーザーグループのメンバーとして、クライアントセルのCell Managerにログオンします。
2. MMDBサーバー名(完全修飾名)が含まれるファイルを作成します。Windowsシステムでは、ファイルをUnicodeとして保存します。

Windowsシステムの場合: *Data_Protector_program_data*\Config\server\cell\mmdb_server

UNIXシステムの場合: /etc/opt/omni/server/cell/mmdb_server

3. 内部データベースのpgディレクトリにあるpg_hba.confファイルを変更してMoM Managerを有効にし、セルへの接続を確立します。

   テキストエディターでファイルを開き、以下の行

   ```
   host hpdpidb hpdpidb_app MoM_Server_IP_Address/32 trust
   ```

   を、次の行の後に追加します。

   ```
   # IPv4 local connections:
   host all all 127.0.0.1/32 md5
   ```

   ファイルを保存します。

   > **注:**
   > MoMクライアント上のCell Managerがクラスター環境の一部である場合、すべてのクラスターノードのIPアドレスを(ノードごとに1行)指定するか、MoMクライアントのCell Manager上のpg_hba.confファイル内のクラスターのサブネットのいずれかを指定する必要があります。

   テキストエディターでファイルを開き、以下の行

   ```
   host hpdpidb hpdpidb_app Cluster_Subnet trust
   ```

   を、次の行の後に追加します。

   ```
   # IPv4 local connections:
   host all all 127.0.0.1/32 md5
   ```

   ファイルを保存します。

4. Data Protectorサービスを再起動します。
5. 次のコマンドを実行して、構成ファイルを更新します。

   ```
   omnicc -update_mom_server
   ```

CMMDBにMMDBをマージするすべてのクライアントセルで、上記の手順を実行します。

MoM ManagerでCMMDBを構成する

手順

1. Manager-of-Managersにログオンし、安全のため、idb表領域ディレクトリを一時的な場所にコピーします。

   idbは、内部データベースにあるサブディレクトリです。

2. 次のコマンドを実行して、ローカルMMDBをCMMDBにマージします。

   ```
   omnidbutil -mergemmdb MoM_Client_Cell_Manager_Hostname
   ```

   コマンドの実行中に、IDBサービス(hpdp-idb)ポート7112がMoM ManagerとクライアントのCell Managerの両方で開いていることを確認します。マージが完了したらポートを閉じてください。

3. 次のコマンドを実行して、ローカルCDBを同期化します。

   ```
   omnidbutil -cdbsync MoM_Client_Cell_Manager_Hostname
   ```

4. メディアプールおよびデバイスの重複する名前を編集します。両方のセルにデフォルトプールが存在す

る場合は、必ずプール名が重複します。重複名は元の名前に"_N"が追加されたものであり、このNは数値を示します。この場合、これらのデバイスを使用するバックアップ仕様を手作業で変更し、新しいデバイス名を使用させます。

CMMDBにMMDBをマージするすべてのクライアントセルで、上記の手順を実行します。

集中型ライセンスについて

集中型ライセンスによって、MoM Managerですべてのライセンスを設定し、必要に応じて特定のセルに割り当てることができます。集中型ライセンスによって、ライセンス管理が簡単になります。ライセンスの配布や移動などのライセンス管理作業は、MoM環境内のすべてのセルに対してMoMの管理者が実行します。

集中型ライセンスの設定は必須ではありません。集中型ライセンスを設定しない場合、ライセンスは各Cell Managerに個別にインストールできます。この場合、ライセンスはインストールしたセルに限定され、すべてのライセンス管理作業はローカルで実行する必要があります。

集中型ライセンスを設定する

エンタープライズ環境のライセンス管理を簡素化するために、集中型ライセンスを設定します。

前提条件

既存のData ProtectorセルをMoM環境に統合する場合は、既存の*Cell Manager*から新しいMoM Managerにライセンスを移動するための要求をHPE Password Delivery Centerに送信します。

手順

1. MoM Managerにログオンし、`licdistrib.dat`ファイルを作成します。

   Windowsシステムの場合: *`Data_Protector_program_data`*`\Config\server\cell\licdistrib.dat`

   UNIXシステムの場合: `/etc/opt/omni/server/cell/licdistrib.dat`
2. MoM環境で各Cell Managerにログオンし、MoM Managerの名前で`lic_server`ファイルを作成します。

   Windowsシステムの場合: *`Data_Protector_program_data`*`\Config\server\cell\lic_server`

   UNIXシステムの場合: `/etc/opt/omni/server/cell/lic_server`
3. 変更を行った各Cell Manager上でData Protectorサービスを停止し、再度開始します。
4. Data Protector Manager-of-Managersで、コンテキストリストの**[クライアント]**をクリックします。
5. Scopingペインで、移動するライセンスの情報が保存されているCell Managerを右クリックし、**[ライセンス付与の構成]**をクリックしてウィザードを起動します。選択したCell Managerで利用可能なライセンスの種類および数が表示されます。

   > **注:**
   > クラスタークライアントは、仮想ホスト名で識別します。

6. **[リモート]**オプションをクリックして、ライセンス管理をローカルからリモートに変更します。列の名前は、

[使用中]から[割り当て済]に変更されます。

7. ライセンス構成を変更します。変更プロセス中は[割り当て済]列のみが使用できます。
   - ライセンスの種類を解放し、利用可能なライセンス数を増やすには、[割り当て済み]列の該当する数を減らします。
   - ライセンスのタイプを割り当てるには、[割り当て済み]列の該当する数を大きくします。
8. **[完了]**をクリックして設定を適用します。
9. 集中型ライセンスを設定するすべてのCell Managerで、上記の手順を実行します。
10. `omnisv -stop`コマンドおよび`omnisv -start`コマンドを使用し、Data Protectorプロセスを停止して再起動します。

    Cell ManagerがHPE Serviceguard上で構成されている場合は、`cmhaltpkg PackageName`コマンドを実行して停止し、`cmrunpkg -n NodeName PackageName`でData Protectorパッケージを起動します。*PackageName*には、Data Protectorクラスターパッケージの名前を指定します。

    Symantec Veritas Cluster Server上にCell Managerを構成する場合、Data Protectorアプリケーションリソースをオフラインにし、Data Protectorアプリケーションリソースをオンラインにします。

変更内容は、変更を行った各Cell ManagerでData Protectorサービスを停止して再度開始すると有効になります。

> **注:**
> Data Protectorでは、MoM Managerを使用してライセンス構成が1時間ごとに確認されます。通信の障害が発生した場合や、MoM Managerが使用不可になっている場合は、ライセンス状態は72時間保持されます。この時間内に障害が解消されない場合は、ローカルライセンスが使用されます。

集中型ライセンスを無効にする

集中型ライセンスを無効にして、ローカルでのライセンス管理に変更できます。

手順

1. Data Protector Manager-of-Managersで、コンテキストリストの**[クライアント]**をクリックします。
2. Scopingペインで、集中型ライセンスを無効にするCell Managerを右クリックし、**[ライセンス付与の構成]**をクリックしてウィザードを起動します。選択したCell Managerで利用可能なライセンスの種類と数が表示されます。

   > **注:**
   > クラスタークライアントは、仮想ホスト名で識別します。

3. **[ローカル]**オプションをクリックして、ライセンス管理をリモートからローカルに変更します。
4. **[完了]**をクリックして設定を適用します。
5. 集中型ライセンスを無効にするすべてのCell Managerで、上記の手順を実行します。
6. MoM Managerにログオンして、デフォルトのData Protectorサーバー構成ディレクトリにある`cell`ディレクトリをマウントします。
7. `licdistrib.dat`のファイル名を`licdistrib.old`.

変更した内容は、変更を行ったMoM Managerや各Cell Manager上で、`omnisv -stop`コマンドおよび`omnisv -start`コマンドを実行し、Data Protectorサービスを終了して再起動するまで有効になりません。

Cell ManagerがHPE Serviceguard上で構成されている場合は、`cmhaltpkg PackageName`コマンドを実行して停止し、`cmrunpkg -n NodeName PackageName`でてData Protectorパッケージを起動します。*PackageName*には、Data Protectorクラスターパッケージの名前を指定します。

Symantec Veritas Cluster Server上にCell Managerを構成する場合、HPE Data Protectorアプリケーションリソースをオフラインにし、HPE Data Protectorアプリケーションリソースをオンラインにします。

MoM環境の管理について

MoM Managerを使用して、エンタープライズバックアップ環境の構成、管理、制御を1つの場所から集中的に行うことができます。

MoMユーザーインターフェイスでは、セルのインポートやエクスポート、セル間でのクライアントの移動、環境内の他のセルへのMoM構成の配布が可能です。

MoM Managerでは、その他の作業もローカル管理者として行う場合と同様に実施できます。通常の手順に従って、バックアップや復元の構成、特定のセルに対するデバイスやメディアの管理、Data Protectorユーザーやユーザーグループの構成、クライアントの追加、実行中のセッションおよびバックアップ環境の状態のモニター、レポートや通知の構成を行います。

> **注:**
> 個々のセル内のクライアントに接続されているデバイスは、対応するCell Managerからのみ構成できます。MoM Managerから構成することはできません。Cell Managerに直接接続されているデバイスだけは、MoM Managerから構成できます。

セルをエクスポートする

セルをエクスポートすると、そのセルはMoM環境から削除されます。

MoM Managerは、クラスタークライアントを仮想サーバー名で識別します。MoM環境内でクラスターをエクスポートする場合、仮想サーバー名以外は使用しないでください。

手順

1. Data Protector Manager-of-Managersで、コンテキストリストの**[クライアント]**をクリックします。
2. Scopingペインで、エクスポートするCell Managerを右クリックし、**[Cell Managerのエクスポート]**をクリックします。
3. 選択を確定します。

セル間でクライアントシステムを移動する

Data Protectorでは、セル間でシステムを移動できます。システムを移動する際にData Protectorは以下の処理を行います。

- 移動対象のクライアントがいずれかのバックアップ仕様内に構成されているかどうかを確認し、当初のCell Manager上で構成されていたバックアップ仕様からそのクライアントに属するバックアップオブジェクトをすべて削除します。Data Protector他のクライアントのバックアップオブジェクトは、そのままの状態で維持します。
- 対象のシステムでデバイスが構成されているかどうかを確認し、構成されたデバイスがある場合は、別のシステムにデバイスを移動する手順を示します。
- 対象のシステムのデバイスで使用されているメディアがあるかどうかを確認し、使用中のメディアがある場合はそれを移動する手順を示します。

手順

1. Data Protector Manager-of-Managersで、コンテキストリストの**[クライアント]**をクリックします。
2. 別のセルに移動するクライアントシステムが含まれたCell Managerを展開します。
3. クライアントシステムを右クリックし、**[クライアントシステムを別のセルへ移動]**をクリックしてウィザードを起動します。
4. 移動先のCell Managerを選択します。
5. **[完了]**をクリックしてクライアントを移動します。

集中型ライセンスを無効にする

ユーザークラス仕様では、共通のユーザークラス仕様、Holidaysファイル設定、グローバルオプション設定、ボールティングを、MoM環境内のすべてのCell Manager上に作成できます。

前提条件

MoM Manager上で、ユーザークラス仕様、Holidaysファイル設定、グローバルオプション設定を作成します。

手順

1. Data Protector Manager-of-Managersで、コンテキストリストの**[クライアント]**をクリックします。
2. **[エンタープライズクライアント]**を右クリックし、**[構成を配布]**をクリックします。
3. [構成を配布]ダイアログボックスで、配布する構成の種類と、配布先のCell Managerを選択します。
4. **[完了]**をクリックして構成を配布します。

HPE Data Protectorユーザーの構成

ユーザーまたはユーザーグループをMoM環境に保存します。保存する方法は、単一のCell Managerの場合と同じです。この手順では、すべてのCell Managerを更新して新しいユーザーを設定します。

手順

1. Data Protector Manager-of-Managersで、コンテキストリストの**[ユーザー]**をクリックします。
2. ユーザーを追加するCell Managerを選択します。
3. [編集]メニューで**[追加]**をクリックし、新しいユーザーを追加する場合は**[ユーザー]**を、新しいユーザーグループを追加する場合は**[ユーザーグループ]**を選択します。
4. 必要事項を入力して**[完了]**をクリックします。

ユーザーを他のセルに追加する

既存のユーザーをMoM環境内の他のセルに追加することができます。追加したユーザーは、ターゲットのCell Manager上のユーザーグループのうち、ソースCell Manager上で所属しているのと同じユーザーグループに自動的に追加されます。

> **注:**
> ソースCell Manager上でユーザーが所属しているのと同じユーザーグループがターゲットCell Manager上に存在しない場合、ユーザーをセルに追加することはできません。

手順

1. Data Protector Manager-of-Managersで、コンテキストリストの**[ユーザー]**をクリックします。
2. Scopingペインで、Cell Managerを展開した後、ユーザーが所属しているユーザーグループを展開します。
3. ユーザーを右クリックし、**[ユーザーを別のセルへ追加]**をクリックしてウィザードを起動します。
4. 1つまたは複数のターゲットCell Managerを選択します。
5. **[完了]**をクリックしてウィザードを終了します。

ユーザーをセルから削除する

ユーザーをMoM環境内のセルから削除できます。

手順

1. Data Protector Manager-of-Managersで、コンテキストリストの**[ユーザー]**をクリックします。
2. Scopingペインで、Cell Managerを展開した後、ユーザーが所属しているユーザーグループを展開します。
3. ユーザーを右クリックし、**[ユーザーをセルから削除]**をクリックしてウィザードを起動します。
4. ユーザーを削除するCell Managerを選択します。
5. **[完了]**をクリックしてウィザードを終了します。

特定のセル用のデバイスとメディアを管理する

デバイスおよびメディアを、エンタープライズ環境内のあらゆるセルに対して構成できます。

手順

1. Data Protector Manager-of-Managersで、コンテキストリストの**[クライアント]**をクリックします。
2. 管理対象のデバイスまたはメディアを含むセルを選択します。
3. **[ツール]**メニューの[デバイスとメディアの管理]**をクリックします。**
   Data Protector Managerが起動され、[デバイス/メディア]コンテキストが表示されます。
4. デバイスとメディアを、自分がローカル管理者であるものとして構成します。

> **注:**
> 個々のセル内のクライアントに接続されているデバイスは、対応するCell Managerからのみ構成できます。MoM Managerから構成することはできません。Cell Managerに直接接続されているデバイスだけは、MoM Managerから構成できます。

特定のセルに対して内部データベースを管理する

エンタープライズ環境内のあらゆるセルに対するIDBを管理できます。

手順

1. Data Protector Manager-of-Managersで、コンテキストリストの**[クライアント]**をクリックします。
2. 管理するCell Managerを選択します。
3. **[ツール]**メニューで、**[データベース管理]**をクリックします。[内部データベース]コンテキストで、ローカル管理者として行う場合と同様にデータベースの管理作業を行います。

第6章: クラスター

クラスターについて

クラスターの概念、アーキテクチャー、およびクラスター環境のHPE Data Protectorの詳細については、『*HPE Data Protectorコンセプトガイド*』を参照してください。

クラスター環境でのHPE Data Protectorのインストールの詳細については、『*HPE Data Protectorインストールガイド*』を参照してください。

HPE Data ProtectorのMicrosoft Cluster Server用統合ソフトウェアについて

クラスターの概念、アーキテクチャー、およびクラスター環境のHPE Data Protectorの詳細については、『*HPE Data Protectorコンセプトガイド*』を参照してください。

クラスター環境でのHPE Data Protectorのインストールの詳細については、『*HPE Data Protectorインストールガイド*』を参照してください。

Data Protectorは高可用性の一部としてMicrosoft Cluster Server (MSCS)との統合を実現しているため、クラスター環境で実行されるクラスター全体(ローカルディスクと共有ディスク)とアプリケーションのバックアップが可能です。サポートされているオペレーティングシステムのバージョン、クラスターサポートのレベル、およびサポートされている構成の詳細については、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。

ここでは、MSCSに関する知識がある読者を想定しています。MSCSの詳細については、MSCSのオンラインドキュメントを参照してください。

ライセンスとMSCS

Data Protector Cell Manager用のライセンスは、仮想サーバーに対するライセンスであり、MSCSクラスター内のどのシステムでData Protector Cell Managerが実行されているかに関係なく使用できます。

構成

この統合ソフトウェアには、以下の2通りの構成方法があります。

- Data Protector Cell ManagerはMSCSにインストールできます。この結果、Data Protector Cell Managerの可用性が向上するとともに、フェイルオーバー発生時に1つのクラスターノードから別のクラスターノードにData Protectorサービスを自動的に移行することが可能となり、それによって失敗したバックアップセッションを自動的に再起動できます。
- Data Protectorクラスター対応クライアントをMSCSにインストールできます。それによって、ファイルシステムのバックアップとクラスター対応アプリケーションのバックアップがサポートされます。

  クラスター対応アプリケーションをバックアップするには、そのアプリケーションの仮想サーバー名を使用してバックアップ仕様を構成します。

> **注:**
> クラスターサービスのコンポーネント(Database Managerなど)では、中央のクラスターデータベースの一貫したイメージを維持します。このデータベースには、ノード、リソース、またはグループのステータスの変更に関する情報が格納されます。クラスターデータベースは、クラスターの共有ディスクボリューム上に置く必要があります。

クラスター対応バックアップの管理方法

Data ProtectorクラスターCell Managerでは、バックアップセッションはクラスター対応です。Data Protectorまたは他のクラスター対応アプリケーションのフェイルオーバーが発生した場合のバックアップ処理を定義するオプションを設定できます。

Data Protectorのフェイルオーバー

クラスター対応Data Protectorのフェイルオーバーがバックアップ中に発生すると、完了していないバックアップセッションがすべて失敗します。Data Protector GUIおよびバックアップ仕様では、Data Protectorのフェイルオーバー時におけるバックアップセッションの自動再開を定義する3つのオプションのいずれかを選択できます。

Data Protector以外のアプリケーションのフェイルオーバー

クラスター対応Data Protectorはクラスター環境内のストレージアプリケーションなので、クラスター内で動作している可能性がある他のアプリケーションを認識する必要があります。他のアプリケーションがData Protectorと異なるノードで動作している場合に、他のアプリケーションがData Protectorと同じノードにフェイルオーバーすると、そのノードの負荷が増大します。つまり、バックアップ処理だけを管理していたノードで重要なアプリケーション要求も処理しなければならなくなります。Data Protectorでは、そのような状況において重要なアプリケーションデータの保護および負荷の再調整を可能にするために実行すべき処理内容を指定することができます。

実行できる内容は次のとおりです。

- すべての実行中バックアップセッションを中止する

  バックアップの重要度がアプリケーションより低い場合は、アプリケーションのフェイルオーバー後に、すべての実行中Data Protectorセッションを自動的に中止して負荷を調整することができます。

  このオプションを設定するには、`omniclus`コマンドを使って適切なスクリプトを作成する必要があります。

- バックアップ処理を一時的に無効化する

  バックアップの重要度がアプリケーションより低い場合は、アプリケーションのフェイルオーバー後に、Cell MaData Protectornagerを一時的に自動で無効化して負荷を調整することができます。すべての実行中セッションが続行されますが、Cell Managerを再度有効化するまでの間は新しいバックアップを開始できません。

  このオプションを設定するには、`omniclus`コマンドを使って適切なスクリプトを作成する必要があります。

- セッションの経過時間に基づいて実行中セッションを中止する

  アプリケーションのフェイルオーバー後に、セッションのこれまでの実行時間に基づいてバックアップセッションを中止することで負荷を調整することができます。実行中のバックアップセッションが終了すると、その

直後にData Protectorはセッションを続行できます。バックアップセッションが開始された直後で、かつそのバックアップが重要でない場合、Data Protectorはセッションを中止できます。

これらのオプションのいずれかを設定するには、omniclusコマンドを使って適切なスクリプトを作成し、Data Protector GUIでクラスターバックアップオプションを設定します。

- 論理IDに基づいて実行中セッションを中止する

  アプリケーションより重要度が高いバックアップセッションがある場合は、そのバックアップセッションを続行することができます。Data Protector フェイルオーバー後に、重要なバックアップセッションを中止IDで指定し、それ以外のバックアップセッションをすべて中止することで負荷を調整できます。

  このオプションを設定するには、omniclusコマンドを使って適切なスクリプトを作成し、Data Protector GUIでクラスターバックアップオプションを設定します。

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

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

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

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

考えられるシナリオ

MSCSのディザスタリカバリに関しては、2通りのシナリオが考えられます。

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

HPE Data ProtectorのHPE Serviceguard用統合ソフトウェアについて

クラスターの概念、アーキテクチャー、およびクラスター環境のHPE Data Protectorの詳細については、『*HPE Data Protectorコンセプトガイド*』を参照してください。

クラスター環境でのHPE Data Protectorのインストールの詳細については、『*HPE Data Protectorインストールガイド*』を参照してください。

Data Protectorでは、高可用性の一部としてHP-UXシステム用とLinuxシステム用のHPE ServiceGuard (HPE SG)との統合を実現しているため、クラスター環境で実行されるクラスター全体(ローカルディスクと共有ディスク)とアプリケーションのバックアップが可能です。サポートされているオペレーティングシステムのバージョン、サポートされている構成、およびクラスターサポートレベルの詳細については、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。

ここでは、HPE Serviceguardに関する知識がある読者を想定しています。HPE Serviceguardの詳細については、『*Managing HPE Serviceguard*』マニュアルを参照してください。

ライセンスとHPE Serviceguard

Data Protector Cell Manager用のライセンスは、仮想サーバーにバインドされており、パッケージが物理ノードのいずれかで実行されている限り、HPE SGクラスター内のどの物理ノードでData Protectorクラスターパッケージが実行されているかに関係なく使用できます。

構成

この統合ソフトウェアには、以下の2通りの構成方法があります。

- Data Protector Cell ManagerはHPE SGにインストールできます。これによって、フェイルオーバーの場合に、Data Protectorサービスを1つのクラスターノードから別のクラスターノードに自動的に移行できるようになり、それによって失敗したバックアップセッションを自動的に再起動できます。

  非アクティブなクラスターノードは、インストールサーバーとしても使用できます。
- Data Protectorクラスター対応クライアントをHPE SGにインストールできます。それによって、ファイルシステムのバックアップとクラスター対応アプリケーションのバックアップがサポートされます。

HPE Data ProtectorのHACMPクラスター用統合ソフトウェアについて

クラスターの概念、アーキテクチャー、およびクラスター環境のHPE Data Protectorの詳細については、『*HPE Data Protectorコンセプトガイド*』を参照してください。

クラスター環境でのHPE Data Protectorのインストールの詳細については、『*HPE Data Protectorインストールガイド*』を参照してください。

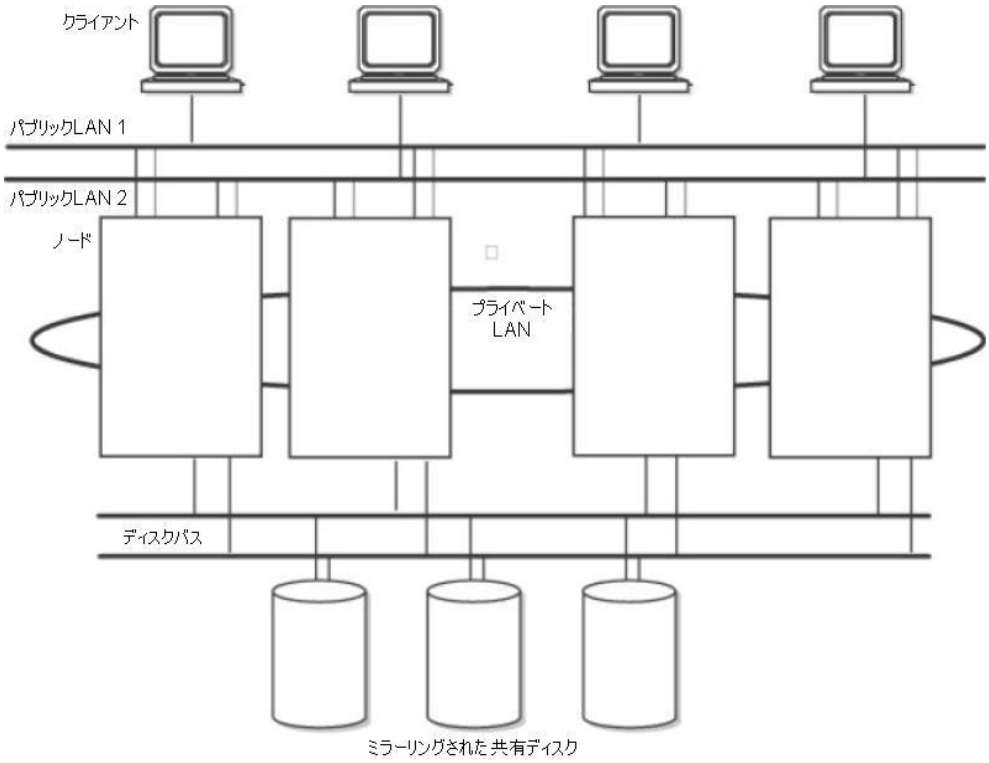
HACMPソフトウェアは、UNIXベースのミッションクリティカルなコンピューター環境を構築するためのIBMのソリューションで、高可用性(HA)とクラスターのマルチプロセッシング(CMP)に基づいています。これは、アプリケーションなどの重要なリソースを確実に処理できるようにします。

HACMPクラスターを作成する主な理由は、ミッションクリティカルなアプリケーションに対して可用性の高い環境を提供することです。たとえば、HACMPクラスターでは、クライアントアプリケーションにサービスを提供するデータベースサーバープログラムを実行できます。クライアントがサーバープログラムにクエリを送信すると、サーバープログラムは共有外部ディスクに格納されているデータベースにアクセスして、要求に応答します。

HACMPクラスター内でアプリケーションを確実に使用できるように、アプリケーションはHACMP制御化に置きます。HACMPは、クラスター内のコンポーネントに障害が発生した場合でも、アプリケーションが引き続きクライアントプロセスを処理できるようにします。コンポーネントに障害が発生した場合、HACMPは、アプリケーションおよびアプリケーションにアクセスするために必要なリソースをクラスター内の別のノードに移動します。

クラスター全体は、ネットワーク上のHACMPクラスター全体を表す仮想サーバー名(仮想環境のドメイン名)を介してアクセスされます。

一般的なHACMPクラスターの設定



図からわかるように、HACMPクラスターは次の物理コンポーネントから構成されています。

- ノード
- 共有外部ディスクインターフェイス
- ネットワーク
- ネットワークインターフェイス
- クライアント

ノード

ノードはHACMPクラスターの中核を形成します。各ノードは一意の名前で識別され、AIXオペレーティングシステム、HACMPソフトウェア、およびアプリケーションソフトウェアを実行するプロセッサーが含まれています。1つのノードが、一連のリソースディスク、ボリュームグループ、ファイルシステム、ネットワーク、ネットワークアドレス、およびアプリケーションを所有することができます。

共有外部ディスクインターフェイス

各ノードは、1つまたは複数の共有外部ディスクデバイス(複数のノードに物理的に接続されているディスク)にアクセスできます。共有ディスクには、ミッションクリティカルなデータ(一般には、データ冗長性用にミラー化またはRAID構成されたデータ)が格納されます。HACMPクラスター内のノードには、オペレーティングシステムおよびアプリケーションのバイナリデータを格納する内部ディスクもありますが、これらのディスクは共有されません。

ネットワーク

HACMPソフトウェアは、AIXオペレーティングシステムの独立した階層化コンポーネントとしてTCP/IPベースのネットワークで動作するように設計されています。ノードはネットワークを介して、次のことを行います。

- クライアントがクラスターノードにアクセスできるようにする。
- クラスターノードがハードビートメッセージをやり取りできるようにする。
- データへのアクセスを逐次化する(同時アクセス環境の場合)。

HACMPソフトウェアが定義する通信ネットワークは2種類あります。これは、使用している通信インターフェイスがTCP/IPサブシステムに基づくTCP/IPベースであるか、または非TCP/IPサブシステムに基づくデバイスベースであるかで決まります。

クライアント

クライアントは、クラスター内のノードにLAN経由でアクセスできるプロセッサーです。クライアントは、"フロントエンド"アプリケーションまたはクライアントアプリケーションを実行して、

クラスターノード上で実行しているアプリケーションをサーバーに照会します。

タスク

Data Protector IBM HACMPクラスター用統合ソフトウェアのインストールおよび構成方法

第7章： ホームコンテキスト

Data Protector 10.00では、新しい管理コンテキストがGUIに導入されています。これにより、**ダッシュボード**、**テレメトリー**UI、およびWebベースの**スケジューラー**へのアクセス方法が統一されます。

ダッシュボード

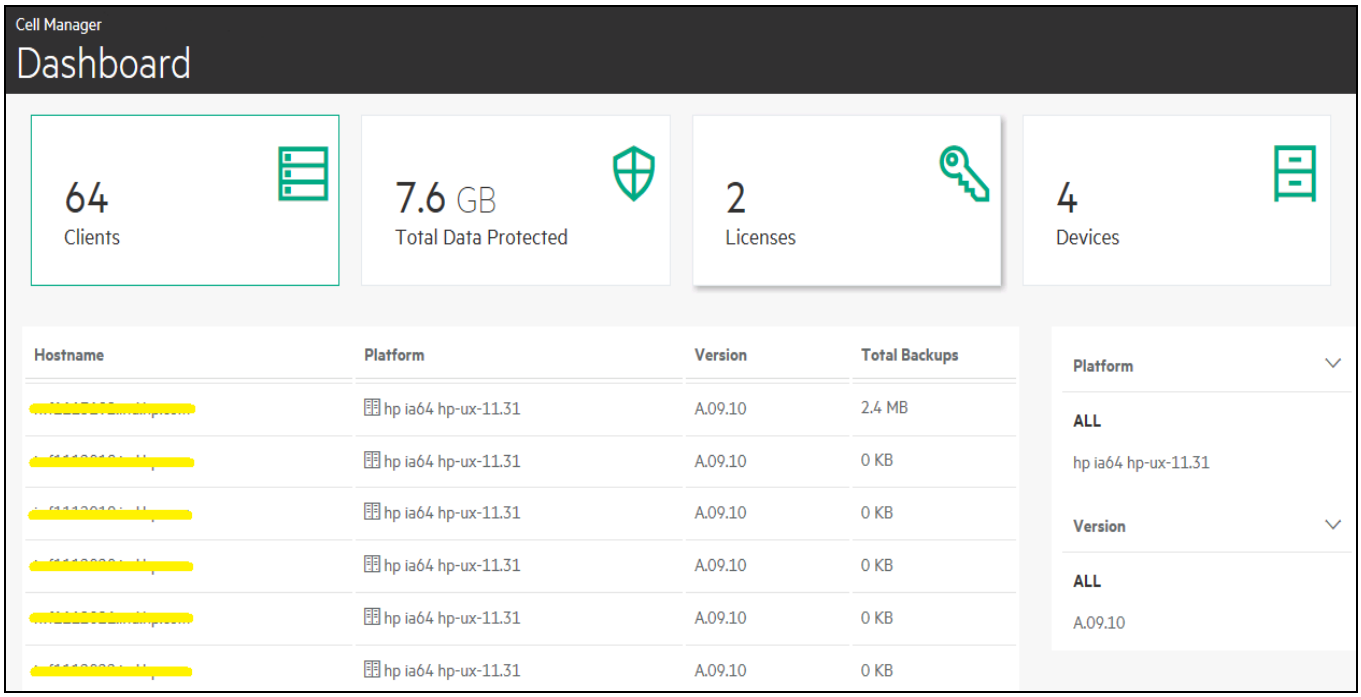
ダッシュボードページには、保護されているデータ合計、使用可能なクライアント、ストレージデバイス、インストールされているライセンスなど、Cell Managerインスタンスの合計概要が表示されます。

ダッシュボードページのアクセス方法は？

ダッシュボードページにアクセスするには、GUIの**ホーム**コンテキストメニューをクリックし、左ペインのダッシュボードをクリックします。

ダッシュボードページは、以下の4つのカテゴリに分割されています。

- クライアント
- 保護されているデータ合計
- ライセンス
- デバイス



クライアント

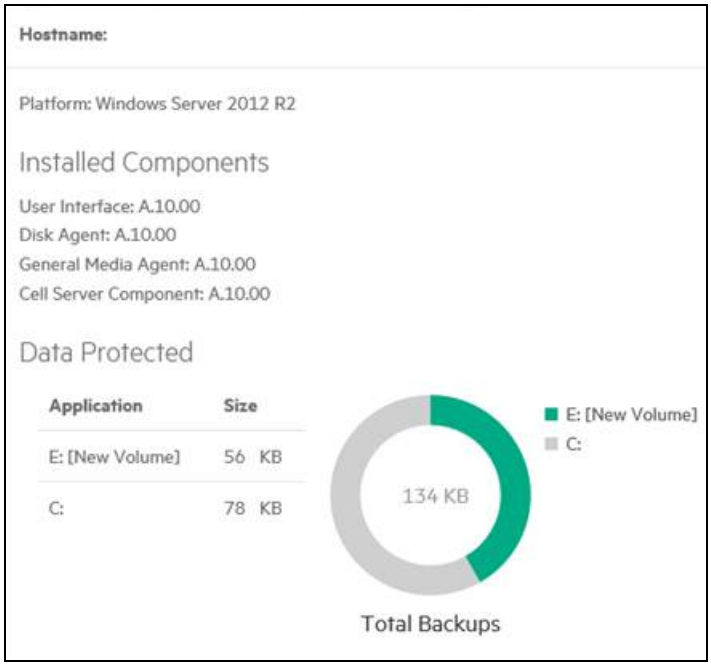
クライアントリストに、現在構成されているすべてのクライアントが、ホスト名、オペレーティングシステム、バージョン、合計バックアップと共に表示されます。

- **ホスト名**: この列には、使用可能なクライアントのすべてのホスト名が表示されます。ホスト名は、選択値に基づいて昇順または降順で並べ替えることができます。

  行をクリックすると、インストールされているコンポーネントとアプリケーションバックアップに関する情報が記載された、**[クライアントの追加の詳細]**ダイアログボックスが表示されます。バックアップは、さまざまなアプリケーションバックアップを示したチャートとして表示されます。
- **プラットフォーム**: この列には、クライアントが使用するすべてのオペレーティングシステムが表示されます。ページの右側にある追加フィルターを使用すると、特定のオペレーティングシステムを持つクライアントを表示できます。
- **バージョン**: この列には、Cell Managerバージョンまたはクライアントバージョンのバージョン番号が表示されます。ページの右側にある追加フィルターを使用すると、特定のバージョンを持つクライアントを表示できます。
- **合計バックアップ**: この列には、各クライアントでバックアップされているデータの合計が表示されます。

保護されているデータ合計

Cell Manager上で保護されているデータの合計です。データは、各データの種類(filesystem)のバックアップ済みデータの量を示したグラフ形式で表示されます。



ライセンス

各システムにインストールされているライセンスの数です。さらに以下のカテゴリに分割されています。

- **オンラインライセンス**: オンラインライセンスは、一定期間ライセンスを取得できるライセンスメカニズムです。
- **容量ライセンス**: 容量ライセンスは、バックアップするデータの量に基づいてライセンスを取得できるライセンスメカニズムです。

デバイス

Cell Manager上のすべてのストレージデバイスのリストを表示します。

さらに以下のカテゴリに分割されています。

- **ホスト名**: この列には、デバイスまたはメディアサーバーのホスト名が表示されます。選択値に基づいて昇順または降順で並べ替えることができます。
- **ライブラリ名**: この列には、ストレージデバイスのすべてのライブラリ名が表示されます。
- **デバイス**: この列には、ストレージデバイスのデバイスの種類が表示されます。ページの右側に、特定のデバイスの種類に基づいて列をフィルターするオプションがあります。
- **種類**: この列には、ストレージデバイスのデバイスの種類が表示されます。
- **プール名**: この列には、ストレージデバイスのすべてのメディアプールが表示されます。
- **使用状況**: データのバックアップに使用されるデバイスの容量です。

テレメトリー

Data Protectorテレメトリークライアントサービスは、アプリケーションサーバーを使用してData Protector Cell Managerからデータを収集し、テレメトリーデータを今後の分析のためにHPE Data Protectorサポートにアップロードします。

テレメトリーページへのアクセス方法

テレメトリーページにアクセスするには、GUIの**[ホーム]**コンテキストメニューをクリックして、左ペインの[テレメトリー]をクリックします。

テレメトリークライアントサービスは、セルコンソール(CC)クライアントに展開されるWindowsおよびLinuxのサービスです。サービスページにはData Protectorテレメトリークライアントサービスが表示され、ユーザーはここでサービスを開始または停止することができます。

Data Protectorはテレメトリクスの以下の上位レベルの情報を収集します。

- コンポーネント情報 - Data Protectorのコンポーネントとそのバージョンホストのバージョンに関する情報も収集されます。
- デバイスまたはメディアサーバー - Cell Manager内のクライアントに関連付けられている詳細情報。ホスト名の詳細、ホストに接続されているデバイスの使用状況、デバイス名、ライブラリ名、デバイスの種類、メディアが配置されているプール名などの情報です。
- デバイス使用状況 – デバイスの使用状況。
- 容量ベースのライセンス(CBL) - CBLは容量に関する情報の収集に活用されます。詳細は、『*HPE Data Protectorインストールガイド*』を参照してください。
- 従来のライセンスのカテゴリ - ホストごとにインストールされているライセンスと、使用可能なライセンスについての情報が収集されます。
- クライアント使用状況 - 情報が、クライアントごとに収集されます。ホスト名、アプリケーション名、バックアップ済みデータの合計サイズなどの情報があります。
- ストレージ使用状況 - デバイスにバックアップされているデータの合計です。

前提条件

- CCに展開するテレメトリークライアントサービスは、HPEサポートバックエンドサーバーと通信するために、プロキシを構成する必要があります。
- テレメトリーを構成する際は、お客様名とプロキシ情報を用意しておく必要があります。

> **注:**
> お客様関連の内部情報が収集されますが、ホスト情報はマスクされます。
>
> テレメトリーデータの収集中に、Cell Managerのパフォーマンスに影響を及ぼすことはありません。

制限事項:

- テレメトリークライアントサービスは、Windows x64およびLinux x64オペレーティングシステムでのみサポートされます。

テレメトリーの機能

テレメトリーの登録時に、情報がIDBに格納されます。DP GUIコンポーネントがインストールされているWindowsホストが、テレメトリークライアントに適しています。構成済みのアップロード間隔に応じて、セルコンソール(CC)クライアントは、IDB設定をチェックして、Cell Managerからテレメトリーデータを取得し、データをバックエンドサーバーにアップロードします。

収集プロセス中にサービスがオフラインになっている場合は、テレメトリーのアップロードは行われません。サービスがオンラインになると、クライアントはテレメトリーデータをアップロードできるようになります。

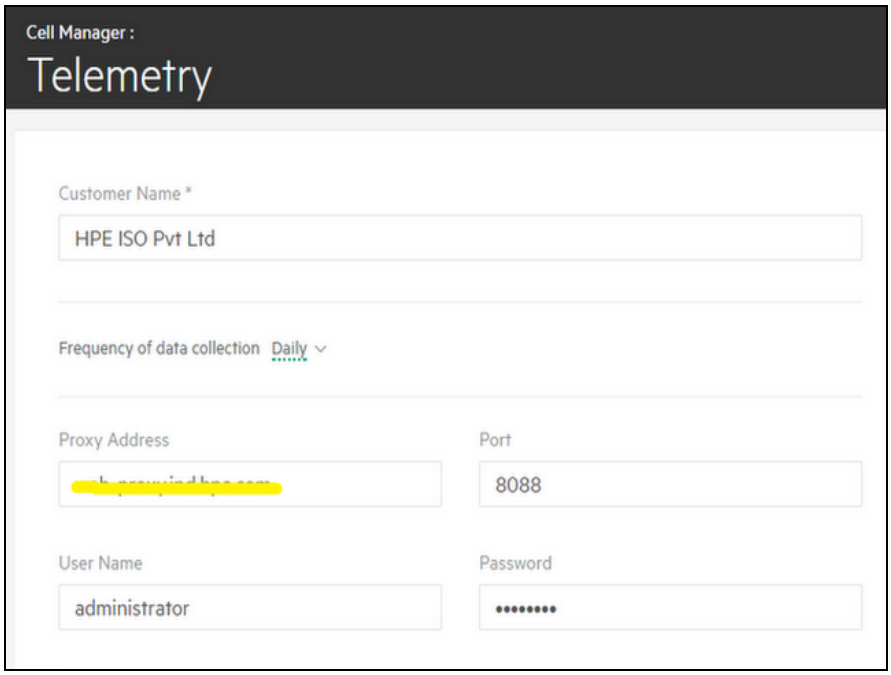
セル内に複数のテレメトリークライアントがある場合、1つのクライアントのみが、アップロード間隔に従ってバックエンドへのアップロードを実行します。IDBは、アップロードのステータスと時間を使用して更新されます。

外部ネットワークにアクセスするためにプロキシが必要な場合は、テレメトリークライアントからプロキシパラメーターを指定する必要があります。これは、直接接続が可能な場合は無視できます。

テレメトリーページ

テレメトリーページから、テレメトリー更新に対する登録または登録解除を行えます。テレメトリー更新に登録する場合は、以下のフィールドに入力してください。

- **お客様名**: お客様の名前。
- **データ収集の頻度**: データ収集を許可する頻度を、[日数単位]、[週単位]、[月単位]、および[四半期単位]から選択できます。
- **プロキシ**[オプション]: 構成済みのプロキシサーバーのアドレス。
- **ポート**[オプション]: プロキシサーバーのポート。
- **ユーザー名** [オプション]: プロキシサーバーに接続するためのユーザー名。
- **パスワード** [オプション]: 指定したユーザー名のパスワード。



上記フィールドに入力し、データ収集の頻度を選択したら、使用条件に同意し、**[登録]**をクリックします。

スケジューラー

> **重要:**
> Data Protector 10.00では、基本スケジューラーとアドバンストスケジューラーが廃止され、代わりに新しいWebベーススケジューラーが導入されました。アップグレード時に、既存のすべてのスケジューラーが、新しいスケジューラーに自動的に移行されます。

Data Protector 10.00では、洗練されたユーザーインターフェイスと簡単で使いやすいWebコントロールが搭載された新しいスケジューラーにより、スケジュール管理が容易になります。スケジュールの優先順位、データ保護、繰り返しパターンの設定や、予定の重複の修正を1つのスケジューラーウィザードで行うことができます。

スケジューラーを使用して、定期的な間隔でバックアップ、メディアコピー、オブジェクト集約およびコピーなどのさまざまな操作を自動化できます。無人で操作をバックグラウンド実行することにより、操作を実行するたびにスケジュールを手動で繰り返す必要がなくなります。

スケジューラーページへのアクセス方法

スケジューラーページにアクセスするには、GUIの**[ホーム]**コンテキストメニューをクリックして、左ペインの**[スケジューラー]**をクリックします。

以前のバージョンからのスケジュールの移行

Data Protector 10.00にアップグレードするとき、既存のスケジュールはすべて新しいWebベースのスケジューラに自動的に移行されます。手動による操作は不要です。

Data Protector 10.00へのアップグレードの際、既存のスケジュールファイルには.migrateというサフィックスが付きます。

たとえば、10.00より前のバージョンのData ProtectorでWeeklyBackupという名前のバックアップ仕様スケジュールを使用していた場合、このファイル名はアップグレード中にWeeklyBackup.migrateに変更されます。移行に失敗した場合、ファイル名は変更されません。

スケジュールが正しく移行されない場合、トラブルシューティングのために、HPEサポートからこれらの.migrateファイルの提供を求められる場合があります。

移行後のスケジュールファイルは以下の場所にあります。

仕様の種類	スケジュールのパス
バックアップスケジュール	Windowsの場合: *Data Protector_program_data*\OmniBack\Config\Server\amoschedules UNIXの場合: /var/opt/omni/server/amoschedules
統合スケジュール	Windowsの場合: *Data Protector_program_data*\OmniBack\Config\Server\Barschedules UNIXの場合: /var/opt/omni/server/Barschedules
コピー操作スケジュール	Windowsの場合: *Data Protector_program_data*\OmniBack\Config\Server\copylists\scheduled\schedules UNIXの場合: /var/opt/omni/server/copylists/scheduled/schedules
集約操作スケジュール	Windowsの場合: *Data Protector_program_data* \OmniBack\Config\Server\consolidationlists\scheduled\schedules UNIXの場合: /var/opt/omni/server/consolidationlists/scheduled/schedules
検証操作スケジュール	Windowsの場合: *Data Protector_program_data*\OmniBack\Config\Server\verificationlists\scheduled\schedules UNIXの場合: /var/opt/omni/server/verificationlists/scheduled/schedules
レポートグループスケジュール	Windowsの場合: *Data Protector_program_data*\OmniBack\Config\Server\rptschedules UNIXの場合: /var/opt/omni/server/rptschedules

アップグレードプロセスでスケジュールの移行に失敗した場合、既存のスケジュールを新しいスケジューラに正常に移行するために、以下のコマンドを手動で実行することができます。

```
omnidbutil -migrate_schedules
```

注:
- 以前のバージョンのData Protectorでは、追加されたスケジュールに名前属性はありませんでした。そのため、移行後のスケジュールの名前は...と表示されます。この部分を編集して、スケジュールに名前を付けることができます。

> - アップグレード時に、Data Protectorの旧バージョンで構成された分/時/年ごとのスケジュールは、Data Protector 10.00に移行されません。

スケジュール用オプション

仕様の種類に基づいて、以下のスケジュールオプションを設定できます。

- バックアップの種類: バックアップの種類([フル]または[増分])。
- ネットワーク負荷: セッションに適用するネットワーク負荷。このオプションを**[中]**または**[低]**に設定すると、Data Protectorの実行中にシステムにかかる負荷を低減できます。この場合、データ転送がほかのユーザーの操作を妨げることはなくなりますが、セッションが完了するまでに要する時間は長くなります。
- データ保護: バックアップしたデータを上書きから保護する期間。
- 繰り返しパターン: スケジュールを実行する頻度。
- 推定時間: セッションの推定時間。これにより、スケジュールがどのように予定ビューに表示されるのが決まります。

ディスク+テープへのZDBまたはディスクへのZDBの場合(インスタントリカバリが有効の場合)は、**[スプリットミラー/スナップショットのバックアップ]**オプションを指定できます。

各バックアップ仕様を異なるオプション値で複数回スケジュール設定することができます。1つのバックアップ仕様内で、ディスクへのZDBセッションとディスク+テープへのZDBセッションの両方をスケジュール設定すること、および個々のバックアップまたは定期的に実行するようにスケジュールしたバックアップにそれぞれ異なるデータ保護期間を指定することができます。

さらに、新しいスケジューラーには、以下の機能が含まれています。

休日中のスケジュールの除外

デフォルトのData Protectorサーバー構成ディレクトリにあるHolidaysファイルを編集することで、さまざまな休日を設定できます。

デフォルトでは、スケジュData Protectorール日時が休日の場合にもバックアップが実行されます。デフォルトの動作を変更する場合には、次の点を考慮して行ってください。1月1日が休日として登録されている場合、Data Protectorはその日にはバックアップを行いません。1月1日にフルバックアップの実施を予定し、1月2日に増分バックアップの実施を予定すると、Data Protectorは1月1日のフルバックアップは実行せず、1月2日に予定されている増分バックアップを実行します。増分バックアップでは、最後に行ったフルバックアップが使用されます。

`Holidays`ファイルを編集したり、このファイルに新しいエントリを追加したりする場合は、次の点に注意してください。

- 各行の最初の数値は日付の連番を表します。この値はData Protectorでは無視されますが、`0`と`366`の間に設定する必要があります。数値がその後の日付に対応しないことを示す場合は、`0`に設定します。
- 日付は、`Mmmd`と指定します。`Mmm`は3文字の月の省略形、`d`は日付の数値です(例: `Jan 1`)。ロケールに関係なく、月は英語で指定する必要があります。
- 休日の説明は必要に応じて入力します。現在、Data Protectorでは使用されません。

ファイルの先頭で指定した年に関係なく、ファイルで指定した休日が常にそのまま使用されます。毎年同じ日が休日にならない場合は、休日を手作業で編集する必要があります。スケジューラーの**[休日]**オ

プションを使用しない場合は、該当エントリを削除またはコメントアウトすると、古いHolidaysファイルや自分の国や会社のニーズに応じてカスタマイズされていないHolidaysファイルが誤って使用されて混乱するのを防ぐことができます。

定義済みスケジュールの使用

Data Protectorスケジューラーには、スケジュール構成を簡素化するのに役立つ一連の定義済みスケジュールが用意されています。これらのスケジュールは、後で修正することができます。

スケジュール重複の処理

定期バックアップのスケジュールを設定するときに、同じバックアップ仕様内で、選択したバックアップ開始時刻に他のバックアップがすでに設定されていることがあります。この場合、Data Protectorスケジュールウィザードは、スケジュール重複があることを示します。繰り返しパターンを再定義するか、スケジューラーが時間スロットの空いている日にスケジュールを設定できるようにします。時間スロットの可用性に基づいて、以下の値がスケジュールステータスとして設定されます。

- アクティブ: スケジュールは重複していないため、スケジュールされた時間に実行されます。
- 重複: スケジュールが重複していますが、選択された日付に使用可能な空き時間スロットがあり、スケジュールを実行できます。
- 休止: スケジュールが重複しており、選択された日付にスケジュールを実行できる使用可能な空き時間スロットがありません。
- 使用不可能: スケジュールはユーザーによって明示的に無効にされています。

異なるタイムゾーンでのスケジュール設定

Cell Managerシステムのタイムゾーン内のカレンダーに、すべてのスケジュールが表示されます。Cell Managerとは異なるタイムゾーンでバックアップまたはオブジェクト操作セッションを指定した場合、セッションは指定した時間とタイムゾーンで実行されます。

スケジュールの優先順位付け

スケジュールウィザードを使用して、各スケジュールの優先順位を設定できます。複数の実行中のセッションが同時に特定のデバイスへのアクセスを要求する場合、セッションが待ち行列に入る順序は優先順位によって決まります。各スケジュールの優先順位を設定できます。

- スケジュールされたセッションが、それよりも優先順位が低い他のセッションを一時停止できるように設定できます。

  > **注:**
  > スケジュールの優先順位と、[優先度の低いジョブを一時停止]オプションは、CMMDB環境ではサポートされません。

- ファイルシステム、VMware、およびOracle Server用統合ソフトウェアのセッションでは、セッションを一時停止して中止されたところから再開する機能を使用できます。その他の統合ソフトウェアでは、一時停止後、セッションは初めから再開されます。
- ディスクへのバックアップセッション(B2D)デバイスは、優先順位による一時停止の対象とはなりません。
- ファイルライブラリとB2Dのように、異なるバックアップデバイスタイプが混在しているバックアップセッション

の場合、一時停止機能はB2D以外のデバイスのみに適用されます。

- スケジューラーは、優先順位を管理するための内部ジョブキューを維持しています。複数のジョブがターゲットデバイスと同じファイルライブラリを共有している場合、スケジューラーは一度に1つのジョブだけを送り出し、先のジョブが完了しデバイスが解放されてからのみ次のジョブを送り出します。最も優先順位の高いジョブが最初に送り出されます。優先順位が同じジョブが複数ある場合は、スケジュール時間が最も早いジョブが最初に送り出されます。優先順位とスケジュール時間が同じジョブが複数ある場合は、1つのジョブがランダムに選択され、送り出されます。

スケジュール設定と優先順位の例

以下の例は、スケジューラーが優先順位と一時停止に基づいてバックアップセッションを処理する方法を示しています。

スケジュールが設定されているセッションが3つあるとします。

- Job1 は、優先順位が2000で**[優先度の低いジョブを一時停止]**オプションが有効になっています。
- Job2 は、優先順位が4000です。
- Job3 は、優先順位が3000で**[優先度の低いジョブを一時停止]**オプションが有効になっています。

1. Job2 が実行中です。
2. Job1とJob3を同じ時間に予定するとします。Job1セッションは、他のセッションを一時停止するオプションが有効になっています。したがって、Job2セッションはJob1のために一時停止します。
3. Job1セッションが完了すると、Job3セッションが実行されます。

   一時停止中のJob2セッションは、スケジュールと優先順位に従って実行可能になるまで停止されます。優先順位の高いセッションが他にもある場合、このセッションは実行されない可能性があります。

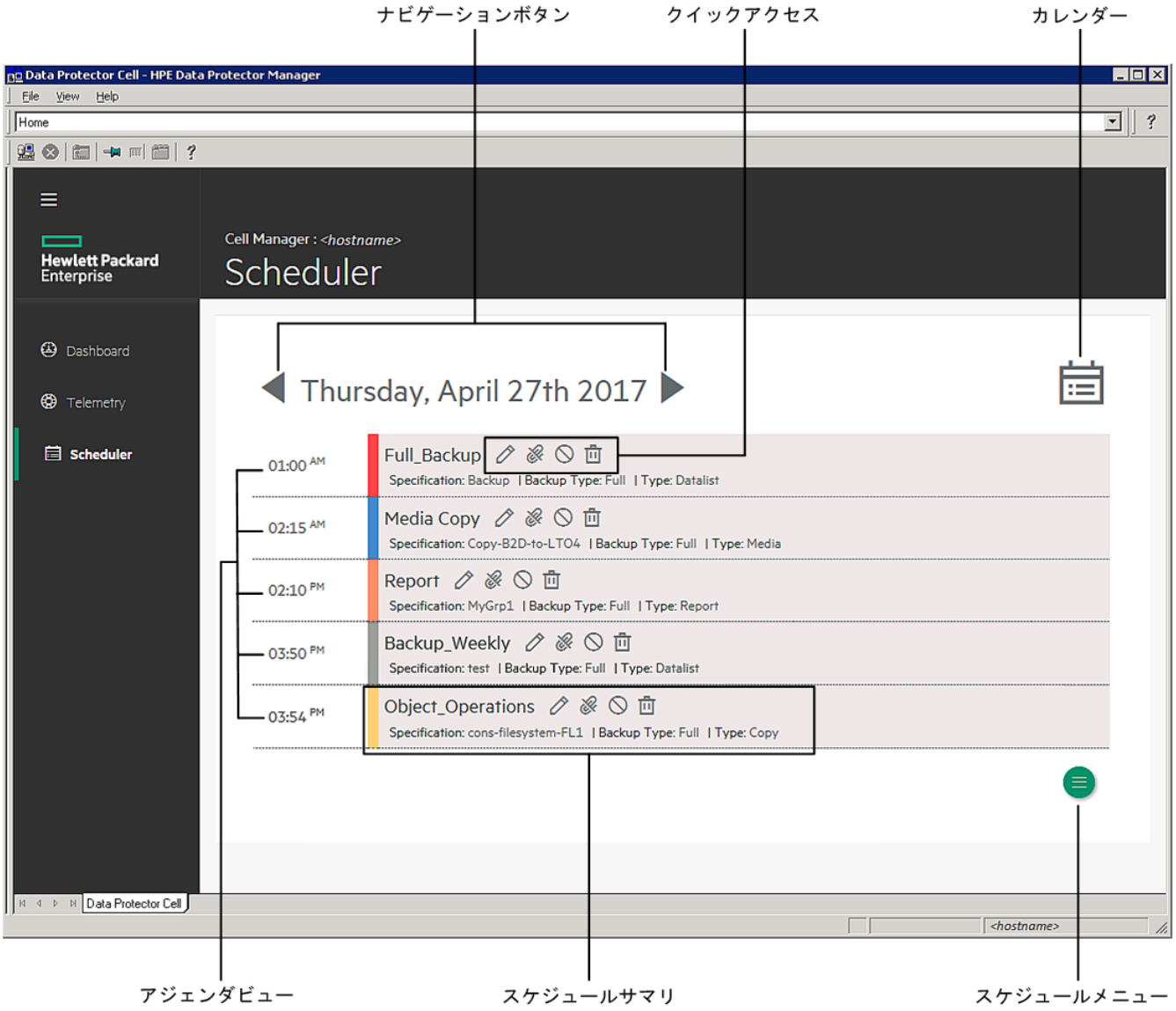
制限事項

Data Protectorスケジューラーには、以下の制限があります。

- ブラウザーの制限事項: [スケジューラ]ページを使用するには、コンピューターにMicrosoft Internet Explorer 11をインストールする必要があります。

スケジューラーのユーザーインターフェイス

以下の図は、スケジューラーのUIと、このページに表示されるさまざまなコントロールを示しています。



下の表は、すべてのコントロールについて説明しています。

コントロール	説明
ナビゲーションボタン	**[戻る]**および**[次へ]**ナビゲーションボタン。これらのボタンを使用すると、日付を戻したり進めたりして、選択した日付の予定を表示することができます。
クイックアクセス	スケジュールごとに使用可能な一連のアイコンで、よく使用するスケジューラーオプションへのショートカットが提供されます。 • 編集: スケジュールウィザードを開き、スケジュールで使用可能なすべて設定を変更できるようになります。

	• インスタンスの無効化: 選択した日付の現在のインスタンスを無効にします。これが繰り返しスケジュールの場合は、選択したインスタンスのみが無効になります。インスタンスを無効にすると、スケジュールは、該当する日の予定から削除されます。 • シリーズの無効化: スケジュールのすべてのインスタンスを無効にします。スケジュールを無効にすると、そのスケジュールは灰色で表示されます。スケジュールを無効にしても、現在実行中のスケジュールは影響を受けません。 • 削除: スケジュールを削除します。
カレンダー	カレンダーを表示します。カレンダーで日付を選択すると、該当する日の予定が表示されます。
予定ビュー	選択した日付のすべてのスケジュールのリスト(無効になっているスケジュールを含む)。
スケジュールのサマリー	スケジュールのサマリーを提供します。例えば、スケジュールが作成されている仕様名、実行するバックアップの種類(フル/増分)、およびスケジュールの種類を確認できます。各スケジュールの横の色分けは、**[種類]**を表しています。 • 赤は、スケジュールがバックアップ操作用に作成されていることを表します。 • 青は、スケジュールがメディア操作用に作成されていることを表します。 • オレンジは、スケジュールがレポート生成用に作成されていることを表します。 • 黄は、スケジュールがコピー操作用に作成されていることを表します。 • 灰色は、スケジュールが無効になっていることを表します。
スケジューラーメニュー	新しいスケジュールを作成するためのオプションを提供するスケジューラーメニュー。

スケジューラーのタスク

スケジューラーを使用して、以下のタスクを実行できます。

- スケジュールの作成
- 既存のスケジュールの編集
- スケジュールの表示
- スケジュールの有効/無効の切り替え
- 休日のスケジュールの有効/無効を切り替える
- 特定の日時のスケジュールの設定
- 定期的なスケジュールの設定

> **廃止:**
> 新しいWebベースのスケジューラーでは、スケジュールをリセットすることはできません。スケジュールのリセットオプションは、仕様に含まれている現在の年のすべてのスケジュール設定をクリアするために使用されていました。

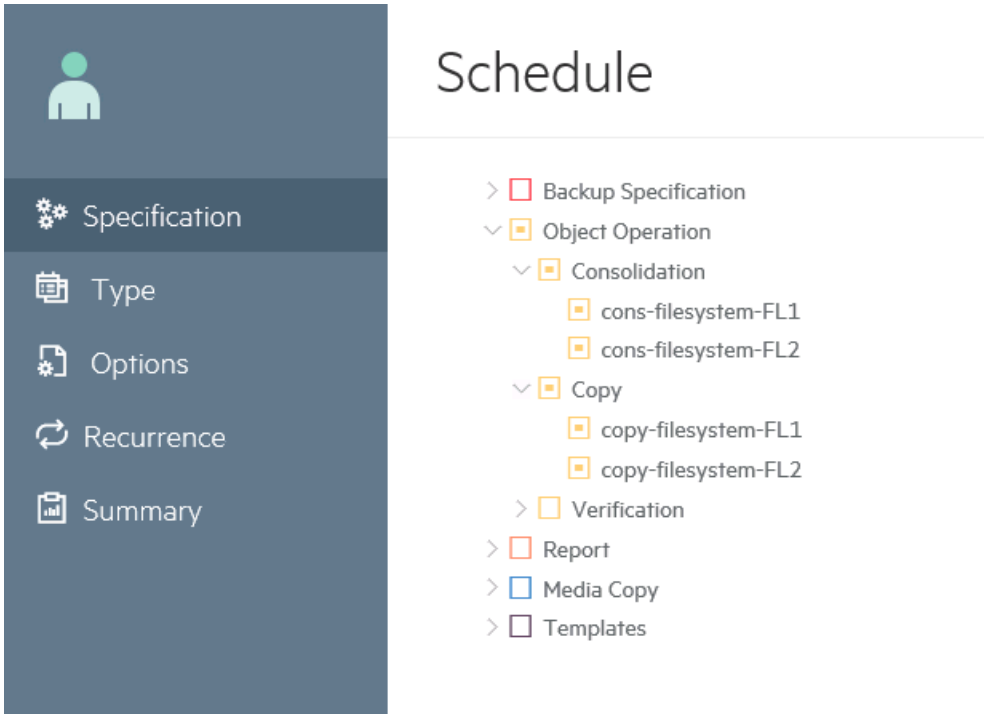
スケジュールの作成

スケジュールを作成するには、以下の手順を実行します。

以下の手順は、バックアップ仕様のスケジュールを作成する方法を示しています。スケジュールウィザードで使用できるオプションは、選択する仕様の種類によって異なります。

1. コンテキストメニューで**[ホーム]**をクリックして、左ペインの**[スケジューラー]**をクリックします。[スケジューラー]ページが開きます。
2. [スケジューラー]ページの右下隅にある[スケジューラーメニュー]アイコンをクリックし、[追加]アイコンをクリックしてスケジュールウィザードを開きます。[仕様]ページが開きます。
3. スケジュールを作成する仕様の種類を選択します。

   例えば、以下の図は、展開された[オブジェクト操作]ツリーを示しています。ここには、スケジュールを作成できる操作(集約、コピー、および検証)のリストが表示されています。



   既存のテンプレートにスケジュールを追加するには、**[テンプレート]**をクリックします。

   次に、このテンプレートを[バックアップ]コンテキストから仕様に適用できます。テンプレートの適用後、テンプレート内のすべてのスケジュールが仕様のためにアクティブになります。

   このウィザードを使用して、テンプレートのスケジュールを作成することはできません。

   [次へ]をクリックします。[種類]ページが開きます。

4. スケジュールの種類をクリックします。
   - **[カスタム]**をクリックして、独自のスケジュールを作成します。
   - **[定義済み]**をクリックして、Data Protectorで使用可能な定義済みスケジュールのいずれかを使用します。次のいずれかを選択します。
     - 毎日(集中的):Data Protectorは、毎日、深夜にフルバックアップを実行し、12:00(昼)と18:00(午後6時)に2つの追加の増分バックアップを実行します。
     - 毎日(フル):Data Protectorは、毎日21:00(午後9時)にフルバックアップを実行します。
     - 毎週(フル):Data Protectorは、毎週金曜日にフルバックアップを実行し、月曜日から金曜日の毎日21:00(午後9時)に増分1バックアップを実行します。
     - 隔週(フル):Data Protectorは、隔週の金曜日にフルバックアップを実行します。これらのバックアップの間に、Data Protectorは、毎週月曜日から木曜日の21:00(午後9時)に増分1バックアップを実行します。
     - 毎月(フル):Data Protectorは、毎月1日にフルバックアップを実行し、毎週増分1バックアップを実行し、1日おきに増分バックアップを実行します。

   [次へ]をクリックします。[オプション]ページが開きます。
5. **[スケジュール名]**テキストボックスにスケジュールの名前を入力します。
6. **バックアップ**の種類として、[フル]または[増分]を選択します。さまざまな種類のバックアップオプションの詳細については、バックアップの種類を参照してください。
7. **[保護レベル]**を選択します。保護レベルは、バックアップデータについての情報をIDB内に保持する期間を指定します。カタログ保護がない場合でもデータは復元できますが、その場合はデータをData ProtectorのGUIで表示することはできません。以下のいずれかのオプションを選択します。
   - [なし]:データを保護しません。
   - デフォルト:IDB内のバックアップデータが保護されている限り、データに関する情報が保護されます。
   - [期限]:指定した日付までIDB内の情報を上書き禁止にします。カタログ保護の期限は、指定した日付の正午に切れます。
   - [日数]:指定した日数が経過するまでIDB内の情報を上書き禁止にします。
   - [週数]:指定した週数が経過するまでIDB内の情報を上書き禁止にします。
   - 無期限:IDB内の情報は無期限に使用可能です。
8. スライダーを移動して優先順位を設定するか、優先順位の数値がスライダー値を超える場合は、**[優先順位]**テキストボックスに数値を入力します。優先順位レベルは、複数セッションが同時に1つのデバイスにアクセスを試みる場合に考慮されます。このような状況では、このオプションにより、セッションが待ち行列に登録される順番が決定します。

   優先順位が高いセッションが待ち行列に入れられる時に優先順位が低いセッションが実行中の場合、その実行中のセッションは完了されます。同じ優先順位の複数セッションが1つのデバイスへのアクセスを要求した場合、これらのセッションのいずれかが最初にアクセスを取得します。
9. **[ネットワーク負荷]**を指定します。このオプションを[中]または[低]に設定すると、Data Protectorの実行中にシステムにかかる負荷を低減できます。この場合、データ転送がほかのユーザーの操作を妨げることはなくなりますが、セッションが完了するまでに要する時間は長くなります。

10. スケジュールされたセッションが、ビジーデバイス上で他の優先順位が低いセッションを一時停止できるようにする場合は、**[優先度の低いジョブを一時停止]**オプションをオンにします。このオプションは、複数セッションが同時に1つのデバイスにアクセスを試みる場合に参照されます。この場合、このオプションは、選択したセッションが完了するまで他のセッションを一時停止できることを指定します。このセッションが完了した後に、一時停止されたセッションが完了します。

    > **注:**
    > この機能は、ファイルシステム、VMware、およびOracle Serverの統合セッションでのみ使用できます。ディスクへのバックアップセッション(B2D)デバイスは、優先順位による一時停止の対象とはなりません。ファイルライブラリとB2Dのように、異なるバックアップデバイスタイプが混在しているバックアップセッションの場合、一時停止機能はB2D以外のデバイスのみに適用されます。

11. デフォルトでは、スケジュールは有効になっています。スケジュールを無効にするには、**[スケジュールの有効化]**オプションをオフにします。
12. 操作を休日に実行する場合は、**[休日に実行]**オプションをオンにします。休日として指定する日を変更するには、Holidaysファイルを編集します。

    [次へ]をクリックします。[再帰]ページが開きます。
13. [繰り返しパターン]で、バックアップを実行する頻度を指定します。以下のオプションから、パターンと頻度を選択します。
    - **1回**:スケジュールは、特定の日に1回のみ実行されます。スケジュールを実行する開始日、タイムゾーン、および時刻を選択できます。
    - **日数単位**:スケジュールは、指定した時刻に定期的に実行されます。[<値>日ごと]フィールドを使用して、スケジュールの頻度を指定できます。例えば、4の繰り返し値を指定すると、スケジュールは4日ごとに実行されます。

      スケジュールを実行する開始日、タイムゾーン、および時刻を選択できます。
    - **週単位**:スケジュールは、毎週指定した日に定期的に実行されます。[<値>週ごと]フィールドを使用して、スケジュールの頻度を指定できます。例えば、2の繰り返し値を指定すると、スケジュールは2週ごとの選択した日に実行されます。

      スケジュールを実行する開始日、タイムゾーン、および時刻を選択できます。
    - **月単位**:スケジュールは、毎月指定した日に定期的に実行されます。[<値>月ごと]フィールドを使用して、スケジュールの頻度を指定できます。例えば、2の値を指定すると、スケジュールは2月ごとの選択した日に実行されます。

      スケジュールを実行する開始日、タイムゾーン、および時刻を選択できます。
14. 以下のいずれかのオプションから、**[繰り返し実行の終了時期]**を選択します。
    - 終了日なし:バックアップを無制限に繰り返す場合に選択します。
    - 終了日:特定の日にスケジュールを終了する場合に選択します。終了日は、開始日と同じタイムゾーン内に発生します。

    [1回]を選択した場合、**[繰り返し実行の終了時期]**オプションは使用できません。
15. **[推定時間]**を指定します。この値は、スケジュールが予定ビューに表示される順序を決定します。

    [次へ]をクリックします。[サマリー]ページが開きます。
16. すべてのスケジュールのオプションを確認します。スケジュールの競合がある場合、**[競合の検出]**オプ

ションが**[はい]**と表示され、以下のいずれかを実行するまで、スケジュール作成タスクを完了できません。

- スケジュールの繰り返しパターンを再定義する。[戻る]をクリックして、**[再帰]**ページに戻ります。
- **[空きスロットを埋める]**オプションをオンにする。このオプションは、選択した日付に空き時間スロットがある場合にのみ使用可能になります。空き時間スロットがない場合は、スケジュールの繰り返しパターンを再定義する必要があります。

[完了]をクリックしてスケジュールを作成します。

既存のスケジュールの編集

既存のスケジュールを編集するには、以下の手順を実行します。

> **注:**
> スケジュールの以下のいずれかのオプションを変更すると、スケジュールが削除され、新しいスケジュールが新しい値で作成されます。この新しいスケジュールはキューの末尾に移動され、時間スロットの可用性に基づいてステータスが適用されます。
>
> - 開始日
> - 終了日
> - タイムゾーン
> - 繰り返しパターン
> - 頻度の値
> - 推定時間
> - 休日

以下の手順は、バックアップ仕様のスケジュールを編集する方法を示しています。スケジュールウィザードで使用できるオプションは、選択する仕様の種類によって異なります。

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 該当するバックアップ仕様を右クリックして、**[スケジュールの編集]**をクリックします。[スケジューラー]ページが開きます。バックアップ仕様に使用可能なすべてのスケジュールが、右ペインにリストされています。
4. [スケジューラー]ページで、構成を変更するスケジュールの**[編集]**アイコンをクリックします。スケジュールウィザードの[オプション]ページが開きます。
5. **[スケジュール名]**テキストボックスで、スケジュールの名前を更新します。

   > **重要:**
   > 10.00より前のバージョンのData Protectorから移行されたスケジュールの場合、スケジュール名は...と表示されます。

6. **バックアップ**の種類として、[フル]または[増分]を選択します。さまざまな種類のバックアップオプションの詳細については、バックアップの種類を参照してください。
7. **[保護レベル]**を選択します。保護レベルは、バックアップデータについての情報をIDB内に保持する

期間を指定します。カタログ保護がない場合でもデータは復元できますが、その場合はデータをData ProtectorのGUIで表示することはできません。以下のいずれかのオプションを選択します。

- [なし]:データを保護しません。
- デフォルト:IDB内のバックアップデータが保護されている限り、データに関する情報が保護されます。
- [期限]:指定した日付までIDB内の情報を上書き禁止にします。カタログ保護の期限は、指定した日付の正午に切れます。
- [日数]:指定した日数が経過するまでIDB内の情報を上書き禁止にします。
- [週数]:指定した週数が経過するまでIDB内の情報を上書き禁止にします。
- 無期限:IDB内の情報は無期限に使用可能です。

8. スライダーを移動して優先順位を設定するか、優先順位の数値がスライダー値を超える場合は、**[優先順位]**テキストボックスに数値を入力します。優先順位レベルは、複数セッションが同時に1つのデバイスにアクセスを試みる場合に考慮されます。このような状況では、このオプションにより、セッションが待ち行列に登録される順番が決定します。

   優先順位が高いセッションが待ち行列に入れられる時に優先順位が低いセッションが実行中の場合、その実行中のセッションは完了されます。同じ優先順位の複数セッションが1つのデバイスへのアクセスを要求した場合、これらのセッションのいずれかが最初にアクセスを取得します。
9. **[ネットワーク負荷]**を指定します。このオプションを[中]または[低]に設定すると、Data Protectorの実行中にシステムにかかる負荷を低減できます。この場合、データ転送がほかのユーザーの操作を妨げることはなくなりますが、セッションが完了するまでに要する時間は長くなります。
10. スケジュールされたセッションが、ビジーデバイス上で他の優先順位が低いセッションを一時停止できるようにする場合は、**[優先度の低いジョブを一時停止]**オプションをオンにします。このオプションは、複数セッションが同時に1つのデバイスにアクセスを試みる場合に参照されます。この場合、このオプションは、選択したセッションが完了するまで他のセッションを一時停止できることを指定します。このセッションが完了した後に、一時停止されたセッションが完了します。

    > **注:**
    > この機能は、ファイルシステム、VMware、およびOracle Server用統合ソフトウェアのセッションに使用できます。ディスクへのバックアップセッション(B2D)デバイスは、優先順位による一時停止の対象とはなりません。ファイルライブラリとB2Dのように、異なるバックアップデバイスタイプが混在しているバックアップセッションの場合、一時停止機能はB2D以外のデバイスのみに適用されます。

11. デフォルトでは、スケジュールはオンになっています。スケジュールを無効にするには、**[スケジュールの有効化]**オプションをオフにします。
12. 操作を休日に実行する場合は、**[休日に実行]**オプションをオンにします。デフォルトでは、Data Protectorは、休日の場合にもスケジュールされた操作を実行します。休日として指定する日を変更するには、Holidaysファイルを編集します。

    [次へ]をクリックします。[再帰]ページが開きます。
13. [繰り返しパターン]で、バックアップを実行する頻度を指定します。以下のオプションから、パターンと頻度を選択します。

- **1回**:スケジュールは、特定の日に1回のみ実行されます。スケジュールを実行する開始日、タイムゾーン、および時刻を選択できます。

- **日数単位**:スケジュールは、指定した時刻に定期的に実行されます。[<値>日ごと]フィールドを使用して、スケジュールの頻度を指定できます。例えば、4の繰り返し値を指定すると、スケジュールは4日ごとに実行されます。

  スケジュールを実行する開始日、タイムゾーン、および時刻を選択できます。

- **週単位**:スケジュールは、毎週指定した日に定期的に実行されます。[<値>週ごと]フィールドを使用して、スケジュールの頻度を指定できます。例えば、2の繰り返し値を指定すると、スケジュールは2週ごとの選択した日に実行されます。

  スケジュールを実行する開始日、タイムゾーン、および時刻を選択できます。

- **月単位**:スケジュールは、毎月指定した日に定期的に実行されます。[<値>月ごと]フィールドを使用して、スケジュールの頻度を指定できます。例えば、2の値を指定すると、スケジュールは2月ごとの選択した日に実行されます。

  スケジュールを実行する開始日、タイムゾーン、および時刻を選択できます。

14. 以下のいずれかのオプションから、**[繰り返し実行の終了時期]**を選択します。
    - 終了日なし:バックアップを無制限に繰り返す場合に選択します。
    - 終了日:特定の日にスケジュールを終了する場合に選択します。終了日は、開始日と同じタイムゾーン内に発生します。

    [1回]を選択した場合、**[繰り返し実行の終了時期]**オプションは使用できません。
15. **[推定時間]**を指定します。この値は、スケジュールが予定ビューに表示される順序を決定します。

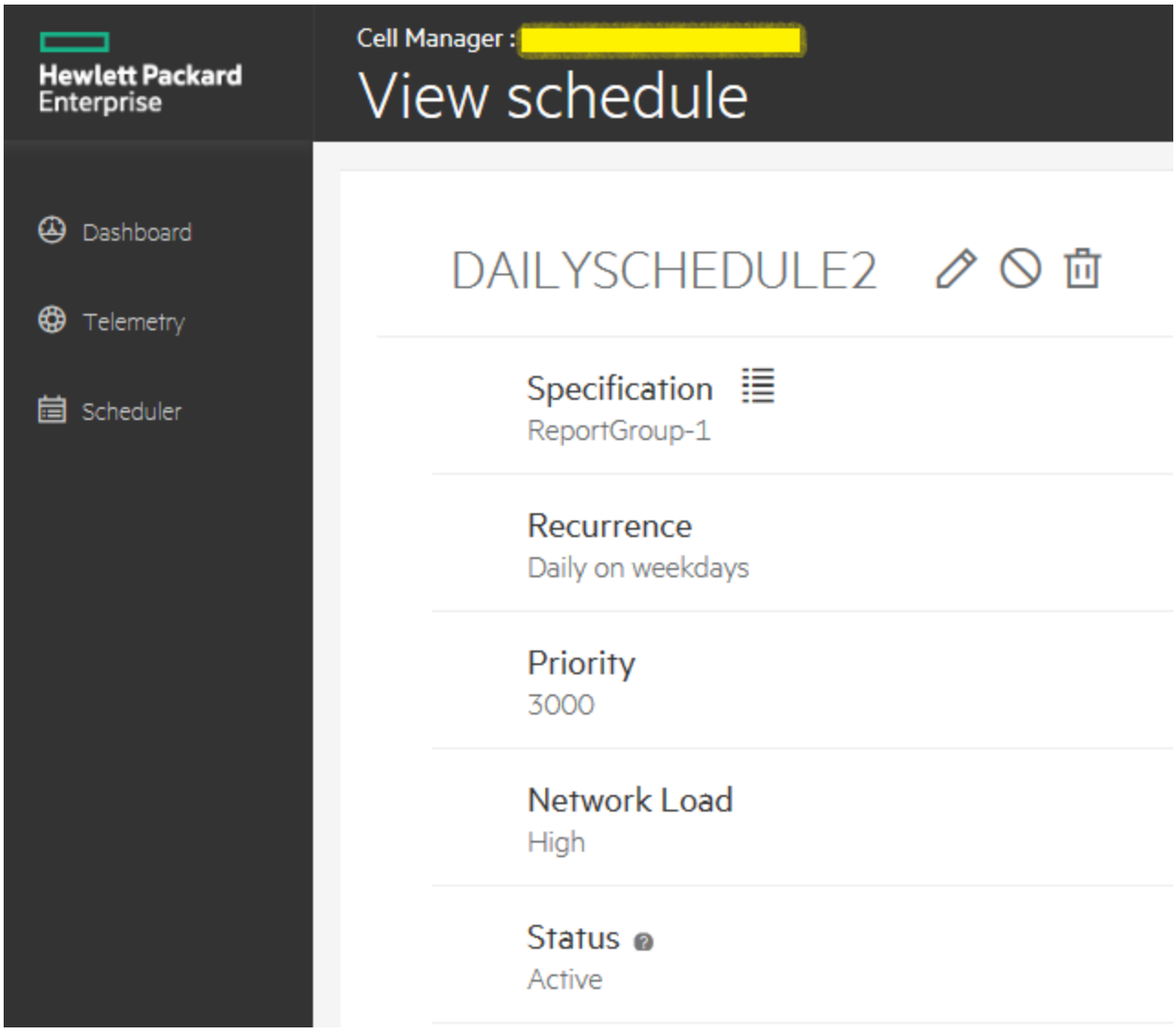
    [次へ]をクリックします。[サマリー]ページが開きます。
16. すべてのスケジュールのオプションを確認します。スケジュールの競合がある場合、**[競合の検出]**オプションが**[はい]**と表示され、以下のいずれかを実行するまで、スケジュール作成タスクを完了できません。
    - スケジュールの繰り返しパターンを再定義する。[戻る]をクリックして、**[再帰]**ページに戻ります。
    - **[空きスロットを埋める]**オプションをオンにする。このオプションは、選択した日付に空き時間スロットがある場合にのみ使用可能になります。空き時間スロットがない場合は、スケジュールの繰り返しパターンを再定義する必要があります。

    [完了]をクリックしてスケジュールを保存します。

スケジュールの表示

特定のスケジュールの詳細を表示するには、予定ビューでスケジュール名をクリックします。

該当する仕様のすべてのスケジュールを表示するには、[スケジュールの表示]ページの☰アイコンをクリックします。該当する仕様のすべてのスケジュールが、右ペインに表示されます。



[スケジュールの表示]ページには、スケジュールに関する以下の詳細が表示されます。

- 仕様: スケジュールが作成されている仕様の種類。
- 繰り返し: スケジュールに設定されている繰り返しパターン。
- 優先順位: スケジュールが実行される順序を決定するスケジュール優先順位。
- ネットワーク負荷: Data Protectorの実行時のネットワークの負荷に設定されている現在の値。
- ステータス: ステータスパラメーターは、時間スロット可用性に基づいて、以下の値を示します。
  - アクティブ: スケジュールは重複していないため、スケジュールされた時間に実行されます。
  - 重複: スケジュールが重複していますが、選択された日付に使用可能な空き時間スロットがあり、スケジュールを実行できます。
  - 休止: スケジュールが重複しており、選択された日付にスケジュールを実行できる使用可能な空き

時間スロットがありません。

- 使用不可能: スケジュールはユーザーによって明示的に無効にされています。

スケジュールの有効/無効の切り替え

デフォルトでは、スケジュールは追加したときには有効になっていますが、無効にして、後で使用するためにスケジュール設定を保持しておくことができます。

バックアップスケジュールを無効化しても、現在実行中のバックアップセッションは影響されません。

以下の手順は、バックアップ仕様のスケジュールを有効および無効にする方法を示しています。スケジュールウィザードで使用できるオプションは、選択する仕様の種類によって異なります。

手順

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]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 該当するバックアップ仕様を右クリックし、**[スケジュールの編集]**をクリックします。[スケジュールの表示]ページが開きます。バックアップ仕様に使用可能なすべてのスケジュールが、右ペインに表示されます。
4. 編集するスケジュールをクリックして、[スケジュールの表示]ページの**[編集]**スケジュールアイコンをクリックします。スケジュールウィザードが開きます。
5. [オプション]ページで、**[スケジュールの有効化]**スライダーを**オフ**にして、スケジュールを使用不可にしてから、**[次へ]**をクリックします。スケジュールを有効にするには、スライダーを**オン**にします。[再帰]ページが開きます。
6. 繰り返しパターンを確認して、**[次へ]**をクリックします。[サマリー]ページが開きます。
7. スケジュールのオプションを確認して、**[完了]**をクリックします。

休日のスケジュールの有効/無効の切り替え

デフォルトで、Data Protectorはスケジュールを休日に実行します。**[休日]**オプションをオンにすると、この動作を変更できます。このオプションをオフにしない限り、休日のバックアップは実行されません。

以下の手順は、休日のバックアップ仕様のスケジュールを有効および無効にする方法を示しています。スケジュールウィザードで使用できるオプションは、選択する仕様の種類によって異なります。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 休日のバックアップスケジュールの有効/無効を切り替えるバックアップ仕様を右クリックし、**[スケジュールの編集]**をクリックします。[スケジューラー]ページが開きます。バックアップ仕様に使用可能なすべてのスケジュールが、右ペインに表示されます。

4. 編集するスケジュールをクリックして、[スケジュールの表示]ページの**[編集]**スケジュールアイコンをクリックします。スケジュールウィザードが開きます。
5. [オプション]ページで**[休日に実行]**スライダーを**オフ**にして、休日に操作が実行されないようにします。休日に操作を実行する場合は、スライダーを**オン**にします。
6. **[次へ]**をクリックします。[再帰]ページが開きます。
7. 繰り返しパターンを確認して、**[次へ]**をクリックします。[サマリー]ページが開きます。
8. スケジュールのオプションを確認して、**[完了]**をクリックします。

特定の日時のスケジュールの設定

セッションは、特定の日時に自動的に開始するように設定できます。

以下の手順は、バックアップ仕様のスケジュールを特定の日時に設定する方法を示しています。スケジュールウィザードで使用できるオプションは、選択する仕様の種類によって異なります。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 該当するバックアップ仕様を右クリックして、**[スケジュールの編集]**をクリックします。[スケジュール]ページが開きます。バックアップ仕様に使用可能なすべてのスケジュールが、右ペインにリストされています。
4. 編集するスケジュールをクリックして、**[編集]**スケジュールアイコンをクリックします。スケジュールウィザードが開きます。
5. [オプション]ページで設定を確認し、**[次へ]**をクリックします。[再帰]ページが開きます。
6. [繰り返しパターン]で**[1回]**を選択し、バックアップを開始する開始日、タイムゾーン、および時刻を指定します。バックアップ期間を指定して、**[次へ]**をクリックすることもできます。
7. [サマリー]ページでスケジュールオプションを確認し、**[完了]**をクリックします。

既存のスケジュールバックアップに既に割り当てられている時間枠に新しいバックアップをスケジュール設定すると、新しいスケジュールバックアップが古いスケジュールバックアップより優先して適用されます。

定期的なスケジュールの設定

周期スケジュールは、一定の期間で実行されるスケジュールです。たとえば、日曜日の午前3時にフルバックアップを行い、2日ごとに繰り返すように構成するとします。この場合、次回のフルバックアップは、翌火曜日の午前3時に行われることになります。周期バックアップにより、定期的なバックアップの構成が簡略化されます。

周期バックアップを設定するには、新しい仕様の種類の作成時にウィザードの指示に従うか、以下の手順で説明されているように、既存の仕様のスケジュールを修正します。

この手順は、バックアップ仕様の定期的なスケジュールを設定する方法を示しています。スケジュールウィザードで使用できるオプションは、選択する仕様の種類によって異なります。

定義済みのバックアップスケジュールを使用する

定義済みのバックアップスケジュールを使うと、ファイルシステムバックアップ仕様の構成作業が簡単になります。これらのスケジュールは、後から修正できます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで**[バックアップ仕様]**と**[ファイルシステム]**を順に展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 該当するバックアップ仕様を右クリックし、**[スケジュールの編集]**をクリックします。スケジュールウィザードが開きます。
4. [種類]ページで、**[定義済み]**を選択してから、定義済みスケジュールのリストから適切なスケジュールを選択します。次のいずれかを選択します。
   - 毎日(集中的): Data Protectorは、毎日、深夜にフルバックアップを実行し、12:00 (昼)と18:00 (午後6時)に2つの追加の増分バックアップを実行します。
   - 毎日(フル): Data Protectorは、毎日21:00 (午後9時)にフルバックアップを実行します。
   - 毎週(フル): Data Protectorは、毎週金曜日にフルバックアップを実行し、月曜日から金曜日の毎日21:00 (午後9時)に増分1バックアップを実行します。
   - 隔週(フル): Data Protectorは、隔週の金曜日にフルバックアップを実行します。これらのバックアップの間に、Data Protectorは、毎週月曜日から木曜日の21:00 (午後9時)に増分1バックアップを実行します。
   - 毎月(フル): Data Protectorは、毎月1日にフルバックアップを実行し、毎週増分1バックアップを実行し、1日おきに増分バックアップを実行します。

   [次へ]をクリックします。[オプション]ページが開きます。
5. [オプション]ページでオプションを指定し、**[次へ]**をクリックします。[再帰]ページが開きます。
6. [再帰]ページでオプションを指定し、**[次へ]**をクリックします。[サマリー]ページが開きます。
7. スケジュールのオプションを確認して、**[完了]**をクリックします。

繰り返しスケジュールの構成

特定の日付と時刻に開始し、定義されたパターンに従って繰り返すスケジュールを作成できます。たとえば、今後6か月の間、毎金曜日の21:00にフルバックアップを実施するスケジュールを作成できます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 該当するバックアップ仕様を右クリックし、**[スケジュールの編集]**をクリックします。スケジュールウィザー

ドが開きます。

4. [種類]ページで、**[カスタム]**を選択し、**[次へ]**をクリックします。[オプション]ページが開きます。
5. [スケジュール名]テキストボックスに、新しいスケジュールの名前を入力します。バックアップの種類([フル]または[増分]。他のバックアップの種類は個々の統合によって異なる)、バックアップ保護, 優先順位、およびネットワーク負荷を選択します。**[次へ]**をクリックします。[再帰]ページが開きます。
6. [繰り返しパターン]で、以下のオプションからパターンと頻度を選択します。
   - **日数単位**: スケジュールは、指定した時刻に定期的に実行されます。[<値>日ごと]フィールドを使用して、スケジュールの頻度を指定できます。例えば、4の繰り返し値を指定すると、スケジュールは4日ごとに実行されます。
   - **週単位**: スケジュールは、毎週指定した日に定期的に実行されます。[<値>週ごと]フィールドを使用して、スケジュールの頻度を指定できます。例えば、2の繰り返し値を指定すると、スケジュールは2週ごとの選択した日に実行されます。
   - **月単位**: スケジュールは、毎月指定した日に定期的に実行されます。[<値>月ごと]フィールドを使用して、スケジュールの頻度を指定できます。例えば、2の値を指定すると、スケジュールは2月ごとの選択した日に実行されます。
7. 以下のオプションから繰り返しの範囲を指定し、**[次へ]**をクリックします。
   - 開始: スケジュールの最初の日付。スケジュールを開始する日付、タイムゾーン、および時刻を指定します。
   - 繰り返し実行の終了時期: 最後のスケジュールを実行する日付。スケジュールを無制限に実行する場合は、**[終了日なし]**を選択します。

   > **注:**
   > 開始日を設定せずに繰り返しを2以上(たとえば、2週間おきの土曜日)に設定した場合、Data Protectorのスケジュール設定アルゴリズムにより、最初のバックアップは、選択条件に一致する最初の日付(この場合は、第2土曜日)にスケジュールが設定されます。

8. [サマリー]ページでスケジュールオプションを確認し、**[完了]**をクリックします。
9. ディスク+テープへのZDBまたはディスクへのZDB(インスタントリカバリが有効)の場合は、[スプリットミラー/スナップショットのバックアップ]オプションを指定します。

   [OK]をクリックします。

スケジュールの設定が競合する場合は、スケジュールを修正するように促すメッセージが表示されます。

スケジュール設定のヒント

スケジュールの作成時に、以下のヒントを役立てることができます。

- スケジュールが開始されると、Data Protectorは、ライセンス、デバイス、IDBへのアクセスなど、必要なすべてのリソースの割り当てを試行します。必要なリソースのいずれかが利用不能の場合、そのセッションは待ち行列に入れられ、タイムアウトになるまで1分おきに待機状態のセッションに必要なリソースの取得がData Protector試行されます。タイムアウトは、`SmWaitForDevice`グローバルオプションを修正することにより変更できます。

  必要なリソData Protectorースがすべて取得されると、待機中のセッションが開始されます。待機中のセッションは、表示されている順に開始されるとは限りません。

- Cell Managerに負荷がかかりすぎないようにするため、セル内で同時に処理されるセッションの数がデフォルトで制限されています。有効なセッション数を超える数のセッションが同時にスケジュールされている場合で、有効なセッション数が構成可能な最大セッション数を下回っている場合は、オーバーフローセッションが待ち行列に格納されます。この制限は、`MaxBSessions`グローバルオプションを使用して変更できます。

  また、構成可能な最大セッション数を超えるセッションが同時に呼び出された場合、それらのセッションは開始されず、対応するエラーがData Protectorイベントログに記録されます。
- スケジュール設定を簡略化するため、Data Protectorではグループクライアント用のバックアップ仕様を利用できます。1つのバックアップ仕様で構成されたクライアントはすべて、1つのバックアップセッション内で同時にバックアップされます。
- 無人バックアップが問題なく実施されるだけの十分な量のメディアとデバイスがあることを確認してください。
- バックアップテンプレートを適用すると、テンプレートのスケジュール設定がバックアップ仕様のスケジュール設定に代わって適用されます。テンプレートを適用した後でも、バックアップ仕様を変更し、別のスケジュールを設定することができます。
- スケジューラーの設定単位は、繰り返しパターンで設定し、1分以上に設定します。
- バックアップセッションとコピーセッションが開始されると、特にMedia Agentサーバー上では、大量のリソースを消費するため、これらのセッションにメモリを割り当てる必要があります。したがって、複数のバックアップセッションおよびコピーセッションが同時に開始しないようにする必要があります。例えば、午後6時頃に9つバックアップ仕様を開始する必要がある場合、最初の3つのバックアップを午後5:45に開始し、次の3つを午後6時、最後の3つのバックアップを午後6:15に開始する必要があります。9つのすべてのバックアップ仕様を午後6時にスケジュールすることは避けてください。

第8章: デバイス

バックアップデバイスについて

Data Protectorでは、物理デバイスの定義とモデル化にData Protector使用プロパティを使用します。複数のData Protectorデバイス定義から同じ物理デバイスを参照できます。このデバイスコンセプトを使用することで、デバイスを簡単かつ柔軟に構成し、バックアップ仕様で使用することができます。

バックアップデバイスとは

バックアップデバイスとは、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です。たとえば、スタンドアロンDDS/DATドライブやライブラリをバックアップデバイスとして使用できます。

Data Protectorでサポートしているデバイスのリストについては、HPE Data Protector Device Support Matrixを参照してください。サポートされていないデバイスは、`scsitab`ファイルを使用して構成できます。

テープドライブなど、バックアップデバイスの中には特定のData Protectorライセンスに依存しているものがあります。詳細については、『*HPE Data Protectorインストールガイド*』を参照してください。

バックアップデバイスの構成について

準備作業を完了したら、Data Protectorで使用するバックアップデバイスを構成することができます。

バックアップデバイスの構成には、Data Protectorの自動構成機能を使用することをお勧めします。Data Protectorでは、代表的なバックアップデバイスやライブラリのほとんどを自動的に構成することができます。バックアップセッションに合わせてメディアを準備する必要はありますが、Data Protectorによって、ポリシー、メディアの種類、メディアポリシー、デバイスファイルまたはデバイスのSCSIアドレスが決定され、ドライブとスロットも構成されます。

バックアップデバイスは手動で構成することもできます。バックアップデバイスの構成方法は、デバイスの種類によって異なります。

『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』にサポート対象と記述されていないデバイスも、使用できます。サポートされていないデバイスは、`scsitab`ファイルを使用して構成します。

> **注:** 外部制御は、Data Protectorが認識するすべてのライブラリをサポートするためのものです。Data Protectorでサポートされていないデバイスに対してユーザー定義のスクリプトまたはプログラムを作成し、特定のスロットから指定したドライブにメディアをロードするときにロボティクス制御を実行することができます。特別なスクリプトを作成すれば、そのスクリプトを参照する外部制御としてライブラリを構成することができます。

バックアップデバイスの種類

Data Protectorでは、構成可能なデバイスの種類として、以下のものをサポートしています。実際に構成可能なデバイスの種類は、インストールしたコンポーネントによって異なります。

- スタンドアロン
- ディスクへのバックアップデバイス
- SCSIライブラリ
- スタッカー
- マガジンデバイス
- ジュークボックス
- スタンドアロンファイルデバイス
- ファイルライブラリデバイス
- 外部制御
- ADIC/GRAU DASライブラリ
- StorageTek ACSライブラリ

スタンドアロン

スタンドアロンデバイスは、一度に1つのメディアに対する読み取り/書き込みを行うドライブを持つ、DDSやDLTのようなシンプルなデバイスです。スタンドアロンデバイスは、小規模なバックアップに使用します。メディアが一杯になった場合、オペレーターはバックアップを継続するためにメディアをすぐに新しいものに手動で交換する必要があります。このため、スタンドアロンデバイスは大規模な無人バックアップには適していません。

ディスクへのバックアップデバイス

ディスクへのバックアップ(B2D)デバイスはディスクベースのストレージデバイスで、Data Protectorジュークボックスやファイルライブラリデバイスと比較して、複数のホストを介したアクセス(ゲートウェイ)や、(デバイスの種類によっては)重複排除などの追加機能を利用することができます。

SCSIライブラリ

SCSIライブラリデバイスは大容量のバックアップデバイスで、オートローダとも呼ばれています。レポジトリ内には多数のメディアカートリッジがあり、複数のメディアを同時に処理できるよう複数のドライブを持っているデバイスもあります。ほとんどのライブラリデバイスでは、ドライブが汚れたときに自動的にクリーニングする機能を使用できます。

通常のライブラリデバイスでは、デバイス内の各ドライブに対して、およびライブラリロボティクスメカニズムに対して、SCSI ID (Windowsシステム)またはデバイスファイル(UNIXシステム)が1つ割り当てられます。ロボティクスメカニズムは、スロットとドライブの間でメディアを移動させ、再度戻します (たとえば、4つのドライブ

を含むライブラリにはドライブに4つ、ロボティクスメカニズムに1つ、合計5つのSCSI IDが割り当てられます)。

メディアは、デバイスのレポジトリ内のスロットに格納されます。各スロットには、Data Protectorによって1から順に番号が割り当てられます。ライブラリを管理する際は、スロット番号で指定します。

ドライブインデックスは、ライブラリ内のドライブの機械的な位置を示します。ロボティック制御では、このインデックス番号が重要な意味を持ちます。ライブラリロボティクスでは、対応するドライブインデックス番号だけが認識され、ドライブのSCSIアドレスに関する情報は維持されません。ドライブインデックスは、1から始まる整数の連番をドライブのSCSIアドレスと組み合わせたものです。多くのSCSIライブラリのWebインターフェイス、コマンドビューTL、またはSCSIライブラリのコントロールパネルでは、ドライブに0から始まる番号が付けられます。Data Protectorのデバイス構成ではドライブ「0」は有効ではありません。最初のドライブは常に「1」になっている必要があります。

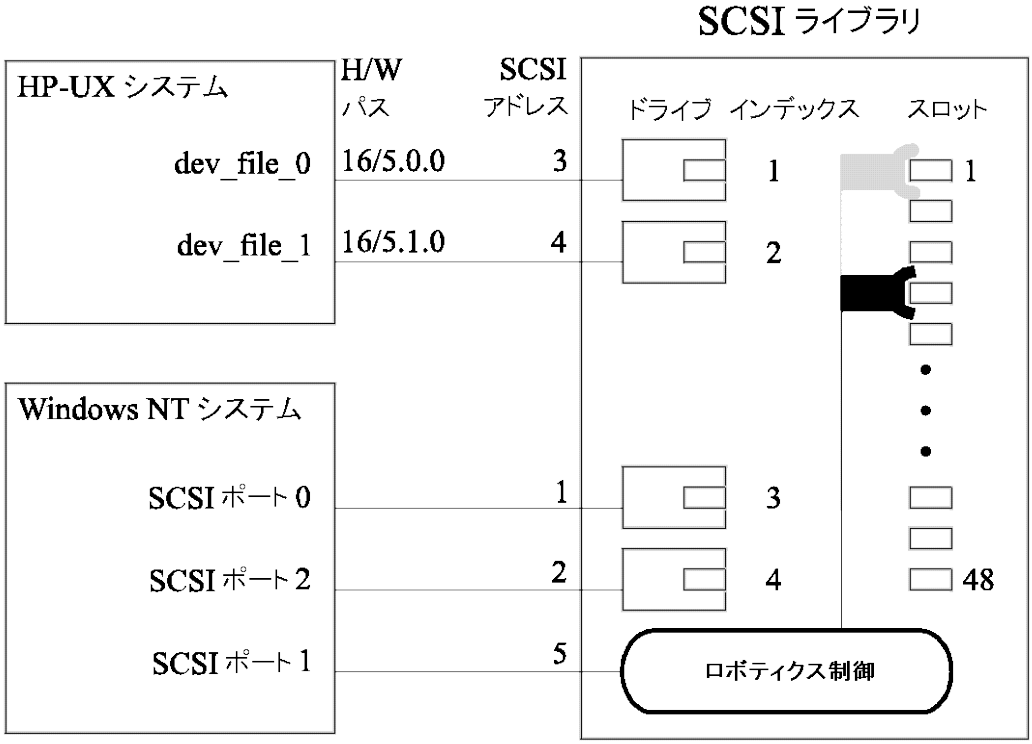
たとえば、4つのドライブを持つライブラリの場合なら、1～4のドライブインデックスがあります。ライブラリ内にドライブが1つしかなければ、ドライブインデックスは1となります。

ドライブインデックスは、SCSIアドレスと一対一で対応させる必要があります。つまり、次のようなペアを構成する必要があります。

インデックス1に対応するSCSI address_A、インデックス2に対応するSCSI address_Bなど

マガジンデバイスの構成時にも、この種類のデバイスを指定します。

ドライブインデックスのSCSIアドレスへのマッピング



スタッカー

スタッカーは、ドライブを常時1つずつ使用する単一のデバイスです。スタッカーのよるメディアのロード順はランダムではなく順番なので、メディア割り当てポリシーとしては[緩和]をお勧めします。スタッカーは、"スタック"(レポジトリ)からメディアを取り出してドライブに挿入します。この交換動作では必ず、ドライブ内にすでに挿入されているメディアを取り出してから、スタックの次のメディアを挿入します。最初のメディアは手動でロードする必要がありますが、それ以外のメディアは自動的にロードされます。テープが一杯になると、現在のテープが取り出され、次のテープが自動的にロードされます。スタッカーマガジン内のすべてのテープが使用されたら、手動でマガジンを取り外し、次のマガジンを挿入する必要があります。このときも、最初のテープは、ドライブに手動でロードしなければなりません。

バックアップまたは復元セッションは、メディアがなくてもマウント要求が発行された場合は中止されません。タイムアウトに達する前にスタッカーマガジンを交換しなければ、その時点でセッション全体が中止されます。

マガジンデバイス

マガジンデバイスでは、複数のメディアをマガジンという1つの単位にまとめて扱います。マガジンを使用すると、多数のメディアを個別に扱うよりも簡単に大量のデータを処理することができます。マガジン内の各メディアに対する操作は、Data Protectorによって完全に制御されます。HPE XP DAT 24x6は、マガジンデバイスとして構成できます。

ジュークボックス

ジュークボックスは、ライブラリデバイスです。ジュークボックスには、光磁気メディアまたはファイルメディアを格納できます。デバイスがファイルメディアの格納に使用された場合、その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。ファイルジュークボックスデバイスに格納するメディアの種類は、初期構成時に定義します。

UNIX上でジュークボックス光磁気ライブラリを実行している場合は、エクスチェンジャースロットまたはプラッタのサイドごとに構成されたUNIXデバイスファイルが必要です。

スタンドアロンファイルデバイス

スタンドアロンファイルデバイスは特定のディレクトリに存在するファイルで、テープにデータを書き込む代わりに、このファイルにデータをバックアップすることができます。

ファイルライブラリデバイス

テープにデータを書き込む代わりに、データをディレクトリにバックアップすることができますが、このディレクトリのセットをファイルライブラリデバイスと呼びます。

外部制御

外部制御は、Data Protectorが認識するすべてのライブラリをサポートするためのものです。Data Protectorでサポートされていないデバイスに対してユーザー定義のスクリプトまたはプログラムを作成し、特定のスロットから指定したドライブにメディアをロードするときにロボティクス制御を実行することができます。特別なスクリプトを作成すれば、そのスクリプトを参照する外部制御としてライブラリを構成することができます。

ADIC/GRAU DASライブラリ

ADIC/GRAU DASライブラリは、複数の種類のバックアップドライブを装着できる非常に大規模な制御ライブラリ(サイロ)です。バックアップデータの量が非常に多く、データの格納に大量のメディアが必要となる複雑な環境で使用されます。数百～数千のテープを処理できます。一般に、ADIC/GRAU DASライブラリには、多くの種類のバックアップドライブと数千のメディアスロットを格納できます。これらのドライブおよびメディアスロットは、内部のロボティックメカニズムによって処理され、特別なライブラリ制御ユニットによって管理されます。Data Protectorと他のアプリケーションでライブラリを共有できるように、ライブラリ内のメディアの一部を共有専用としてアプリケーションに割り当てることができます。

Data Protectorのユーザーインターフェイスからすべてのメディア処理を実行することができます。認識可能な形式のメディアの場合は、`tar`などのようにメディアの種類に従ってそData Protectorの形式が表示されます。認識不可能な形式のメディアの場合は、`foreign`とみなされます。

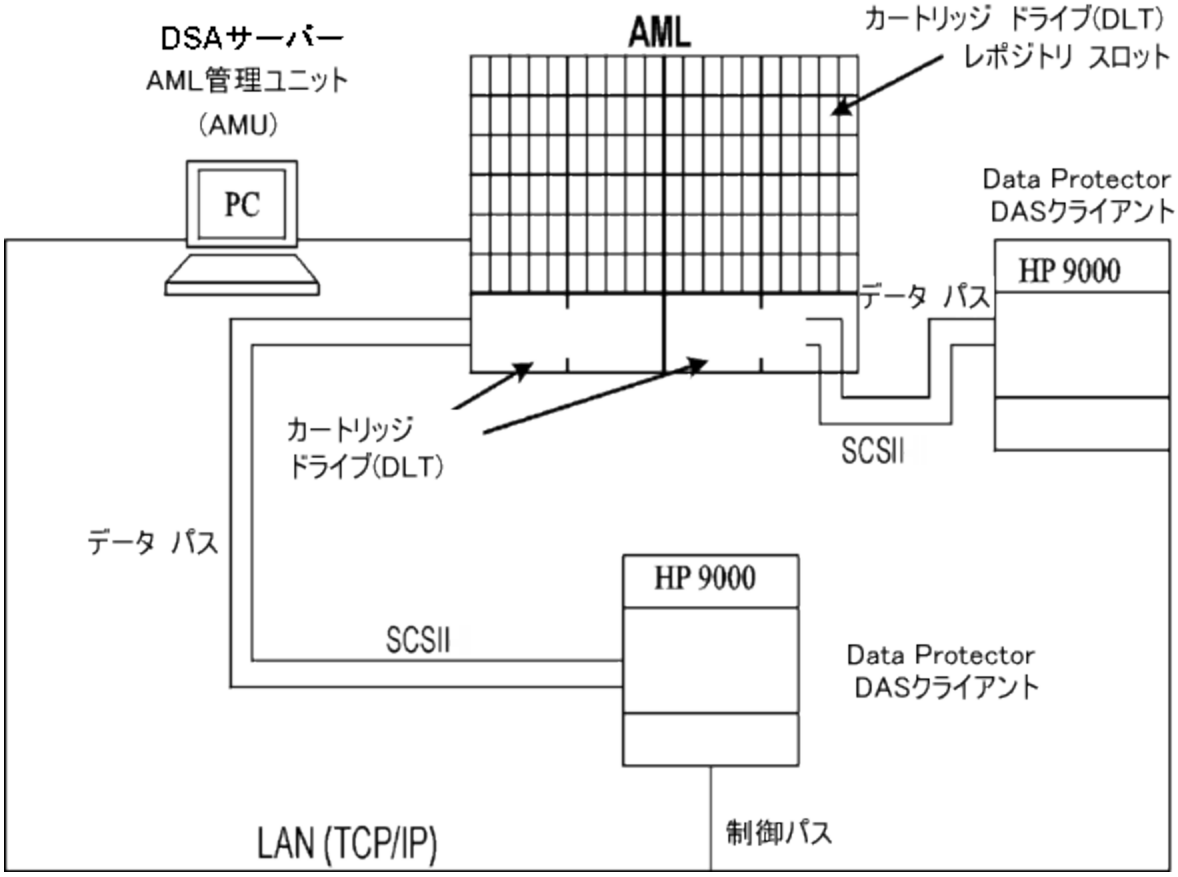
メディア管理データベースは、Data Protectorのメディアとそれ以外のメディアのすべてを、常駐(デバイスのレポジトリ内のData Protectorメディア)か非常駐(デバイスのレポジトリ外のメディア)かに関係なく記録し、高度な上書き保護を実現しています。Data Protectorは認識可能な形式のデータを含むメディアは上書きしません。ただし、テープにあるData Protectorのデータが同じメディアを使用している別のアプリケーションによって上書きされないという保証はありません。Data Protectorに使用されるメディアを他のアプリケーションで使用しないことをお勧めします。また、その逆も同様です。

メディアの実際の格納場所は、DASサーバーによって維持されます。DASサーバーは、VOLSERを使用して位置を追跡します。レポジトリ内でメディアを移動すると、その都度、異なる物理スロットにメディアが割り当てられます。したがって、メディアの取り扱い時には、スロット番号ではなく、バーコード(VOLSER)を基準として使用してください。

ADIC/GRAU DASライブラリには、ドライブが所定の回数使用された後にドライブを自動クリーニングする機能があります。ただし、この機能の使用はお勧めしません。これは、ドライブのクリーニングによってその時点で実行されていたセッションが中断されて失敗するためです。ライブラリの自動クリーニング機能を使用したい場合は、Data Protectorセッションが一切実行されていないことを確認した上で、クリーニング機能を使用してください。

> **重要:**
> メディアの種類ごとに、Data Protectorの論理ライブラリを1つずつ作成する必要があります。ADIC/GRAUシステムまたはSTK ACSシステムでは、多数の物理的に異なる種類のメディアを扱うことができますが、Data Protectorでは1種類のメディアが格納されたライブラリしか認識できません。

Data ProtectorとADIC/GRAU DASライブラリシステムとの統合



StorageTek ACSライブラリ

StorageTek Automated Cartridge System (ACS)ライブラリは、ロボティックライブラリ(サイロ)です。バックアップデータの量が非常に多く、データの格納に大量のメディアが必要となる複雑な環境で使用されます。数百本のテープを処理できます。Data Protectorと他のアプリケーションとでライブラリを共有できるように、デバイス内のメディアの一部を共有専用としてアプリケーションに割り当てることができます。

通常は、StorageTek ACSライブラリには多くの種類のバックアップドライブと数千のメディアスロットが含まれており、いずれも内部のロボティクスメカニズムによって処理され、ACSライブラリサーバー(ACSLS)ソフトウェアによって制御されます。Data Protectorが開始するメディアおよびデバイスに関係するアクションは、ACSLSのユーザーインターフェイスを通じて指定します。ACSLSは、指定に沿って自動化メカニズムを直接制御し、メディアの移動およびロードを実行します。

ライブラリが正しく設置および構成されている場合は、バックアップおよび復元のセッション時にData Protectorを使用してメディアを簡単に処理することができます。Data Protectorのユーザーインターフェイスからすべてのメディア処理を実行することができます。認識可能な形式のメディアの場合は、`tar`などのようにメディアの種類に従ってそData Protectorの形式が表示されます。認識不可能な形式のメディアの場合は、`foreign`とみなされます。

メディア管理データベースは、Data Protectorのメディアとそれ以外のメディアのすべてを、常駐(デバイスのレポジトリ内のData Protectorメディア)か非常駐(デバイスのレポジトリ外のメディア)かに関係なく記録し、高度な上書き保護を実現しています。Data Protectorは認識可能な形式のデータを含むメディアは上書きしません。ただし、テープにあるData Protectorのデータが同じメディアを使用している別のアプリケー

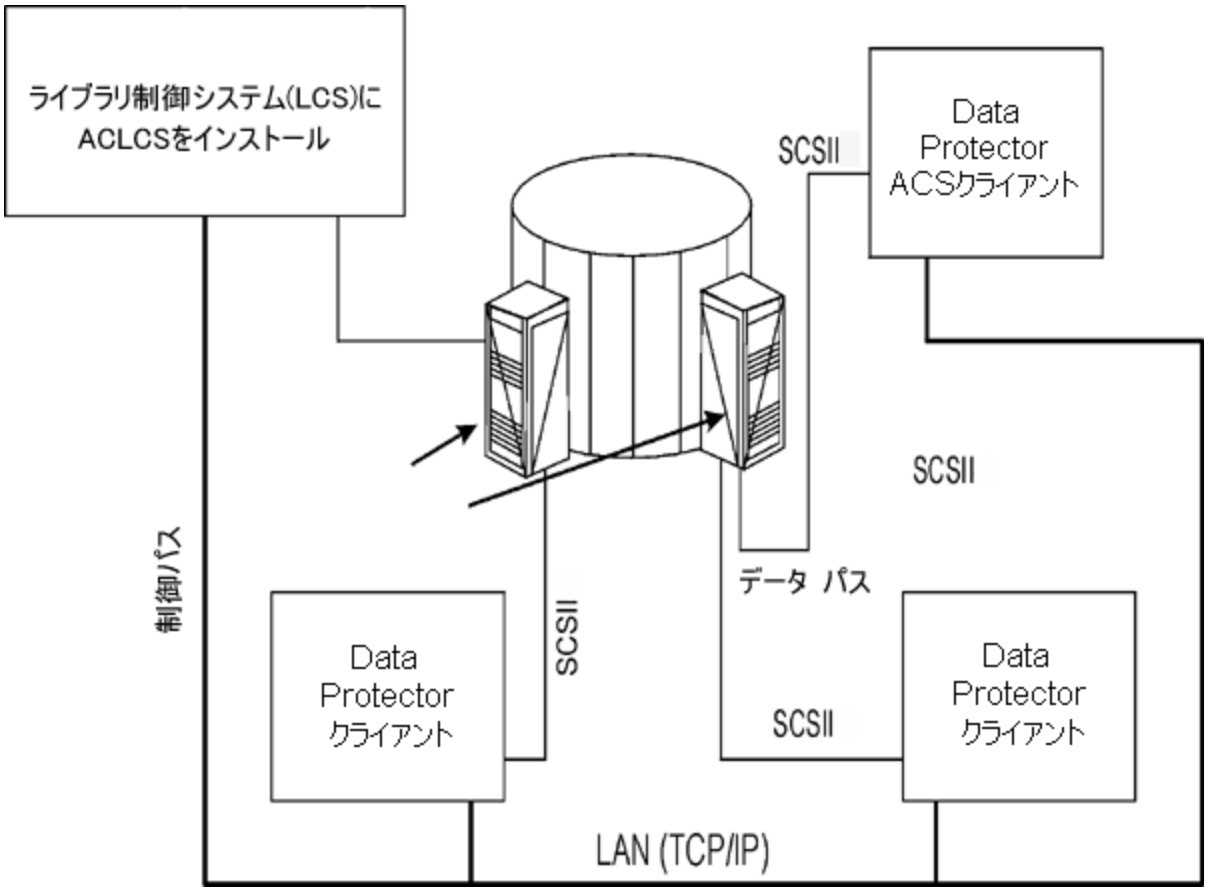
ションによって上書きされないという保証はありません。Data Protectorに使用されるメディアを他のアプリケーションで使用しないことをお勧めします。また、その逆も同様です。

メディアの実際の格納場所は、ACSサーバーによって維持されます。ACSサーバーは、VOLSERを使用して位置を追跡します。レポジトリ内でメディアを移動すると、その都度、異なる物理スロットにメディアが割り当てられます。したがって、メディアの取り扱い時には、スロット番号ではなく、バーコード(VOLSER)を基準として使用してください。

StorageTek ACSライブラリには、ドライブが所定の回数使用された後にドライブを自動クリーニングする機能があります。ただし、この機能の使用はお勧めしません。これは、ライブラリによるドライブのクリーニングによってその時点で実行されていたセッションが中断されて失敗するためです。ライブラリの自動クリーニング機能を使用したい場合は、Data Protectorセッションが一切実行されていないことを確認した上で、クリーニング機能を使用してください。

> **重要:**
> メディアの種類ごとに、Data Protectorの論理ライブラリを1つずつ作成する必要があります。ADIC/GRAUシステムまたはSTK ACSシステムでは、多数の物理的に異なる種類のメディアを扱うことができますが、Data Protectorでは1種類のメディアが格納されたライブラリしか認識できません。

Data ProtectorとStorageTek ACSライブラリデバイスとの統合



StoreOnceソフトウェア重複排除コンポーネントについて

インストール

ここでは、主なインストール作業、およびStoreOnceソフトウェア重複排除コンポーネントのインストールに特有の要件について大まかに説明します。

前提条件

HPE Data Protector 10.00 Cell Manager、ユーザーインターフェイスクライアント、およびInstallation Serverが対応システムにインストールされていることを確認してください。

詳細については、http://support.openview.hp.com/selfsolve/manualsで、HPE Data Protectorに関する最新のサポート一覧を参照してください。各種アーキテクチャーでのData Protectorのインストール方法については、『*HPE 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。

ファイアウォールの構成

内向きの接続に対して次のポートがオープンになっていることを確認してください。

- `9387/tcp` – コマンドポート(StoreOnceソフトウェアシステムおよびStoreOnce Backupシステム向け)
- `9388/tcp` – データポート(StoreOnceソフトウェアシステムおよびStoreOnce Backupシステム向け)

ポート9387および9388は、ターゲットデバイスをすべてのゲートウェイから切り離すファイアウォールでオープンにする必要があります。(Windowsシステム: インストールプロセス中はポートが開かれています。UNIXシステム: ポートを手動で開く必要があります)。Data Protectorのポートの詳細については、『HPE Data Protectorヘルプ』のキーワード「ポート範囲」で表示される内容を参照してください。

インストール手順

Data Protector Media AgentまたはNDMP Media Agentコンポーネントを、ソース側重複排除を有効にするクライアントを含み、ゲートウェイとなるすべてのシステムにインストールします。

手順については、『HPE Data Protectorインストールガイド』を参照してください。サポートされているオペレーティングシステムのバージョンの詳細なリストについては、http://support.openview.hp.com/selfsolve/manualsにある最新のサポート一覧を参照してください。

StoreOnceソフトウェア重複排除の追加手順

Data ProtectorのStoreOnceソフトウェア重複排除コンポーネントは、StoreOnceストアをホストするシステムにインストールします。

StoreOnceソフトウェア重複排除コンポーネントは、ローカルまたはリモートでインストールできます。

Data ProtectorのStoreOnceソフトウェア重複排除コンポーネントのリモートインストール

1. Data Protectorのユーザーインターフェイスコンポーネントを任意のクライアントに接続します。
2. Data ProtectorのGUIを開き、コンテキストリストで[クライアント]を選択します。
3. Data ProtectorのStoreOnceソフトウェア重複排除コンポーネントをバックアップクライアントに追加します。

- バックアップクライアントがData Protectorのセルに組み込まれていない場合は、Data Protectorの[クライアントの追加]機能を使用します。
- バックアップクライアントがすでにData Protectorのセルに組み込まれている場合は、Data Protectorの[コンポーネントの追加]機能を使用します。

インストールが正常に終了すると、StoreOnceソフトウェア重複排除コンポーネントがインストール済みコンポーネント一覧に表示されます。

StoreOnceソフトウェア重複排除を使用するには、ストアのルートディレクトリを事前に構成しておく必要があります。

Data ProtectorのStoreOnceソフトウェア重複排除コンポーネントのローカルインストール

Windowsシステム:
Data Protectorのローカルインストール中に、コンポーネントリストから`the StoreOnce Software Deduplication` コンポーネントを選択します。

Linuxシステム:
`omnisetup.sh –installStoreOnceSoftware`を実行します。

StoreOnceSoftwareサービス/デーモンの設定

Windowsシステムの場合:
インストールが正常に終了すると、StoreOnceSoftware実行可能プログラムがサービスとして起動します(タスクマネージャーの[サービス]タブを参照)。サービス名は「Data Protector StoreOnceSoftware」、説明は「`StoreOnce Software Deduplication`」、および起動の種類は自動です。

Linuxシステムの場合:
システムの再起動後にStoreOnceSoftwareデーモンが自動的に起動するようにインストールするには、`StoreOnceSoftwared`ファイルを`/etc/init.d`ディレクトリにコピーし、起動スクリプトに追加します。デーモンの開始や停止は、次のコマンドを使用して手動で行うこともできます。

```
/opt/omni/lbin/StoreOnceSoftwared start
```

および

```
/opt/omni/lbin/StoreOnceSoftwared stop
```

StoreOnceソフトウェア重複排除コンポーネントをシステムから削除すると、プロセスが自動的に停止し、`StoreOnceSoftwared`ファイルが`/etc/init.d/`ディレクトリから削除されます。

インストールディレクトリの構造

Windowsシステムの場合:
インストールコンポーネントには次のファイルが含まれます。

ファイル名	ファイルの場所
StoreOnceSoftware.exe	*Data_Protector_home*\bin
system.db	*Data_Protector_program_data*\Config\client\StoreOnceSoftware

Linuxシステムの場合:
インストールが正常に終了すると、StoreOnceSoftwareがバックグランドプロセス(デーモン)として起動します。StoreOnceSoftwareは、再起動後に自動で起動させることができます。

インストールコンポーネントには次のファイルが含まれます。

ファイル名	ファイルの場所
StoreOnceSoftware	/opt/omni/lbin
StoreOnceSoftwared	/etc/init.d/ /opt/omni/lbin
system.db	/etc/opt/omni/client/StoreOnceSoftware

トラブルシューティング

ここでは、Data ProtectorのStoreOnceソフトウェア統合使用時のログおよびイベント報告、警告、診断、および問題解決情報について説明します。Data Protectorの全般的なトラブルシューティング情報については、『*HPE Data Protectorトラブルシューティングガイド*』を参照してください。

ディスクスペース不足の警告

ストアが存在するディスクのスペースが不足することがないように、事前に定義したしきい値に達すると、警告メッセージが(Windowsシステムの場合はイベントログに、Linuxシステムの場合はシスログに)書き込まれます。デフォルトのしきい値はストア容量の10%です。このデフォルトの値は、omnircオプションを使用することにより変更可能です。警告メッセージは、ストアに対する読み込み/書き込み操作がそれ以上行われる前に、1日に1回またはStoreOnceSoftwareユーティリティの再起動時に生成されます。また、セッションの開始時および終了時にも、警告がバックアップセッションメッセージに表示されます。ディスクスペース不足の警告を次に示します。

```
You are running out of disk space on Deduplication Store root directory: [path].
The threshold x% is reached. Please free space or add more disks. [warning].
```

system.dbファイルのバックアップ

system.dbデータベースファイルには、ルートディレクトリ情報とストアに関する情報が含まれています。これは、次の場所にあります。*DataProtector_Program_Data*\OmniBack\Config\client\StoreOnceSoftware。このファイルを削除または紛失すると、ストアおよびバックアップ済みデータにアクセスできません。この状況を回避するため、データベースが変更されるたびに、system.db ファイルのバックアップコピーが.\Store_Root\StoreOncelibrary\system.db.bakに作成されます。 system.dbファイルの復元は、バックアップファイルを元の場所にコピーし、名前を変更してStoreOnceSoftwareユーティリティを再起動することで行えます。

ルートディレクトリの下のファイルが保護されていること(RAIDまたはバックアップ)を確認してください。

StoreOnceSoftwareユーティリティで報告されている一般的な問題とエラーを以下に示します。エラーは、運用環境、および重複排除ストアのディレクトリ構造に関するものが一般的です。

StoreOnceSoftwareユーティリティがストアのルートディレクトリを見つけられません。

問題
Accessing the system.db file: The system.db file is inaccessible (for example, permission denied, or disk full).
対処方法
パーミッションの変更やディスクスペースの解放を行うか、データベースをアクセスできるように変更します。データベースファイル(system.db)が空か、重複排除ストアのルートディレクトリに対して値が何も指定されていません。

StoreOnceSoftwareユーティティティが起動しません。

問題
system.dbファイルへのアクセス: ストアのルートディレクトリにsystem.dbファイルが存在しない。
対処方法
system.dbファイルの復元または再作成を行います。1つ前の問題を参照してください。

ストアの起動時にエラーが記録されます。ストアにはアクセスできません。

問題
ストアの開始: ストアディレクトリにアクセスできない。
対処方法
ストアのディレクトリをアクセスできるように変更し、パーミッションをチェックして、ルートディレクトリが存在することを確認します。

ストアは正常に起動しますが、アイテムが何も見つかりません。

問題
ストアの開始: ストアディレクトリがない。
対処方法
ルートディレクトリとルートディレクトリの下にあるストアを復元します。

エラーが記録されます。ストアにはアクセスできません。

問題
ストアの開始: ストアがダーティで復旧できない。
対処方法
ルートディレクトリとルートディレクトリの下にあるストアを復元します。

ストアを停止すると、エラーが報告されます。

問題
ストアの停止: アイテムがオープン状態 (バックアップセッションまたは復元セッションの実行中など)。
対処方法
StoreOnceSoftwareユーティリティを終了する前に、すべての動作が終了していることを確認します。

シャットダウン中にエラーが記録されます。次回の再起動時に復旧が行われることがあります。

問題
ストアの停止: メンテナンスユーティリティを停止できない。
対処方法
すべての動作が終了していることを確認してから、StoreOnceSoftwareユーティリティを終了します。次回の再起動時に復旧が行われることがあります。

使用可能なディスクスペースが少ない場合は、警告メッセージが記録されます。

問題
ディスクスペースとメモリが少ないため、StoreOnceSoftwareサービス/デーモンによって、警告およびエラーメッセージがWindowsのイベントログまたはLinuxのシスログに記録される。 システムの仮想空きメモリが残り25%に達した場合、エラーメッセージが記録されます。また、仮想空きメモリが残りわずか20%になった場合は、エラーメッセージが記録され、それ以上の読み込み操作と書き込み操作がサービス/デーモンによって拒否されます。

対処方法
システムリソースを解放します。ディスクスペースまたはメモリを解放すると、サービス/デーモンは操作の拒否を停止します。

Data Protectorに「ストアが存在しません」と警告が表示され、バックアップセッションが失敗する。

問題
StoreOnce Backupシステムデバイスを使用したバックアップセッションの実行時に、次のような警告が表示され、セッションが異常終了します。 `[Warning] From: BSM@computer.company.com "CS2BackupTmp" Time: 6/18/2012 1:34:08 PM Got error: " Store does not exist. " when contacting " DeviceName" B2D device!` この問題は、B2Dデバイス上のストアが削除されたか、またはこのストアのパーミッションが変更された場合に発生する可能性があります。
対処方法
• ストアが存在するかどうか、またはこのストアに対するパーミッションが変更されたかどうかを確認します。 • ストアが正しく設定されている場合は、Data Protectorのデバイス設定を確認します。デバイスを右クリックして[プロパティ]を選択し、[デバイス] - [ストアおよびゲートウェイ]ページで[クライアントID]を確認します。

B2Dデバイスでのステータスの更新が間隔をおいて実行されます。

問題
バックアップサイズのソフトクォータまたはストアサイズのソフトクォータを超えても、Data Protectorで警告が表示されない。
対処方法
ありません。次のバックアップセッションでは、警告が正しく表示されます。

StoreOnceストアおよびDD Boost重複排除デバイス

Data Protectorは、HPE (StoreOnce)およびEMC (DD Boost)の重複排除製品をサポートしています。Catalystは、前者の重複排除を管理するソフトウェアのことであり、以下の説明では同じ意味で使用されています。詳細については、『*HPEData Protectorコンセプトガイド*』を参照してください。

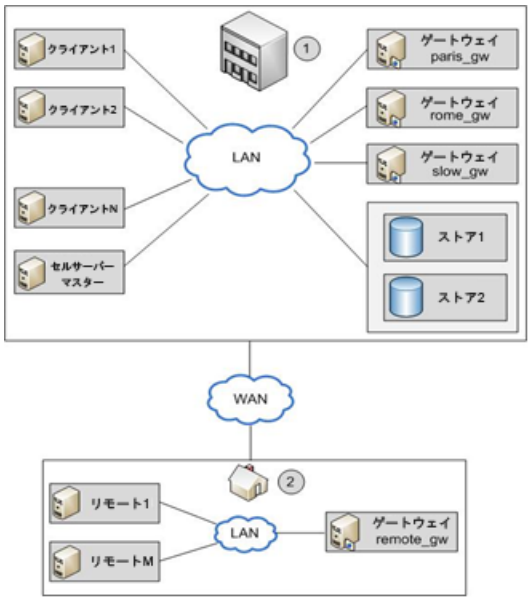
ここでは、環境例と構成手順について説明します。

マルチインターフェイスサポート

Data Protectorはマルチインターフェイスサポートを提供しています。IP接続とFC接続の両方で、同じCatalystストアまたはBoostストアに接続できます。Data Protectorでは、個別にストアを構成する必要はなく、同じCatalyst/DDBoostストアへのIP接続とファイバーチャネル接続をサポートしています。ストアには、両方のインターフェイス経由で同時にアクセスできます。たとえば、1つのCatalyst/DDBoostストアにローカルクライアントが高速バックアップのためにファイバーチャネル経由でアクセスし、リモートクライアントが低速バックアップのためにWAN経由でアクセスすることができます。

B2Dデバイスを使用した構成例

以下の図は、本社/リモートオフィス構成の代表的な使用モデルを示しています。



アイテム	説明
1	本社。このLANは本社に敷設されており、WAN経由でリモートオフィスのLANに接続されています。
2	リモートオフィス。このLANはリモートオフィスに敷設されています。

Data ProtectorのCell Managerは、本社のマスターホスト上にインストールされています。本社には、*client1*から*clientN*までの非ゲートウェイクライアントと、*paris_gw*、*rome_gw*、および*slow_gw*のゲートウェイクライアントがあります。さらに、2つのオブジェクトストア(ストア1およびストア2)が本社の構成に組み込まれています。

リモートオフィスには、*リモート1*から*リモートM*までのクライアントと*remote_gw*が設置されており、すべてのクライアントが本社のクライアントと同じData Protectorセルに組み込まれています。リモートオフィスは、低速のWANネットワーク経由で本社に接続されています。

> **注:**
> ゲートウェイは、単にMedia Agentコンポーネントがインストールされたクライアントです。ゲートウェイ

> クライアントと考えてください。ゲートウェイとするクライアントには、必ず64ビットシステムを使用してください。

B2Dデバイスの構成時には、ストアの名前と場所、ゲートウェイおよびネットワークパスといった、決められたパラメーターを指定する必要があります。上記の例では、ストア1というストア(StoreOnceソフトウェア重複排除のアクセス先)を環境内のクライアントのバックアップに使用します。このため、ストア1をレポジトリとして使用するようにB2Dデバイスを構成します。また、クライアントの*paris_gw*、*rome_gw*、および*slow_gw*は、本社にある他のData Protectorクライアントのゲートウェイとして使用します。このほか、次の点にも注意してください。

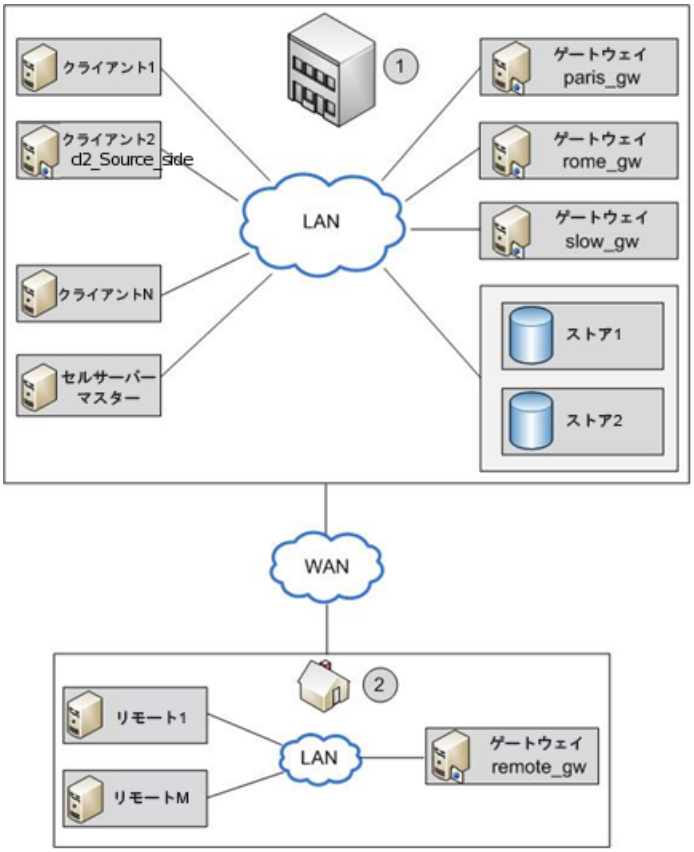
- 同時処理数によって、同時にデバイスへの書き込みを行うDisk Agentの数を指定します。複数のDisk Agentが並行して(ディスクから)データを読み込むことで、Media Agentへのデータストリームを一定に保ちます。StoreOnceソフトウェア重複排除では、各Media Agentに対するDisk Agentの同時処理数が1に設定(これによって重複排除率が向上)されています。
- Data Protectorは、暗号化されたストアへのバックアップと同様に、暗号化されていないストアへのバックアップもサポートします。暗号化はストアの作成時に有効にできます。いったんストアを作成すると、その状態を暗号化から非暗号化に、またはその逆に変更できません。
- 1台のデバイスに構成できるストアは1つだけです。
- ストアは、重複排除システムとストア名に関する情報を示すネットワークパス(UNC)で表されます。(注記: B2Dデバイスのコンテキストでは、重複排除システムが、重複排除ストアが存在するホスティングマシンの名前を参照します。)

ソース側重複排除

上記のシナリオは、個々のクライアントからバックアップされるデータの量が限られている場合に適しています。ただし、ソース側ゲートウェイを構成して、ネットワークのトラフィックを削減することもできます。

たとえば、上記のシナリオで、クライアント2のデータが大量に重複しているが、システムの負荷は中程度であるとします。ネットワークの負荷は、B2Dデバイスに対してソース側重複排除を有効にすることで低減できます。また、バックアップ仕様でクライアント2に対してソース側重複排除を有効にすると、クライアント2上にソース側ゲートウェイが自動的に作成され、Media Agentが重複排除済みデータのみをネットワーク経由で送るようになります。

同様に、他のクライアントに対してソース側重複排除を有効にすると、そのクライアント上にもソース側ゲートウェイが自動的に作成されます。



B2Dデバイスの追加

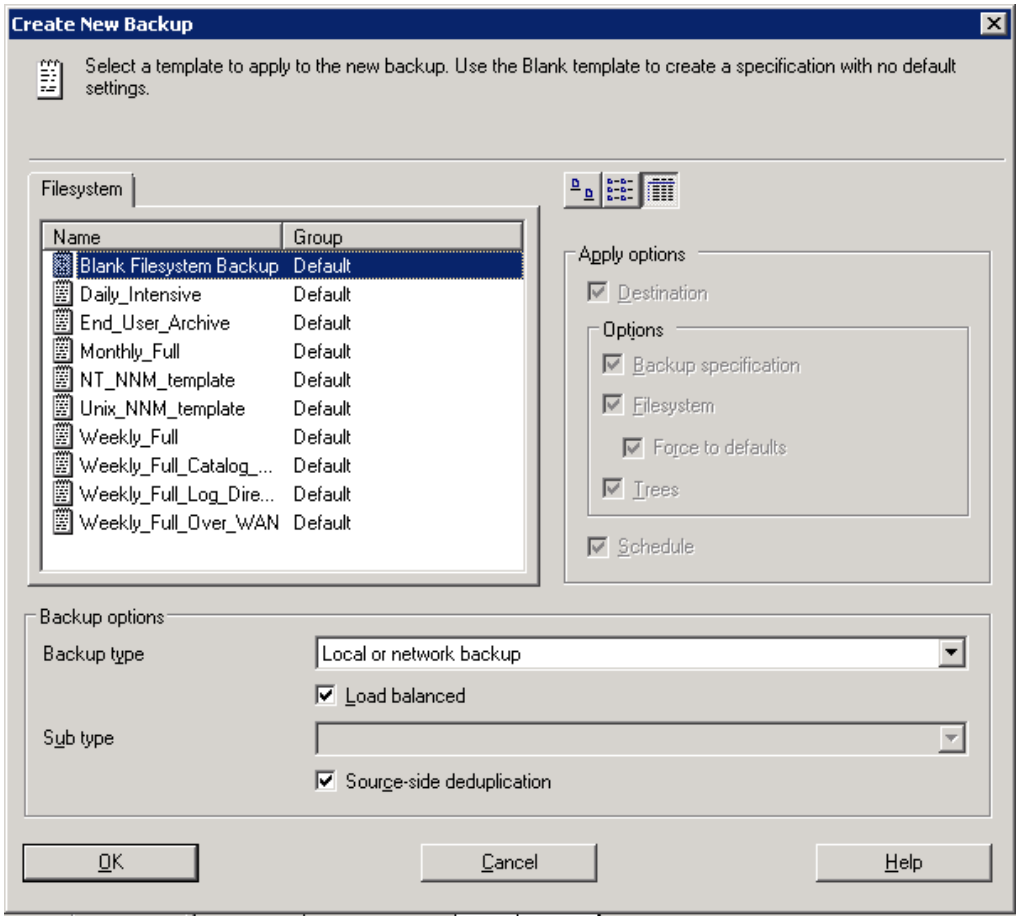
B2Dデバイスの追加手順は、デバイスの種類を追加する手順とほぼ同じです。詳細については、『*HPE Data Protectorオンラインヘルプ*』および『*HPE Data Protector管理者ガイド*』を参照してください。

バックアップ

Data Protectorでは、バックアップ仕様でB2Dデバイスを指定することで、重複排除型のバックアップを行えます。重複排除プロセスがバックグランドで稼働し、重複排除済みデータがStoreOnceソフトウェアシステムまたはStoreOnce Backupシステムに書き込まれます。

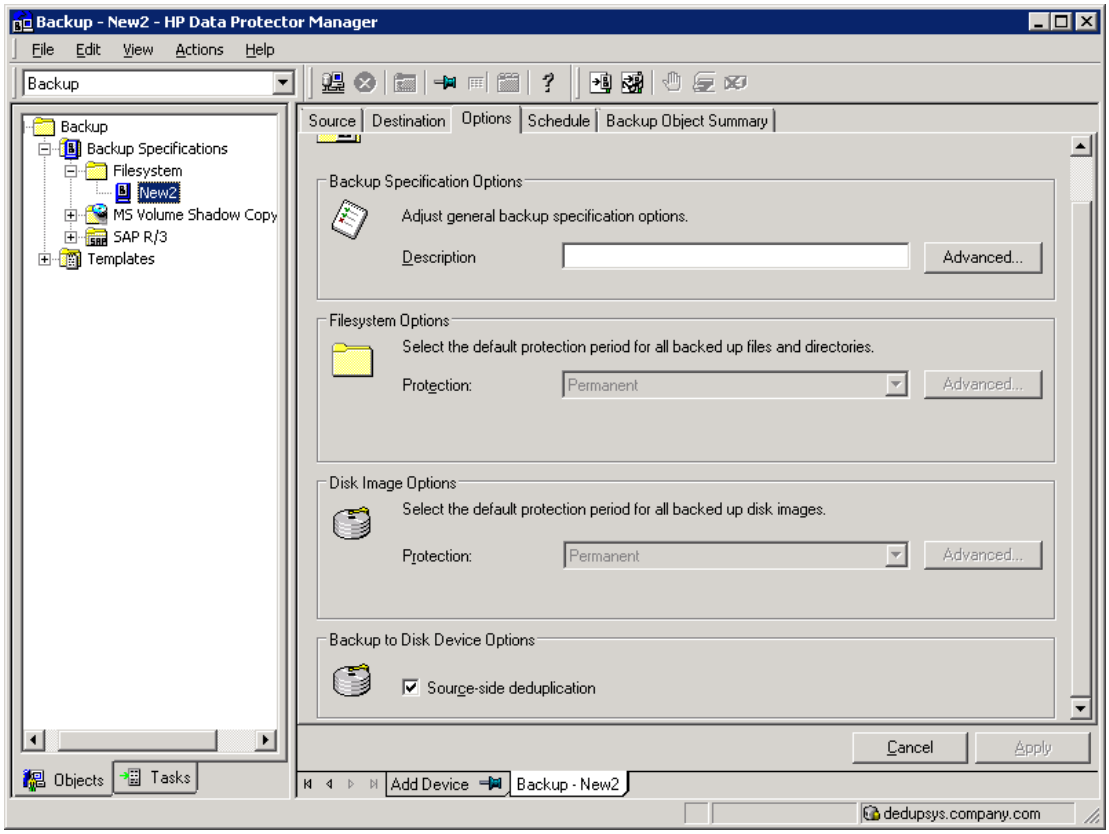
重複排除型のデータバックアップは、従来のバックアップと同じ方法で作成します。

1. 新規B2Dデバイスを追加(この場合は、StoreOnceソフトウェア重複排除またはStoreOnce Backupシステムを指定)します。
2. このデバイスを対象とするバックアップ仕様を作成します。詳細については、『*HPE Data Protectorヘルプ*』のキーワード「作成、バックアップ仕様」で表示される内容を参照してください。ソース側重複排除を有効にする場合には、バックアップ仕様の作成時に[ソース側重複排除]オプションを選択します。



[ソース]ページでバックアップオブジェクトを選択する際、ソース側ゲートウェイが構成されていないクライアントは、すべて網がけで表示されます。クライアント一覧は、[表示]ドロップダウンリストで**[ソース側重複排除]**を選択してフィルターできます。

ソース側重複排除は、バックアップ仕様を選択し、[オプション]ペインを開いて**[ソース側重複排除]**を選択しても有効にできます。



3. [あて先]ページで、バックアップに使用するゲートウェイを選択します。**[プロパティ]**をクリックして、ゲートウェイのオプションを確認および変更します。**[ゲートウェイごとの並列ストリームの最大数]** オプションを指定すると、デバイスの構成中に設定した値が上書きされます。

> **注:**
> ソース側重複排除を選択すると、ソース側ゲートウェイを使用できるクライアントからのオブジェクトのみのバックアップと、ソース側ゲートウェイが構成されたデバイスのみの選択が行えます。このオプションの選択を解除した場合は、ソース側ゲートウェイの代わりに、B2Dデバイスのすべてのゲートウェイが自動的に選択され、警告メッセージが表示されます。

> **重要:**
> 既存のバックアップ仕様でソース側重複排除を有効にすると、ソース側重複排除を行えないクライアントの選択が解除され、バックアップは行われません。

復元

バックアップ済みデータは、従来の復元操作と同じ方法で復元します。ただし、重複排除ストアからデータを復旧するバックグランドプロセスは従来の復元プロセスとは大きく異なり、特別な作業を伴いません。復旧プロセスの主な操作としては、復元するデータのメモリへのロード、インデックステーブルからの参照情報の読み込み、およびバックアップ済みデータの*リハイドレート*に必要な情報の使用が挙げられます。『*HPE Data Protectorヘルプ*』のキーワード「復元」で表示される内容を参照してください。

ソース側重複排除に関する注意

ソース側重複排除を有効にしたままバックアップを行い、ソース側ゲートウェイを使用できないクライアントに対して復元を行うと、ソース側ゲートウェイではなく通常のゲートウェイが使用されます。

Catalyst over Fibre Channel用のStoreOnce Catalystクライアント構成

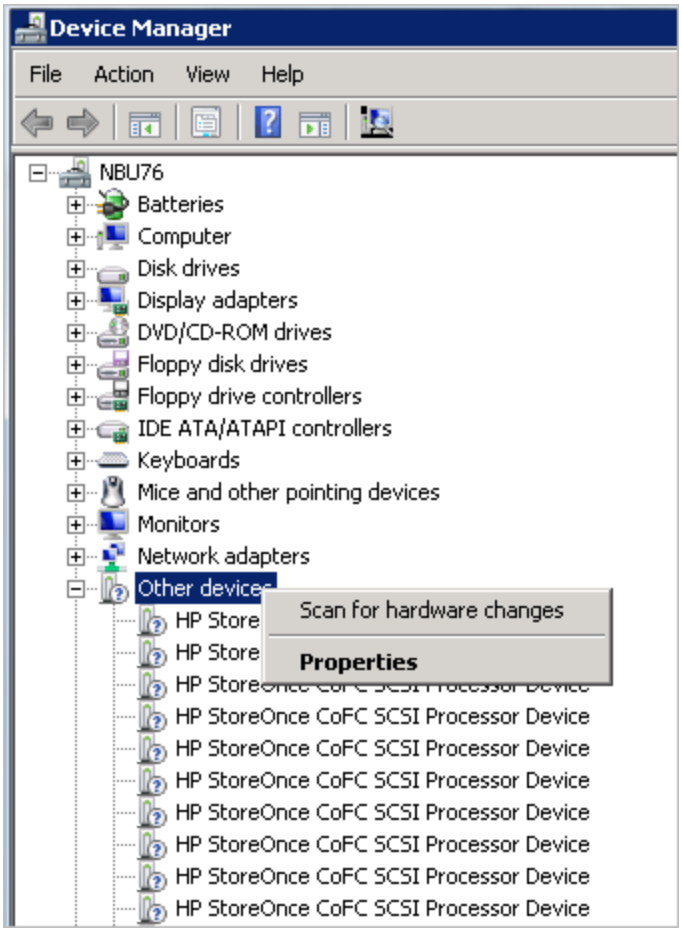
> **注:**
> 以下は、正式な情報ではりません。最新の詳細情報については、StoreOnceのドキュメントを参照してください。

Windowsクライアント

Catalyst over Fibre Channelのバックアップを実行するには、管理者パーミッションが必要です。

StoreOnce Catalyst over Fibre Channelが提示するデバイスの種類は**プロセッサー**です。デバイスのゾーニングまたはイニシエーターポートごとのデバイス数の変更後に、以下の手順を実行します。

1. Windowsの**[デバイス マネージャ]**に移動して、**[その他のデバイス]**を右クリックします。
2. **[ハードウェア変更のスキャン]**を選択して、新しいデバイスを検出します。



Linuxクライアント

StoreOnce Catalyst over Fibre Channelが提示するデバイスの種類はプロセッサーです。Linuxでは、デバイスファイルは`/dev/sg*`に作成されます。デフォルトで、`/dev/sg*`デバイスにアクセスできるのは、ルートユーザーのみです。ルートユーザー以外の場合は、Linux udevルールを使用して、デバイスファイルにアクセスするためのバックアップユーザーパーミッションを提供します。

udevルールを作成するには、以下の手順を実行します。

a. バックアップサーバーごとに、以下の場所にudevファイルを作成します。

   `/etc/udev/rules.d/70-cofc.rules`

b. ファイルに以下のルールを追加します。

   ```
   KERNEL=="sg[0-9]*", ATTRS{vendor}=="HP*", ATTRS{model}=="StoreOnce CoFC*",
   ATTRS{rev}=="CAT1", GROUP="##CORRECT_USER_GROUP##"
   ```

   `##CORRECT_USER_GROUP##` は、バックアップと復元を実行するLinuxユーザーグループで置き換えられます。例: `dba/oracle`。

c. パーミッションを更新するために、デバイスファイルの変更をスキャンします。

   `lsscsi --generic`コマンドを使用して、Catalyst over Fibre Channelに属する/dev/sg*デバイスファイルを判別できます。

AIXクライアント

3.14より前のバージョンのStoreOnceソフトウェアでは、StoreOnce Catalyst over Fibre Channel on AIXは、要求後に使用可能になります。

> **注:**
> 3.14より前のバージョンのStoreOnceを使用するCatalyst over Fibre Channel on AIX 6.1または7.1を使用する必要がある場合は、StoreOnceサポートにお問い合わせください。

StoreOnce Catalyst over Fibre ChannelがAIXで提示するデバイスの種類はシーケンシャルです。これらのデバイスファイルは、`/dev/rmt*`に作成されます。デバイスのゾーニングまたはイニシエーターポートごとのデバイス数の変更後に、以下の手順を実行します。

a. `storeonce-cofc-passthrough-install.sh`スクリプトを実行します。

> **注:**
> このインストールスクリプトは、HPE Data Protectorではなく、StoreOnceソフトウェアキットの一部です。

b. `cfgmgr` コマンドをルートユーザーとして実行し、デバイスファイル内の変更をスキャンします。

c. デフォルトで、`/dev/rmt*`デバイスファイルには、ルートユーザーのみがアクセスできます。ルートユーザー以外がバックアップを実行するには、追加のパーミッションが必要です。

HP-UXクライアント

StoreOnce Catalyst over Fibre Channelが提示するデバイスの種類はプロセッサーです。HP-UXでは、デバイスファイルは`/dev/pt/ptX`に作成されます。

デバイスのゾーニングまたはイニシエーターポートごとのデバイス数の変更後に、以下の手順を実行します。

a. デバイスファイルの変更をスキャンします。

b. `ioscan -fnC /dev/pt` コマンドをルートユーザーとして実行します。

   デフォルトで、`/dev/pt/ptX` デバイスにアクセスできるのは、ルートユーザーのみです。ルートユーザー以外の場合は、`chmod o+rwx /dev/pt/pt*` コマンドを使用して、デバイスファイルにアクセスするためのバックアップユーザーパーミッションを提供します。

c. /dev/pt/ptXデバイスファイルのパーミッションを取得するには、以下のCatalyst over Fibre Channelコマンドを使用します。

   ```
   /usr/sbin/scsimgr -p get_attr all_lun -a device_file -a dev_type -a pid |
   grep StoreOnce
   ```

d. 該当するデバイスに対して、chmod o+rwxコマンドを使用します。

Solarisクライアント

StoreOnce Catalyst over Fibre Channelが提示するデバイスの種類はプロセッサーです。Solarisでは、デバイスファイルは`/dev/scsi/processor/*`に作成されます。デバイスのゾーニングまたはイニシエーターポートごとのデバイス数の変更後に、以下の手順を実行します。

a. デバイスファイルの変更をスキャンします。

b. ルートユーザーとして、以下のコマンドを実行します。

- `add_drv -vi scsiclass,03 sgen`
- `update_drv -vai scsiclass,03 sgen`

  デフォルトで、/dev/scsi/processor/*デバイスにアクセスできるのは、ルートユーザーのみです。ルートユーザー以外の場合は、`chmod -R o+rwx /dev/scsi/processor/*`コマンドを使用して、デバイスファイルにアクセスするためのバックアップユーザーパーミッションを提供します。

c. /dev/scsi/processor/*デバイスファイルのパーミッションを取得するには、以下のCatalyst over Fibre Channelコマンドを使用します。

```
for i in /dev/scsi/processor/*; do echo $i; ls $i; luxadm inq $i | egrep
"Vendor|Product"; echo; done
```

d. 該当するデバイスに対して、chmod -R o+rwxコマンドを使用します。

B2Dデバイス関連のOmnircオプション

omnircファイルは、次のオプションが追加され、拡張されています。このファイルは、ポート番号およびディスクスペースのしきい値警告など、パラメーターの設定に使用します。

`OB2_STOREONCESOFTWARE_COMMAND_PORT=`*`PortNumber`*

このオプションは、Media AgentとStoreOnceSoftwareユーティリティ間のコマンド通信に使用するポートの変更に使用します。

例: `OB2_STOREONCESOFTWARE_COMMAND_PORT=12345`

デフォルト: 9387

`OB2_STOREONCESOFTWARE_DATA_PORT=`*`PortNumber`*

このオプションは、Media AgentとStoreOnceSoftwareユーティリティ間のデータ通信に使用するポートの変更に使用します。

例: `OB2_STOREONCESOFTWARE_DATA_PORT=12346`

デフォルト: 9388

`OB2_STOREONCESOFTWARE_SESSION_IDLE_TIMEOUT=s`

StoreOnceSoftwareデーモンが、定期的にアイドル状態の接続をチェックして終了させます。このオプションには、接続をアイドル状態と判断するまでの動作停止時間を秒数で指定します。

デフォルト: 300 (範囲: 最小: 10)

`OB2_STOREONCESOFTWARE_DISK_SPACE_THRESHOLD=%`

このオプションは、ディスクの空きスペースに対するしきい値の設定に使用します。

デフォルト: 10% (範囲: 1% - 95%)

OB2_STOREONCESOFTWARE_MINIMUM_DISK_SPACE=n

このオプションは、StoreOnceSoftware用に予約しておく最少ディスクスペース(MB)の制御に使用します。この最小値に達すると、ストアへのデータの書き込みが行われません。デフォルト: 1000 (最小: 500)

OB2_STOREONCESOFTWARE_SSL_ENABLE=0|1

デフォルト: 1

このオプションは、クライアントとStoreOnceSoftwareデーモン間のセキュアな制御通信の有効化または無効化の指定に使用します。このオプションを0に設定すると、StoreOnceSoftwareデーモンが稼働するクライアントがセキュアな制御通信を使用する設定になっていても、セキュアな制御通信は使用されません。

セキュアな通信を有効にした後は、StoreOnceSoftwareデーモンを手動で再起動してください。

OB2_STOREONCESOFTWARE_DISABLE_IPV6_LISTEN=0|1

デフォルト: 0

デフォルトでは、StoreOnceSoftwareデーモンはデュアルスタックソケット(同一ポート上のIPv6およびIPv4)を監視します。1に設定すると、IPv6が無効になります。このオプションは、RPCおよびIpcServerのリスンポートに適用されます。

OB2D2D_COMMAND_PORT=PortNumber

このオプションは、Media AgentとStoreOnce Backupシステム間のコマンド通信に使用するポートの変更に使用します。

例: OB2D2D_COMMAND_PORT =12345

デフォルト: 9387

OB2D2D_DATA_PORT=PortNumber

このオプションは、Media AgentとStoreOnce Backupシステムユーティリティ間のデータ通信に使用するポートの変更に使用します。

例: OB2D2D_DATA_PORT=12346

デフォルト: 9388

OB2D2D_NUM_OF_LBWTHREADS=ThreadNum

この変数は、Media Agentクライアント上で重複排除を行う際の重複排除計算に使用するスレッド数の定義に使用します。より処理能力が高いゲートウェイを使用している場合は、この数を8スレッドまで増やせます。このオプションは、各ゲートウェイに対して個別に設定してください。

デフォルト: 4

OB2D2D_BANDWIDTH_BUFF_SIZE=Size

この変数は、Media Agentクライアント上で重複排除を行う際のバッファーサイズの設定に使用します。Media AgentとD2Dデバイス間の通信をLAN経由で行う場合は、デフォルト設定を変更する必要はありません。WANネットワークを通信に使用する場合は、20 MBがより適切な値です。このオプションは、各ゲートウェイに対して個別に設定してください。

デフォルト: 10 MB

クラウド(Helion)デバイスについて

クラウド(Helion)デバイスは、クラウド(Helion)の資格情報を使用して構成されたデバイスで、HPE Public Cloudをサポートします。Media Agentは、クラウド(Helion)デバイスにデータを転送するクラウドゲートウェイとして機能するように改良されています。Media Agentの動作は、ディスクへのバックアップ(B2D)デバイスと似ています。

前提条件

HPE Public Cloudの前提条件:

- HPE Public Cloudのアカウントと資格情報が必要です。詳細については、https://horizon.hpcloud.comを参照してください。
- HPE Public Cloud内のオブジェクトストアのサブスクリプションが必要です。
- HPE Public Cloud内のプロジェクトのプロジェクト名をメモする必要があります。
- 自社のデータセンターに最も近い地域の認証サービスのURLを用意します。
- ユーザー名とパスワードの代わりにアクセスキーを使用して認証を行う場合は、HPE Public Cloud内にアクセスキーを作成します。

Data Protectorの前提条件:

- Data Protectorの最新のCell Manager、ユーザーインターフェイスクライアント、およびインストールサーバーが、最新の9.04一般パッチリリースバンドルと共に、サポートされるシステムにインストールされていることを確認してください。

  詳細については、最新のHPE Data Protectorサポート一覧(https://softwaresupport.hpe.com/)を参照してください。HPE Data Protectorをさまざまなアーキテクチャーにインストールする方法については、『*HPE Data Protectorインストールガイド*』を参照してください。
- クラウド(Helion)デバイスが有効になるクライアントを含め、クラウドゲートウェイとして使用するWindowsシステムとLinuxシステムに、Data Protector Media AgentまたはNDMP Media Agentコンポーネントをインストールします。手順については、『*HPE Data Protectorインストールガイド*』を参照してください。

  サポートされるオペレーティングシステムのバージョンの詳細なリストは、最新のサポート一覧(https://softwaresupport.hpe.com/)を参照してください。

制限事項

- クラウド(Helion)デバイスのオブジェクトコピーは試験済みであり、以下の仕様をサポートします。
  - ソースデバイス: ファイルライブラリデバイスおよびStoreOnceデバイス
  - VMwareバックアップ仕様

- HPEオブジェクトストア内でコンテナーを選択または作成するときには、次の制限事項が適用されます。
  - 各デバイスに1つのコンテナーのみを割り当てることができます。
  - 異なるデバイスで同じコンテナーを使用することはできません。
  - 一度デバイスに割り当てたコンテナーは変更できません。
- クラウド(Helion)デバイスを構成するときには、そのデバイスのブロックサイズがオンプレミスのソースデバイスと同じかそれより大きいことを確認してください。

  オンプレミスデバイスとクラウド(Helion)デバイスの間でオブジェクトコピーを行う場合は、両方のデバイスのブロックサイズが一致している必要があります。ブロックサイズはゲートウェイのプロパティで設定できます。

推奨事項

HPEは、クラウド(Helion)デバイスについて以下の事項を推奨します。

- VMwareの仕様をバックアップするときには、データソースのローカルのクラウドゲートウェイを使用し、オブジェクトコピー操作中のネットワーク負荷を減らしてください。
- 使用可能な場合は認証モードとして**アクセスキー**を使用してください。これにより、クラウド(Helion)デバイスへのアクセス全体が制限され、システムのセキュリティが強化されます。
- 大きなデータセットをHPE Cloudにコピーするときには複数のバックアップ仕様に分割してください。

  これにより、多くのコピーセッションを並列実行できるようになり、全体的な帯域幅の使用率が向上し、HPE Cloudへのデータコピーの効率も向上します。
- クラウド(Helion)サービスを統合すると、必要な帯域幅が大きくなり、それに関連したHPE Cloudのコストが発生するので推奨されません。

クラウド(Helion)デバイスの準備

クラウド(Helion)デバイスへのオブジェクトコピー操作を構成するには次の作業を実行する必要があります。

1. ローカルバックアップデバイスにデータをバックアップするためのバックアップ仕様を構成します。詳細については、バックアップ仕様を作成するを参照してください。
2. HPE Public Cloudで、認証に必要なユーザーアカウントの資格情報またはアクセスキー、オブジェクトストアのサブスクリプション、認証サービスのURL、および他のHPE Public Cloudの前提条件を取得します。これはクラウド(Helion)デバイスを構成するために使用されます。
3. HPE Data Protectorで、クラウド(Helion)デバイスを構成します。詳細については、クラウドデバイスを構成するを参照してください。
4. ローカルバックアップデバイスをソースデバイスとして使用し、クラウド(Helion)デバイスをバックアップ先デバイスとして使用して、オブジェクトコピーセッションを構成します。

   クラウド(Helion)デバイスへのオブジェクトのコピーの操作を作成すると、ローカルバックアップデバイスに保存されたデータをHPE Public Cloudにコピーできるようになります。クラウド(Helion)デバイスに送信されたデータはデフォルトで圧縮および暗号化されます。
5. クラウド(Helion)デバイスからデータを復元するには、以下のいずれかを実行します。

- クラウド(Helion)デバイスからローカルバックアップデバイスにオブジェクトコピーを作成し、ローカルのバックアップデバイスからクライアントを復元します。
- ローカルメディアをリサイクルおよびエクスポートし、クラウド(Helion)デバイスからクライアントに直接復元します。
- 複数のローカルバージョンがある場合でも、復元に使用するクラウド(Helion)デバイスを指定して、クラウド(Helion)デバイスから直接復元する。
- ローカルメディアではなくクラウド(Helion)メディアを優先されるメディアの場所として設定します。メディア位置の優先順位の設定を参照してください。

クラウド(Azure)デバイスについて

Data ProtectorからMicrosoft Azureオブジェクトストアへのバックアップとオブジェクトコピーを可能にするために、新しいクラウドデバイスが使用されます。クラウド(Azure)デバイスは、Azureの資格情報を使用して構成され、データをクラウドに送信します。

前提条件

クラウド(Azure)デバイスポータルの前提条件:

- Microsoft Azureアカウントが必要です。詳しくは、Microsoft Azureポータルを参照してください。
- Microsoft Azureストレージアカウントの作成中にMicrosoft Azureが生成する2つのアクセスキーが必要です。

  アカウントに対して生成された2つのアクセスキーが存在します。資格情報を提供するプロセスの一部として、関連するData Protectorデバイスを作成するときにこれらのキーが必要になります。
- ゲートウェイホストとMicrosoft Azureの間の同期が正しく行われるように、システム時刻を正確に設定する必要があります。

Data Protectorの前提条件:

- Data Protectorの最新のCell Manager、ユーザーインターフェイスクライアント、およびインストールサーバーが、最新の一般パッチリリースバンドルと共に、サポートされるシステムにインストールされていることを確認してください。

  さまざまなアーキテクチャーにHPE Data Protectorをインストールする方法の詳細については、『*HPE Data Protectorインストールガイド*』を参照してください。
- クラウド(Azure)デバイスが有効になるクライアントを含め、クラウド(Azure)ゲートウェイとして使用するWindowsシステムとLinuxシステムに、Data Protector Media AgentまたはNDMP Media Agentコンポーネントをインストールします。手順については、『*HPE Data Protectorインストールガイド*』を参照してください。

  サポートされているオペレーティングシステムのバージョンの詳細なリストについては、https://softwaresupport.hpe.com/manualsにある最新のサポート一覧を参照してください。

  > **注:**

> - Webに接続するためにプロキシーサーバーを構成する必要があるMedia Agentシステムの場合は、omnirc 変数のOB2_CLOUD_DEVICE_PROXY=<proxy_server:port_number>をomnirc ファイルに設定する必要があります。
> - Media Agentには、さまざまなエラー条件を扱うための再試行メカニズムが組み込まれています。そのため、ユーザーの操作が完了するまで時間がかかる場合があります。このような問題は、通常の状況では観察されていません。

制限事項

以下はクラウド(Azure)デバイスの制限です。

- クラウド(Azure)デバイスのオブジェクトコピーは、以下の仕様をサポートします。
  - ソースデバイス: ファイルライブラリデバイスおよびStoreOnceデバイス
  - ファイルシステムバックアップ仕様。
- クラウド(Azure)デバイス内でコンテナーを選択または作成するときには、次の制限事項が適用されます。
  - 各デバイスに1つのコンテナーのみを割り当てることができます。
  - 複数のデバイスで同じコンテナーを使用することはできません。
  - 一度デバイスに割り当てたコンテナーは変更できません。

クラウド(Azure)デバイスのblobサイズ制限

Data Protectorメディアが、データおよびメタデータの1つまたは複数のblobとしてクラウド(Azure)デバイスにアップロードされます。クラウド(Azure)には、195 GBのblobサイズ制限がありますが、Data Protectorメディアにはサイズの上限がありません。ただし、この制限に従うため、1つのData Protectorメディアが複数のblob(それぞれの最大サイズは75 GB)にまたがっても構いません。各blobに格納されるデータの正確な量は、データの圧縮率によって異なります。

推奨事項

以下はクラウド(Azure)デバイスを構成するための推奨事項です。

- ファイルシステムの仕様をバックアップするときには、データソースのローカルのクラウド(Azure)デバイスゲートウェイを使用し、オブジェクトコピー操作中のネットワーク負荷を減らしてください。
- クラウド(Azure)へのオブジェクトコピージョブはデフォルトで暗号化されるため、コピー操作のためのデータを生成する初期バックアップ仕様で暗号化をオフにしておく必要があります。暗号化がオンになっている場合、データは2回暗号化され、余分のCPUリソースが消費されて、オブジェクトコピーデータが圧縮不能になります。その結果、クラウド(Azure)に転送されるデータ量が増え、コピー時間も長くなります。
- データをクラウド(Azure)デバイスにコピーする際に大容量のデータセットを複数のバックアップ仕様に分割し、複数のコピーセッションを並列処理することができます。したがって、全体の帯域幅が増えます。
- クラウドサービスを統合すると、必要な帯域幅が大きくなり、それに関連したコストが発生するので推奨されません。

クラウド(Azure)デバイスの準備

クラウド(Azure)デバイスへのオブジェクトコピー操作を構成するには次の作業を実行する必要があります。

1. ローカルバックアップデバイスにデータをバックアップするためのバックアップ仕様を構成します。詳細については、『バックアップ仕様を作成する、ページ 282』を参照してください。
2. Microsoft Azureポータルにログインして、Microsoft Azureストレージアカウントを使用するために必要なアクセスキーを取得します。
3. Data Protectorでクラウド(Azure)デバイスを構成します。詳細については、ディスクへのバックアップデバイスを構成する - クラウド(Azure)、ページ 178を参照してください。
4. ローカルバックアップデバイスをソースデバイスとして使用し、クラウド(Azure)デバイスをバックアップ先デバイスとして使用して、オブジェクトコピーセッションを構成します。

   クラウド(Azure)デバイスへのオブジェクトのコピーの操作を作成すると、ローカルバックアップデバイスに保存されたデータをクラウド(Azure)デバイスにコピーできるようになります。クラウド(Azure)に送信されたデータはデフォルトで圧縮および暗号化されます。
5. クラウド(Azure)デバイスからデータを復元します。以下のいずれかの方法で復元できます。
   - クラウド(Azure)デバイスからローカルバックアップデバイスにオブジェクトコピーを作成し、ローカルのバックアップデバイスからクライアントを復元します。
   - ローカルメディアをリサイクルおよびエクスポートし、クラウド(Azure)デバイスからクライアントに直接復元します。
   - 複数のローカルバージョンがある場合でも、復元に使用するクラウド(Azure)デバイスを指定して、クラウド(Azure)から直接復元する。
   - ローカルメディアではなくクラウド(Azure)メディアを優先されるメディアの場所として設定します。メディアの位置の優先順位を設定する、ページ 265を参照してください。

デバイスのパフォーマンスチューニング

ブロックサイズ

論理デバイスはすべて、特定のサイズ(ブロックサイズ)単位のデータを処理するよう構成できます。デフォルトのブロックサイズはデバイスによって異なります。そのサイズを使うことはできます(セッションはすべて正常に完了します)が、最適でない可能性があります。ブロックサイズを調整すると、Data Protectorセッションのパフォーマンスを向上させることができます。

最適なブロックサイズの値は、環境によって異なります。

- ハードウェア(デバイス、ブリッジ、スイッチなど)
- ファームウェア
- ソフトウェア(オペレーティングシステム、ドライバー、ファイアウォールなど)

最適な結果を得るには、まず最新のドライバーとファームウェアをインストールして環境を最適化し、ネットワークなどを最適化します。

最適なブロックサイズを特定する

最適なブロックサイズを特定するには、さまざまなブロックサイズ値を使用して通常のData Protectorタスク(バックアップ、復元、コピーなど)をテストし、パフォーマンスを計測します。

> **注:**
> なお、デバイスのブロックサイズを変更すると、そのデバイスでは(古いブロックサイズの)古いバックアップを復元できなくなります。。
>
> そこで、古い論理デバイスとメディアプールを残して古いメディアからデータを復元できるようにしておき、さまざまなブロックサイズ値を持つ新しい論理デバイスとメディアプールをテスト目的で作成します。または、復元を実行するときにブロックサイズの変更方法を確認します。復元ダイアログでブロックサイズを入力するように求められます。

制限事項

- ディザスタリカバリ: オフラインEADR/OBDR復旧(拡張自動ディザスタリカバリ、ワンボタンディザスタリカバリ)を実行できるようにするには、デフォルトのブロックサイズを使用してデータをバックアップしてください。
- ライブラリ: 同じライブラリ内で同様の技術を使った複数のドライブを使用する場合は、ドライブのブロックサイズが同じでなければなりません。
- SCSIアダプター: 選択したブロックサイズが、デバイスの接続先のホストSCSIアダプターでサポートされているかどうかを確認してください。
- オブジェクトコピー機能: あて先デバイスのブロックサイズは、ソースデバイスのブロックサイズ以上でなければなりません。
- オブジェクト集約機能: あて先デバイスのブロックサイズは、ソースデバイスのブロックサイズ以上でなければなりません。
- ミラーリング: デバイスのブロックサイズは、ミラーチェーン内で小さくすることはできません。ミラー1の書き込みに使用するデバイスのブロックサイズは、バックアップに使用するデバイスのブロックサイズ以上でなければなりません。ミラー2の書き込みに使用するデバイスのブロックサイズは、ミラー1の書き込みに使用するデバイスのブロックサイズ以上でなければなりません。以下、同様の関係が続きます。

その他の制限事項については、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。

ブロックサイズを変更する

[拡張オプション]の[サイズ]タブで特定のデバイスのブロックサイズを設定できます。詳細については、「[デバイス/メディア]の拡張オプションを設定する」を参照してください。

デバイスのパフォーマンス

テープに対するデータの読み書きの維持速度はデバイスによって異なります。このため、バックアップと復元のパフォーマンスは、デバイスの種類と機種に依存します。

データ転送速度は、ハードウェア圧縮を使用するかどうかによっても異なります。可能な圧縮率は、バックアップされるデータの性質によって異なります。多くの場合、高速デバイスをハードウェア圧縮オプションをオンにして使用することにより、性能が向上します。ただし、このように性能を向上できるのはデバイスのストリーミングが行われている場合に限ります。

バックアップセッションの開始時と終了時には、バックアップに使用するメディアの巻き戻し、メディアのマウントやアンマウントといった操作のための時間が必要となります。

ライブラリ使用による自動化の利点:バックアップ時には新しいメディアや再使用可能なメディアのロードが必要になり、復元時には復元対象のデータが格納されているメディアにすばやくアクセスする必要がありますが、ライブラリアクセスが自動化されているため、プロセスにかかる時間が短縮されます。

ディスクベースのデバイスの方が、従来のデバイスを使用した場合よりすばやく行えます。ディスクベースのデバイスを使用する場合にはメディアのマウントやマウント解除が不要であるほか、ディスクベースのデバイスに入っているデータには高速でアクセスできるため、バックアップと復元にかかる時間が短縮されます。

新しいデバイスのサポート

『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』にサポート対象と記述されていないデバイスを使用するには、`scsitab`ファイルを使用します。

`scsitab` ファイルは、HPE Data Protector Support Matrixのマシンで読み取り可能な形式であり、すべてのサポートされるデバイスに関する情報が含まれています。`scsitab`ファイルは、HPE Data Protector Media Agentによって、特定のデバイスまたはライブラリがサポートされるかどうかを判断するために使用されます。さらに、デバイスおよびデバイスの特定のパラメーターに関する情報も提供します。

> **重要:**
> `scsitab`ファイルを修正して使用することはできません。

『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』にサポート対象として記載されていないデバイスを使用するには、HPE Data Protector Webサイト(http://www.hpe.com/software/dataprotector)から`scsitab`ファイルの最新ソフトウェアパッケージをダウンロードしてください。

`scsitab`ソフトウェアパッケージをダウンロードした後、ソフトウェアパッケージに含まれているインストールプログラムの指示に従ってください。

`scsitab`ファイルは、デバイスの接続先のシステムにインストールされます。インストール場所は、以下のとおりです。

Windowsシステムの場合: *`Data_Protector_home`*`\scsitab`

HP-UXシステム、Solarisシステム、Linuxシステムの場合: `/opt/omni/scsitab`

その他のUNIXシステムの場合: `/usr/omni/scsitab`

デバイスの構成中に同じエラーが発生する場合は、HPEサポート窓口に連絡して、デバイスのサポート予定時期をご確認ください。

バックアップデバイスを準備する

バックアップデバイスを準備するには、デバイスをシステムに接続し(SAN環境の場合はSANに接続し)、関連付けられているデバイスファイル(SCSIアドレス)のどれを使用するかを確認します。

前提条件

Media Agent (General Media AgentまたはNDMP Media Agent)が、バックアップデバイスが接続されている各システム(SAN環境の場合はSAN上のバックアップデバイスを制御するシステム)にインストールされていること。

手順

1. コンピューターシステム(SAN環境の場合はSAN)にバックアップデバイスを接続します。
2. 以下のように操作を続行します。

   Windowsシステムの場合:

   Windowsシステムに接続されているデバイスについて、SCSIアドレス構文を指定します。

   UNIXシステムの場合:

   UNIXシステムに接続されているデバイスについて、デバイスファイル名を検索するかデバイスファイルを作成します。
3. 同じメディアを複数のデバイスで使用する予定の場合は、書き込み密度とブロックサイズの設定が同じであることを確認します。
4. システムをブートし、システムにデバイスを認識させます。
5. 一部のバックアップデバイスでは、さらに他の操作が必要になります。

バックアップデバイスを準備したら、Data Protectorで使用できるように構成します。バックアップで使用するメディアを準備します。

- SAN環境の場合
- ファイルデバイス
- マガジン
- SCSIライブラリ、ジュークボックス、外部制御
- Windowsのロボティクスドライバー

SAN環境の場合

手順

1. 共有ライブラリへのアクセスが必要なすべてのシステムに同じロボティクスデバイスファイル名が存在することを確認します。ライブラリに間接的にアクセスする場合には、この必要はありません。

   HP-UXおよびSolarisシステムの場合:

デバイスファイルの識別条件を満足できるように、必要に応じてハードリンクまたはソフトリンクを設定します。

Windowsシステムの場合:

テキストファイル`libtab`を使用して、デフォルトのSCSIデバイスIDを置き換え、他のホスト上で定義されている論理ドライブにロボティクス制御デバイスを再割り当てする必要があります。

テキストファイル`libtab`は、Media Agentクライアント上で、*`Data_Protector_home`* ディレクトリに作成する必要があります。このファイルには、次の構文のエントリを記述します。論理ドライブ名には空白文字を使用できます。

`hostnamecontrol_device_filedevice_name`

例:

```
computer.company.com scsi2:0:4:0 DLT_1
```

ファイルデバイス

デバイスとして使用するファイルのWindows圧縮オプションを無効にします。この操作は、Windowsエクスプローラーを使用して実行できます。

手順

1. ファイルを右クリックし、**[プロパティ]**をクリックして、**[属性]**の**[圧縮]**オプションをオフにします。

マガジン

手順

1. マガジンデバイスを構成する前に、マガジンをサポートするメディアプールを作成します。デバイスとしては、マガジンサポート付きのもの(HPE12000eなど)を使用する必要があります。

SCSIライブラリ、ジュークボックス、外部制御

手順

1. ライブラリ内のどのスロットをData Protectorに使用するかを決定します。使用するスロットは、ライブラリの構成時に指定する必要があります。

Windowsのロボティクスドライバー

Windowsシステムでは、テープライブラリを有効にすると、対応するロボティクスドライバーが自動的にロードされます。WindowsシステムでData Protectorがライブラリロボティクスを使用できるようにするには、対応するWindowsドライバーを無効にする必要があります。

手順

1. [コントロールパネル]で、**[管理ツール]**をダブルクリックします。
2. **[コンピューターの管理]**をダブルクリックし、**[デバイスマネージャー]**をクリックします。
3. **[メディアチェンジャー]**を展開します。
4. メディアチェンジャーを右クリックし、**[無効化]**を選択します。
5. システムを再起動して変更を適用します。これで、ロボティクスをData Protector用に構成する準備ができました。

Windowsシステム上でSCSIアドレスを作成する

SCSIアドレス構文は、Windowsシステムに接続されている物理デバイスが光磁気デバイスとテープのどちらであるかによって異なります。システムをブートする前に、デバイスをシステムに接続し、デバイスの電源を入れておく必要があります。

> **ヒント:**
> Data Protectorには、SCSIアドレスを自動検出する機能があります。

光磁気デバイス

システムに光磁気デバイスが接続されている場合のSCSIアドレス構文は、`N:B:T:P:L`となります。ここで、`N`には、取り外し可能メディアドライブのマウントポイントを指定し、`B`にはバス番号、`T`にはSCSIターゲットID、`P`にはパス、`L`にはLUNを指定します。

[コントロールパネル]で**[SCSIアダプター]**を開き、目的のデバイスの名前をダブルクリックします。次に、**[設定]**をクリックして、デバイスのプロパティページを開きます。必要な情報がすべて表示されます。

テープデバイス

システムにテープデバイスが接続されている場合のSCSIアドレス構文は、ネイティブテープドライバーがロードされているかアンロードされているかによって異なります。また、システムによってもアドレス構文に違いがあります。ターゲットSCSIアドレスの作成方法については、下記のトピックを参照してください。

Windowsでネイティブテープドライバーを使用していない場合

Windowsでネイティブテープドライバーを使用している場合

Windowsでネイティブテープドライバーを使用していない場合

ネイティブテープドライバーがアンロードされている場合のSCSIアドレス構文は、`P:B:T:L`となります。ここで、`P`にはSCSIポート番号を指定し、`B`にはバス番号、`T`にはSCSIターゲットID、`L`にはLUNを指定します。接続されているテープドライブのプロパティページを開くと、これらの情報を確認できます。

[コントロールパネル]で**[SCSIアダプター]**を開き、目的のデバイスの名前をダブルクリックします。次に、**[設定]**をクリックして、デバイスのプロパティページを開きます。必要な情報がすべて表示されます。

Windowsでネイティブテープドライバーを使用している場合

ネイティブテープドライバーがロードされている場合のSCSIアドレス構文は、tapeNです。ここで、Nには、ドライブのインスタンス番号を指定します。テープドライブファイルを作成するには、ドライブのインスタンス番号が必要です。たとえば、Nにtape0を指定すると、ファイル0が作成されます。

手順

1. Windowsのコントロールパネルで、**[管理ツール]**をダブルクリックします。
2. [管理ツール]ウィンドウで、**[コンピューターの管理]**をダブルクリックします。**[リムーバブル記憶域]**と**[物理的な場所]**を順に展開します。
3. テープドライブを右クリックし、**[プロパティ]**を選択します。

   ネイティブテープドライバーがロードされていれば、[一般]プロパティページにデバイスファイル名が表示されます。ロードされていない場合は、[デバイス情報]プロパティページで、関連する情報を確認できます。

UNIXシステム上でデバイスファイル名を検索する

UNIXシステムに接続されているデバイスを構成するには、デバイスファイル名を把握している必要があります。

デバイスファイルが自動的に作成されるかどうかは、UNIXオペレーティングシステムのベンダーによって異なります。HP-UXプラットフォームおよびSolarisプラットフォーム上のデバイスについては、以降の節を参照してください。他のUNIXプラットフォーム上のデバイスの場合は、ベンダーに問い合わせてください。

HP-UX上でデバイスファイル名を検索する

前提条件

/usr/sbin/ioscan -fコマンドを使って、デバイスが適切に接続されているかどうかを確認しておきます。

手順

1. HP-UXシステム上で**System Administration Manager (SAM)**アプリケーションを起動します。
2. **[Peripheral Devices]**をクリックし、**[Tape Drives]**をクリックします。
3. ターゲットデバイスをクリックします。
4. [Actions]メニューで**[Show Device Files]**をクリックします。デバイスファイル名が表示されます。
   *BESTという構文のデバイスファイルを使用してください。非巻き戻しデバイスの場合、'BESTn'という構文のデバイスファイルを使用してください。

デバイスファイル名が何も表示されなかった場合は、デバイスファイルを作成する必要があります。

Solaris上でデバイスファイル名を検索する

手順

1. **[Stop]** + **[A]**キーを押してクライアントシステムを停止します。
2. okプロンプトでprobe-scsi-allコマンドを使って、デバイスが適切に接続されているかどうかを確認しておきます。

   これにより、接続したSCSIデバイスに関する情報(接続したバックアップデバイスの正しいデバイスID文字列など)が取得されます。
3. okプロンプトにgoと入力して、通常の動作モードに戻ります。
4. /drv/rmtディレクトリの内容と、マルチドライブライブラリを使用している場合は/drvディレクトリの内容をリストします。
   - /drv/rmtディレクトリには、バックアップデバイスのドライブのデバイスファイル名がリストされます。
   - /drvディレクトリには、マルチドライブライブラリデバイスを使用している場合にロボティクスのデバイスファイル名がリストされます。

デバイスファイル名が何も表示されなかった場合は、デバイスファイルを作成する必要があります。

デバイスファイルの詳細は、『*HPE Data Protectorインストールガイド*』を参照してください。

UNIXシステム上でデバイスファイルを作成する

システムの初期化(ブートプロセス)中に特定のバックアップデバイスに対応するデバイスファイルが作成されなかった場合は、デバイスファイルを手動で作成する必要があります。ライブラリ制御デバイス(ライブラリロボティクス)の管理に必要なデバイスファイルがこれに該当します。

デバイスファイルが自動的に作成されるかどうかは、UNIXオペレーティングシステムのベンダーによって異なります。HP-UXプラットフォームおよびSolarisプラットフォーム上のデバイスについては、以降の節を参照してください。他のUNIXプラットフォーム上のデバイスの場合は、ベンダーに問い合わせてください。

HP-UXシステム上でデバイスファイルを作成する

前提条件

- /usr/sbin/ioscan -fコマンドを使って、デバイスが適切に接続されているかどうかを確認しておきます。

手順

1. HP-UXシステム上で**System Administration Manager (SAM)**アプリケーションを起動します。
2. **[Peripheral Devices]**をクリックし、**[Tape Drives]**をクリックします。
3. ターゲットデバイスをクリックします。

4. [Action]メニューの**[Create Device Files]**をクリックし、**[Create Default Device Files]**をクリックします。

Solarisシステム上でデバイスファイルを作成する

前提条件

- Solarisクライアント上で新しいバックアップデバイスを使用する前に、クライアントのデバイス/ドライバー構成ファイルを更新し、別のドライバーをインストールして(ライブラリデバイスを使用する場合のみ)、クライアント用の新しいデバイスファイルを作成しておく必要があります。

手順

1. **[Stop]** + **[A]**キーを押してクライアントシステムを停止します。
2. okプロンプトからprobe-scsi-allコマンドを実行して、クライアントシステム上の使用可能なSCSIアドレスをチェックし、接続するデバイスのアドレスを選択します(単一ドライブデバイスの場合のみ)。マルチドライブデバイスの場合は、各ドライブのSCSIアドレスとロボティックメカニズム用のSCSIアドレスを個別に選択する必要があります。
3. okプロンプトにgoと入力して、通常の動作モードに戻ります。
4. クライアントシステムをシャットダウンし、電源を切ります。
5. 選択したSCSIアドレスをバックアップデバイス上で設定します。
6. SCSIデバイスをクライアントシステムに接続するときは、必要に応じてシステムをシャットダウンし、電源を切ります。
7. デバイスをクライアントシステムに接続します。
8. 最初にバックアップデバイスの電源を投入した後、クライアントシステムの電源を投入します(前の手順で電源を切った場合)。
9. **[Stop]** + **[A]**キーを押してシステムを再度停止します。
10. okコマンドプロンプトで、probe-scsi-allコマンドを実行します。

    これにより、接続したSCSIデバイスに関する情報(新たに接続したバックアップデバイスの正しいデバイスID文字列など)が取得されます。
11. okプロンプトにgoと入力して、通常の動作モードに戻ります。
12. 構成ファイルst.confを編集し、必要なデバイス情報とドライブのSCSIアドレスを追加します。

    詳細は、『*HPE Data Protectorインストールガイド*』を参照してください。
13. ロボティクスメカニズムを備えたマルチドライブデバイスを接続する場合は、以下の手順も実施する必要があります。詳細は、『*HPE Data Protectorインストールガイド*』を参照してください。
    a. sstドライバーをクライアントにコピーしてインストールします。
    b. 構成ファイルst.conf(Solaris 8または9)またはsgen.conf(Solaris 10)を目的のクライアントシステムにコピーして編集し、ロボティックメカニズムに関するエントリを追加します。
    c. /etc/devlink.tabファイルを編集し、ロボティックメカニズムデバイスファイルのエントリを追加します。
14. ドライバーと構成ファイルを必要に応じて更新し終えたら、クライアントシステム用の新しいデバイスファイルを作成します。

a. `/drv/mnt/`ディレクトリから既存のデバイスファイルをすべて削除します。
b. `shutdown -i0 -g0`コマンドを実行して、システムをシャットダウンします。
c. `boot -rv`コマンドを実行して、システムを再起動します。
d. 再ブートが完了したら、`/dev`ディレクトリの内容をチェックし、デバイスファイルが作成されていることを確認します。ロボティックメカニズム用のデバイスファイルは`/dev`ディレクトリに、ドライブ用のデバイスファイルは`/dev/rmt`ディレクトリにある必要があります。

デバイスファイル名およびSCSIアドレスを自動検出する

Windows、HP-UX、およびSolarisの各プラットフォームに接続されたデバイスのデバイスファイル名(SCSIアドレス)は、ほとんどの場合、自動検出が可能です。

既存のData Protectorデバイス定義を変更する場合

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**をクリックします。構成されているデバイスのリストが[結果エリア]に表示されます。
3. [結果エリア]で、目的のデバイスを右クリックして**[プロパティ]**をクリックします。
4. **[ドライブ]**タブをクリックします。
5. ドロップダウンリストを使用して、デバイスのSCSIアドレス(デバイスファイル名)を自動検出します。

新しいData Protectorデバイス定義を作成する場合

手順

1. デバイスの構成手順に従います。
2. ウィザード画面に対してデバイスファイル名(SCSIアドレス)を指定するときに、ドロップダウンリストから利用可能なデバイスのいずれかを選択します。

デバイスファイル名およびライブラリ用SCSIアドレスを自動検出する

Windows、HP-UX、およびSolarisの各プラットフォームに接続されたライブラリロボティクスのデバイスファイル名(SCSIアドレス)は、自動検出が可能です。

構成済みのライブラリの場合

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**をクリックします。構成されているデバイスのリストが[結果エリア]に表示されます。
3. [結果エリア]で、目的のライブラリを右クリックして**[プロパティ]**をクリックします。
4. **[コントロール]**タブをクリックします。
5. [ライブラリロボティクスのSCSIアドレス]エリアで、ドロップダウンリストからライブラリロボティクス用に利用可能なファイル名(SCSIアドレス)のいずれかを選択します。

ライブラリを構成中の場合

手順

1. 構成手順に従ってライブラリロボティクスを構成します。
2. ウィザード画面でSCSIアドレス(ファイル名)を指定するときに、ドロップダウンリストからライブラリロボティクス用に利用可能なファイル名(SCSIアドレス)のいずれかを選択します。

バックアップデバイスの構成について

準備作業を完了したら、Data Protectorで使用するバックアップデバイスを構成することができます。

バックアップデバイスの構成には、Data Protectorの自動構成機能を使用することをお勧めします。Data Protectorでは、代表的なバックアップデバイスやライブラリのほとんどを自動的に構成することができます。バックアップセッションに合わせてメディアを準備する必要はありますが、Data Protectorによって、ポリシー、メディアの種類、メディアポリシー、デバイスファイルまたはデバイスのSCSIアドレスが決定され、ドライブとスロットも構成されます。

バックアップデバイスは手動で構成することもできます。バックアップデバイスの構成方法は、デバイスの種類によって異なります。

『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』にサポート対象と記述されていないデバイスも、使用できます。サポートされていないデバイスは、`scsitab`ファイルを使用して構成します。

ライブラリ管理コンソールについて

ライブラリ管理コンソールとは

最近のテープライブラリの多くは、リモートライブラリの構成、管理、および監視タスクを実行する機能を提供する統合管理コンソールを備えています。ライブラリ管理コンソールは、ライブラリへのWebインターフェイスで、通常のWebページと同じようにWebブラウザーに表示されます。このようなWebコンソールを備え

たテープライブラリを使用すると、任意のリモートシステムからさまざまなタスクを実行できます。たとえば、ライブラリ構成パラメーターの設定、ライブラリドライブへのテープのロード、現在のライブラリステータスのチェックなどの操作を実行できます。リモートで実行可能なタスクの範囲は管理コンソールの実装によって異なり、Data Protectorには依存しません。

ライブラリ管理コンソールは、それぞれに独自のURL (Webアドレス)を持っています。これが管理コンソールインターフェイスへのエントリポイントになります。コンソールインターフェイスにアクセスするには、Webブラウザーのアドレスバーにこの URLを入力します。

Data Protectorでのライブラリ管理コンソールのサポート

ライブラリ構成には、ライブラリ管理コンソールのURLを表すパラメーターが含まれます。**[管理コンソールのURL]**を、ライブラリの構成プロセスまたは再構成プロセスの最中に指定できます。

管理コンソールインターフェイスへのアクセスは、拡張されたData Protector GUI機能によって簡単になります。Data Protector GUIからWebブラウザーを起動し、コンソールインターフェイスをロードできます。オペレーティングシステムに応じて、システムのデフォルトWebブラウザー(Windowsシステム)またはData Protector構成で指定したWebブラウザー(UNIXシステム)が使用されます。

> **重要:**
> ライブラリ管理コンソールを使用する際には、コンソールで実行可能な操作の一部によって、メディア管理操作、バックアップセッション、復元セッションなどに影響が出る可能性があることに注意ください。

制限事項

管理コンソールURLに空白文字や二重引用符を含めることはサポートされていません。URLセーフコードを入力してください。下表に、サポートされていない文字とそのURLセーフコードを示します。

文字	URLセーフコード
空白文字	%20
二重引用符(")	%22

バックアップデバイスを自動構成する

バックアップデバイスを構成対象のシステムに接続し、デバイスファイル(SCSIアドレス)が存在することを確認したら、そのデバイスをData Protectorで使用できるように構成することができます。自動構成では、デバイス定義が自動的に作成されます。Data Protector

Data Protectorでは、SAN内の1つまたは複数のシステムに接続されている代表的なバックアップデバイスのほとんどを自動的に検出して構成することができます。このように自動構成されたデバイスのプロパティは、後で実際のニーズに応じて修正することができます。

自動構成は、以下のオペレーティングシステム上でサポートされています。

- Windows
- HP-UX

- Solaris
- Linux

> **注:**
> Removable Storageサービスの実行中にライブラリを自動構成しても、ドライブとロボティクス(エクスチェンジャー)は正しく組み合わせられません。

前提条件

自動構成する各クライアントシステムにはMedia Agentがインストールされている必要があります。

デバイスの自動構成

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を右クリックし、**[デバイスの自動構成]**を選択して、ウィザードを起動します。
3. 構成対象のデバイスを持つクライアントシステムを選択し、**[次へ]**をクリックします。
4. システム上で構成するバックアップデバイスを選択します。**[次へ]**をクリックします。
5. 変更されたSCSIアドレスの自動検出を有効にするには、**[変更されたSCSIアドレスの自動検出]**を選択し、**[完了]**をクリックします。マガジンデバイスについては、自動構成後にメディアプールをマガジンサポート付きのものに変更します。

デバイス名が構成済みデバイスのリストに表示されます。デバイスをスキャンすると、構成を確認できます。

SAN環境でのデバイスの自動構成

Data Protectorでは、複数の異なるクライアントが同じライブラリ内のテープドライブを使用するSAN環境でも、デバイスを自動構成することが可能です。Data Protectorの自動構成機能を使うと、複数のクライアントシステムに対するデバイスとライブラリの構成が自動化されます。

Data Protectorでは、ロック名、ポリシー、メディアの種類、メディアのポリシー、およびデバイスファイルまたはデバイスのSCSIアドレスを識別し、ドライブやスロットを構成します。

> **注:**
> SAN環境に新しいホストを導入した場合、構成済みのライブラリとデバイスは自動的に更新されません。
>
> - 既存のライブラリを新しいホストで使用する場合は、このライブラリを削除し、同じ名前を指定して新しいホスト上で新しいライブラリを自動構成します。
> - 既存のライブラリにデバイスを追加する場合は、ライブラリを削除し、同じ名前を指定して新しいホスト上で新しいライブラリを自動構成するか、またはドライブをライブラリに手動で追加することができます。

制限事項

SAN環境内の以下のデバイスに対しては、自動構成を使用できません。

- 混合メディアライブラリ
- DASライブラリまたはACSLSライブラリ
- NDMPデバイス

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を右クリックし、**[デバイスの自動構成]**を選択して、ウィザードを起動します。
3. 構成するクライアントシステムを選択します。Microsoft Cluster Server環境の場合は、仮想サーバーを選択します。

   [次へ]をクリックします。
4. 構成対象のデバイスとライブラリを選択します。
5. 複数のクライアントに接続されているライブラリを構成する場合は、ライブラリロボティクスを制御するクライアント(制御ホスト)が示されます。ライブラリが接続されているシステムのいずれかがCell Managerであれば、デフォルトでCell Managerが選択されます。以下の2つのビューを交互に切り替えることができます。
   - **デバイスごとにグループ化**

     すべてのデバイスとライブラリのリストが表示されます。ライブラリまたはデバイスを展開すると、構成対象のクライアントシステムを選択することができます。
   - **ホストごとにグループ化**

     デバイスが接続されているクライアントのリストが表示されます。クライアントを展開すると、そのクライアントに接続されているデバイスまたはライブラリを構成することができます。
6. 必要に応じてマルチパスデバイスを有効にするには、**[マルチパスデバイスを自動構成]**を選択します。**[次へ]**をクリックします。
7. 変更されたSCSIアドレスの自動検出を有効にするには、**[変更されたSCSIアドレスの自動検出]**を選択します。
8. **[完了]**をクリックします。構成済みデバイスのリストが表示されます。

デバイスをスキャンすると、構成を確認できます。

スタンドアロンデバイスを構成する

バックアップデバイスをシステムに接続し、デバイスファイル(SCSIアドレス)が存在することを確認したら、そのデバイスをData Protectorで使用できるように構成することができます。

バックアップデバイスの構成には、Data Protectorの自動構成機能を使用することをお勧めします。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックして、ウィザードを起動します。
3. [デバイス名]テキストボックスにデバイスの名前を入力します。
4. [説明]テキストボックスに必要に応じて説明を入力します。
5. 必要に応じて、**[マルチパスデバイス]**を選択します。
6. **[マルチパスデバイス]**オプションを選択*していない*場合は、[クライアント]ドロップダウンリストからクライアント(バックアップシステム)の名前を選択します。
7. [デバイスの種類]リストで、デバイスの種類として**[スタンドアロン]**を選択し、**[次へ]**をクリックします。
8. 物理デバイスのSCSIアドレス(Windowsシステムの場合)またはデバイスファイル名(UNIXシステムの場合)を入力し、**[追加]をクリックします。**

   マルチパスデバイスの場合は、ドロップダウンリストからクライアントを選択し、デバイスのデバイスファイル名を入力します。**[追加]**をクリックして、構成済みパスのリストにパスを追加します。

   > **ヒント:**
   > 複数のアドレスを入力すると、デバイスチェーンを作成できます。
   >
   > デバイスチェーンにデバイスが追加された順番によって、Data Protectorがそれらのデバイスを使用する順番が決まります。
   >
   > デバイスチェーン内のすべてのメディアがいっぱいになると、マウント要求が発行されます。Data Protector最初のデバイス内のメディアを新しいメディアに置き換えて、それをフォーマットしたら、マウント要求を確認してください。Data Protectorは、認識済みで保護されていないメディアをすぐに使うことができます。ブランクメディアも使用できます。

9. 変更されたSCSIアドレスの自動検出を有効にする場合は、**[変更されたSCSIアドレスの自動検出]**を選択します。**[次へ]**をクリックします。
10. 構成するデバイスのメディアの種類を[メディアの種類]リストから選択します。
11. 選択したメディアの種類に対応するメディアプールを指定します。既存のプールを[メディアプール]ドロップダウンリストから選択するか、新しいプール名を入力します。新しいプール名を入力した場合は、プールが自動的に作成されます。
12. **[完了]**をクリックしてウィザードを終了します。

デバイス名が構成済みデバイスのリストに表示されます。デバイスをスキャンすると、構成を確認できます。デバイスが正しく構成されていれば、Data Protectorはメディアのロード、読み込み、スロットへのアンロードができるようになります。

ディスクへのバックアップデバイスを構成する

ディスクへのバックアップ(B2D)デバイスを使用してバックアップを実行する前に、Data Protectorで使用できるようにデバイスを構成する必要があります。使用可能なディスクへのバックアップデバイスは、StoreOnceバックアップシステム、StoreOnceソフトウェア、クラウド(Helion)、クラウド(Azure)、データドメインブースト、およびSmart Cacheです。

マルチインターフェイスサポート

Data Protectorは、マルチインターフェイスをサポートしています。Data Protectorでは、個別にストアを構成する必要はなく、同じCatalyst/DDBoostストアへのIP接続とファイバーチャネル接続をサポートしています。ストアには、両方のインターフェイス経由で同時にアクセスできます。

たとえば、1つのCatalyst/DDBoostストアにローカルクライアントが高速バックアップのためにファイバーチャネル経由でアクセスし、リモートクライアントが低速バックアップのためにWAN経由でアクセスすることができます。

この機能はSolaris環境で使用できず、また重複排除ターゲットの識別子としてFCを構成した場合では使用できません。このオプションはStoreOnceバックアップシステムとDD Boostのみに適用されます。

この機能の動作の詳細については、『*HPE Data Protector Administrator's Guide*』および『*HPE Data Protector Command Line Interface Reference*』を参照してください。

> **重要:**
> StoreOnceデバイスまたはDDBoostデバイスを追加するときは、マルチインターフェイス機能を利用できるようにするために、IPアドレスまたはホスト名を使用することを強く推奨します。

手順

B2Dデバイス(既存のストアをターゲットとする)は、次の手順に従って追加します。

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックして、ウィザードを起動します。
3. デバイスの名前と説明(オプション)を指定します。
4. **ディスクへのバックアップ**デバイスタイプを選択し、**インターフェイスタイプ**として**StoreOnceバックアップシステム**、**データドメインブースト**、**StoreOnceソフトウェア**、**クラウド(Helion)**, **クラウド(Azure)**または**Smart Cache**を選択します。
5. デバイスを構成する手順は、選択したインターフェイスタイプによって異なります。
   - StoreOnceを構成する
   - StoreOnceソフトウェアを構成する
   - データドメインブーストを構成する
   - Smart Cacheを構成する
   - クラウドデバイス(Helion)を構成する
   - クラウドデバイス(Azure)を構成する

B2Dデバイスの追加手順は、デバイスの種類を追加する手順とほぼ同じです。また、StoreOnceソフトウェア重複排除デバイスに対しては、ルートディレクトリを構成してからストアを作成してください(「ディスクへのバックアップデバイスを構成する - StoreOnceソフトウェア」を参照してください)。

ディスクへのバックアップデバイスを構成する - StoreOnce

ディスクへのバックアップ(B2D)デバイスを使用してバックアップを実行する前に、Data Protectorで使用できるようにデバイスを構成する必要があります。

StoreOnceソフトウェア重複排除デバイスの構成には、さらに手順が必要です。「ディスクへのバックアップデバイスを構成する - StoreOnceソフトウェア」を参照してください。

> **注:**
> HPE Data Protectorは、最大8個のメンバーのフェデレーションストアをサポートします。ストアのメンバーの数はStoreOnceで変更できます。この変更を反映するには、HPE Data Protector GUIまたはCLIを使用して、HPE Data Protectorキャッシュを手動で更新します。詳細については、「ストアのキャッシュを更新する」を参照してください。フェデレーションストアが機能するには、すべてのフェデレーションメンバーがオンラインになっている必要があります。

手順

StoreOnceバックアップシステムまたはStoreOnceソフトウェアB2Dデバイス(既存のストアをターゲットとする)は、次の手順に従って追加します。

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックして、ウィザードを起動します。
3. デバイスの名前と説明(オプション)を指定します。
4. **ディスクへのバックアップ**デバイスタイプを選択し、インターフェイスタイプとして**StoreOnceバックアップシステム**または**StoreOnceソフトウェア**を選択します。
5. 必要に応じて、デバイス管理コンソールの有効なURLを**[管理コンソールのURL]**テキストボックスに入力します。**[次へ]**をクリックします。
6. StoreOnceバックアップシステムデバイスでは、**[クライアントID]**を入力して、オプションでストアにアクセスする際に使用するパスワードを入力します。パスワードには次の文字を使用できます。[a-z][A-Z][0-9][_-.+()&{}:#$*;=?@[]^|~]?
7. **[重複排除システム]**ボックスに、重複排除システム(重複排除ストアが置かれているホストマシン)のIPアドレス、ホスト名、完全修飾ドメイン名(FQDN)、またはファイバーチャネル(FC)アドレスを入力します。

   または、**[サービスセットを選択]**をクリックして、重複排除システムのアドレスを照会および取得します。

   > **注:**
   > StoreOnceソフトウェアインターフェイスの場合は、IPv4アドレスかIPv6アドレス、またはFQDNがサポートされます。ただし、StoreOnceバックアップシステムインターフェイスの場合、最新バージョンのStoreOnce Catalystを使用していれば、IPv4またはIPv6アドレス、FQDN、またはFCグローバルIDがサポートされます。
   >
   > FCを使用してStoreOnceバックアップシステムに接続している場合は、デバイスのFCアドレスを指定します。FCデバイスに接続されているMedia Agentまたはゲートウェイを使用し、それらがStoreOnceバックアップシステムデバイスと同じゾーンに置かれていることを確認してください。

8. **[ストアの選択/作成]**ボタンをクリックし、既存のフェデレーションストアまたは非フェデレーションストアを

選択するか、非フェデレーションストアを作成します。ストア名をリストから選択

暗号化ストアを作成するには、**[暗号化ストア]**オプションを選択します。**[OK]**をクリックします。

> **注:** 暗号化はストアの作成時にのみ有効にできます。ストアを作成すると、暗号化状態から暗号化されていない状態(またはその逆)にストアを変換できません。StoreOnceソフトウェア重複排除デバイスは、ストアの暗号化をサポートしていません。
> Data Protector GUIを使用してフェデレーションストアを作成することはできません。
> StoreOnce管理コンソールを使用してそれらを作成する必要があります。

9. 必要に応じて**[ソース側重複排除]**を選択し、ソース側重複排除を有効にします。ソース側重複排除のプロパティウィンドウが表示されます。重複排除のプロパティを確認し、必要に応じて変更します。デフォルトのソース側ゲートウェイ名は「`DeviceName_Source_side`」です。各デバイスには、ソース側ゲートウェイを1つだけ作成できます。この(仮想)ゲートウェイは、バックアップ仕様でソース側重複排除が有効になっている場合、バックアップ済みシステム上で自動的に拡張されます。

> **注:**
> フェデレーションストアの場合、すべての書き込み操作は低帯域幅モード(サーバー側重複排除)で実行されます。ゲートウェイがターゲット側重複排除(高帯域幅モード)として構成されている場合でも、自動的に低帯域幅モードに切り替わります。

10. ゲートウェイを選択し、**[追加]**をクリックしてプロパティダイアログを表示します。必要に応じてゲートウェイのプロパティを変更し、**[OK]**をクリックしてゲートウェイを追加します。FCを使用してStoreOnce Backupシステムに接続している場合は、FCデバイスに接続されているMedia Agentまたはゲートウェイを使用し、それらがStoreOnceバックアップシステムデバイスと同じゾーンに置かれていることを確認してください。

> **注:**
> HPE Data Protectorゲートウェイに接続されるフェデレーションメンバーは、フェデレーションストアのメンバーになっている必要があります。フェデレーションメンバーがStoreOnceを使用しない契約になっている場合は、「ストアのキャッシュを更新する」に記載されている手順を使用して、HPE Data Protectorゲートウェイを調整し、異なるフェデレーションメンバーに接続します。

ゲートウェイのプロパティを表示するには、目的のゲートウェイを選択して、**[プロパティ]**をクリックします。その他のゲートウェイオプションを設定する場合は、**[設定]**タブをクリックし、**[拡張]**をクリックして[拡張プロパティ]ウィンドウを開きます。

[拡張プロパティ]ウィンドウで、各ゲートウェイのストリーム数を制限するには、**[ゲートウェイごとの並列ストリームの最大数]**を選択します。最大100のストリームを指定できます。このオプションを選択しなかった場合、ストリーム数は制限されません。このオプションはバックアップ仕様の作成時に設定することもできますが、この場合、B2Dデバイスの作成中に指定した値は上書きされるので注意してください。

ゲートウェイが使用するネットワーク帯域幅を制限するには、**[ゲートウェイネットワーク帯域幅の制限(kbps)]**を選択して、制限値(kbps)を入力します。

ソース側重複排除を有効にするには、**[サーバー側重複排除]**を選択します。

重複排除ターゲットとしてIPアドレスまたはFQDNを構成した場合は、**[FUを使用]**と**[IPにフォールバック]**オプションが使用できます。これらはデフォルトで選択されています。

11. 接続を検証するには、**[チェック]**をクリックします。
12. **[次へ]**をクリックして、設定ウィンドウを表示します。ここでは、次のオプション指定できます。

- ストアごとの最大接続数(M)
- バックアップサイズのソフトクォータ(GB)
- ストアサイズのソフトクォータ(GB)
- **Catalystアイテムサイズのしきい値(GB)**: StoreOnceソフトウェア重複排除およびStoreOnceバックアップシステムデバイスのCatalystアイテムのサイズのしきい値を定義します。このサイズを超えると、オブジェクトは現在のCatalystアイテムに追加されません。デフォルトでは、Catalystアイテムサイズは無制限になっています。
- **Catalystアイテムごとのシングルオブジェクト**: StoreOnceソフトウェア重複排除およびStoreOnceバックアップシステムデバイスのCatalystアイテムごとに1つのオブジェクトを有効にする場合に選択します。

13. **[次へ]**をクリックして、構成済みのB2Dストアの詳細が含まれるサマリーウィンドウを表示します。フェデレーションストアについては、すべてのフェデレーションメンバーとそれらのステータス(オンラインまたはオフライン)のリストも含まれています。
14. 設定を確認して、**[完了]**をクリックします。新しく構成されたB2DデバイスがScopingペインに表示されます。

ストアのキャッシュを更新する

StoreOnce 3.12では、フェデレーションストアのフェデレーションメンバーを追加または削除できます。この変更を反映するには、HPE Data Protector GUIまたはCLIを使用して、HPE Data Protectorキャッシュを手動で更新します。

HPE Data Protector GUIを使用してキャッシュを更新する

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[デバイス]**を展開します。
3. 目的のStoreOnceデバイスを右クリックし、**[プロパティ]**をクリックします。
4. **[ストアおよびゲートウェイ]**タブをクリックして**[ストアの選択/作成]**をクリックします。必要な場合は、現在アクティブなフェデレーションメンバーのアドレスが含まれるようにディレクトリパスを変更します。
5. StoreOnceデバイスに関連付けられている同じストアを選択し、**[OK]**をクリックします。
6. **[適用]**をクリックします。

HPE Data Protector GLIを使用してキャッシュを更新する

1. 次のコマンドを実行します。

   ```
   omnidownload -library <DPDeviceName> -file <DPDeviceOutputFile>
   ```

2. `DPDeviceOutputFile`を編集します。

   デバイスがフェデレーションではない場合は、次の行を削除します。

   ```
   B2DTEAMEDSTORE 1
   B2DTEAMEDMEMBERS
   "<teamed.device.one>"
   ```

```
"<teamed.device.two>"
...
```

デバイスがフェデレーションである場合は、適切なチーミングされたデバイスのIPアドレスを置き換えた後で、これらの行を`DPDeviceOutputFile`に追加します。必要な場合は、現在アクティブなフェデレーションメンバーのアドレスが含まれるようにディレクトリパスを変更します。

> **注: 注:** アドレスとフォーマットはStoreOnceチーミングポリシーファイル内と正確に一致している必要があります。たとえば、チーミングポリシーファイルにIPv6アドレスが含まれている場合、このファイルにも同じアドレスを追加する必要があります。

3. 次のコマンドを使用して変更されたファイルを保存します。

```
omniupload -modify_library <DPDeviceName> -file <DPDeviceOutputFile>
```

これらのコマンドの詳細については、『*HPE Data Protector Command Line Interface Reference*』を参照してください。

ディスクへのバックアップデバイスを構成する - StoreOnceソフトウェア

StoreOnceソフトウェア重複排除デバイスの構成には、さらに手順が必要です。

- 重複排除ストアのルートディレクトリの構成
- ストアの作成

重複排除ストアのルートディレクトリの構成

ここでは、ストアのルートディレクトリの構成方法について説明します。この操作は、ソフトウェアのインストール後、最初の重複排除ストアを作成する前に行ってください。

1つのStoreOnceソフトウェア重複排除システムに複数の重複排除ストアをホストできます。この場合、ストアは同じルートディレクトリを共有します。個々のストアは他のストアとは独立して作動します。つまり、重複排除は1つのストア内で行われ、各ストアには独自のインデックステーブルが存在します。すべてのストアは同じプロセスで実行されますが、ストアの開始/停止は個別に行えます(ただし、ストアを物理的に開始/停止するわけでありません。詳細については「*Deduplication, White Paper - Appendix A: StoreOnceSoftware utility*」を参照してください)。ストアでの操作は停止(オフライン)時には行えません。

ルートディレクトリを共有するストアは物理的に分離することはできません。この設計により、すべてのディスクへのロードを確実に均一化し、優れたパフォーマンスを実現しています。

インストールが正常に終了すると、StoreOnceSoftwareユーティリティが起動します。この段階では、ユーティリティは実行されていますが、ストアのルートディレクトリが構成されるのを待っている状態です。ルートディレクトリを構成するまで、B2Dデバイスを追加して、ストアを作成することはできません。

ストアのルートディレクトリは、以下の方法で構成できます。

- GUI: デバイスの追加手順に従い、プロンプトに応じてルートディレクトリを指定します(詳細は下記を参照)。
- CLI: StoreOnceSoftware --configure_store_rootコマンドを使用します(詳しくは「*Deduplication White Paper - Appendix A: StoreOnceSoftware utility*」を参照)。

> **注: 注記**: ルートディレクトリは(サーバー上に)先に構成しておく必要があり、設定には書き込み権限が必要です。これは、(GUIによる)構成プロセスでルートディレクトリの場所の指定が求められるためです。

GUIを使用したルートディレクトリの構成手順は、ストアの作成手順と似ていますが、いくつか追加の手順が必要になります。ルートディレクトリを一度構成すると、これらの追加手順は不要になります。ルートディレクトリは、次の手順に従って構成(同時にストアを作成)します。

1. デバイスの追加手順に従います。
   a. [デバイス/メディア]コンテキストで、**[デバイス]**を右クリックして**[デバイスの追加]**をクリックします。
   b. デバイス名を指定し、説明を追加してから、デバイスの種類として**[ディスクへのバックアップ]**を選択し、**[StoreOnceソフトウェア重複排除]**インターフェイスを選択します。
   c. 必要に応じて、デバイス管理コンソールの有効なURLを**[管理コンソールのURL]**テキストボックスに入力します。
   d. **[次へ]**をクリックして、ストアとゲートウェイ一覧を指定する画面を表示します。
   e. StoreOnceバックアップシステムデバイスでは、**[クライアントID]**を入力して、オプションでストアにアクセスする際に使用する**パスワード**を入力します。
2. [重複排除システム]ボックスに、重複排除ストアが置かれているホストマシンのホスト名、IPアドレス、または完全修飾ドメイン名(FQDN)を入力します。
3. ゲートウェイを選択し、**[追加]**をクリックしてプロパティダイアログを表示し、**[OK]**をクリックしてゲートウェイを追加します。
4. **[チェック]**をクリックします。「ルートディレクトリが構成されていません」というメッセージが表示されます。
5. ダイアログで、すべてのストアが存在するルートディレクトリのパス(C:\Volumes\StoreOnceRootなど)を指定し、**[OK]**をクリックします(注記: 有効なルートディレクトリのブラウズは行えません)。
6. ルートディレクトリが存在する場合は、ダイアログが閉じてデバイス設定が継続します。また、StoreOnceSoftwareユーティリティによって、指定したルートディレクトリ内にサブディレクトリ(ストア)が作成されます。ルートディレクトリが存在しない場合は、エラーメッセージが表示されます。
7. デバイスの追加手順を続行します。

ルートディレクトリの構成時およびストアの作成時には、次の点に注意してください。

- オペレーティングシステム(OS)がインストールされているディスクは使用しないでください。
- 専用のストレージディスクを使用してください。
- Data Protectorがサポートするストアはボリュームあたり最大32です。

> **注:** Windowsシステム上では、パフォーマンスを向上させるため、ストアのルートが存在するNTFSボリュームで以下のオプションを適用してください。
> 次のコマンドで、ボリューム上での(DOSのような)ショートファイル名の作成を無効にします。
> `fsutil behavior set Disable8dot3 Volume 1`
> 次のコマンドで、NTFSの内部ログファイルの容量を増やします。`Chkdsk Volume /L:131072`

ストアの作成

ストアを作成する前に、ストアのルートディレクトリが構成されていること、および物理ストレージディスク(LUNデバイス)がフォーマットされてStoreOnceソフトウェア重複排除システムにマウントされていることを確認してください。LUNデバイスは、ローカルディスク、ディスクアレイ(SCSIまたはファイバーチャネルインターフェイス)、または同一LAN内のNASデバイス(iSCSIインターフェイス)上に構成できます。iSCSIインター

フェイスを使用する場合は、待ち時間が最大2msでスループットが最低1Gbit/sの安定したネットワーク接続が必要です。

ストアは、以下の方法で作成できます。

- GUI: デバイスの追加手順に従い、プロンプトに応じてストア名を指定します(詳細は下記を参照)。
- CLI: StoreOnceSoftware --create_storeコマンドを使用します(詳しくは「*Deduplication White Paper - Appendix A: StoreOnceSoftware utility*」を参照)。

ストアの作成手順はデバイスの追加手順と似ていますが、いくつか追加の手順が必要になります。次の手順に従ってストアを作成してください。

1. デバイスの追加手順に従います。
   a. [デバイス/メディア]コンテキストで、**[デバイス]**を右クリックして**[デバイスの追加]**をクリックします。
   b. デバイス名を指定し、説明を追加してから、デバイスの種類として**[ディスクへのバックアップ]**を選択し、**[StoreOnceソフトウェア重複排除]**インターフェイスを選択します。
   c. **[次へ]**をクリックして、ストアとゲートウェイ一覧を指定する画面を表示します。
2. [重複排除システム]を選択し、ストア名を指定します。ストア名の最大文字数は80文字(英数字のみ)です。
   a. ゲートウェイを選択し、**[追加]**をクリックしてプロパティダイアログを表示し、**[OK]**をクリックしてゲートウェイを追加します。
   b. **[チェック]**をクリックして接続を検証します。ストアが存在しない場合は、ストアが作成されます。(注記: **[次へ]**をクリックしても接続の検証が行われます。)
   c. デバイスの追加手順を続行します。

誤ったストア名を指定した場合、GUIでは変更できません。手順を始めからやり直し、正しい名前のストアを作成してください。データを書き込む前の場合は、CLIを使用して誤った名前のストアを削除できます。

ディスクへのバックアップデバイスを構成する - データドメインブースト

ディスクへのバックアップ(B2D)デバイスを使用してバックアップを実行する前に、Data Protectorで使用できるようにデバイスを構成する必要があります。

前提条件

- データドメインデバイス間の複製をサポートするには、データドメインデバイス上で仮想合成を有効にする必要があります。
  - sshを使用して、データドメインデバイスに接続し、次のコマンドを実行します。

    ```
    ddboost option set virtual-synthetics enabled
    ```

- 複製をサポートするには、ソースとターゲットの両方のデバイスで同じ管理者の役割を使用して同じデータドメインブースとユーザーを構成する必要があります。詳細については、データドメインのドキュメントを参照してください。

制限事項

- 対話型の複製を実行する場合は、複製で一度に1つのセッションのみを選択できます。
- [暗号強度]がデフォルト値から変更されている場合、Data Protectorの操作はサポートされません。

> **注:** データドメインブーストデバイスに言及するときは、「ストア」の代わりに「ストレージユニット」という語が使用されます。

手順

DDBoost B2Dデバイス(既存のストアをターゲットとする)は、次の手順に従って追加します。

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックして、ウィザードを起動します。
3. デバイスの名前と説明(オプション)を指定します。
4. **[ディスクへのバックアップ]**デバイスタイプを選択し、**[インターフェイスの種類]**として**[データドメインブースト]**を選択します。
5. 必要に応じて、デバイス管理コンソールの有効なURLを**[管理コンソールのURL]**テキストボックスに入力します。**[次へ]**をクリックします。
6. **ユーザー名**と**パスワード**を入力します。パスワードには次の文字を使用できます。[a-z][A-Z][0-9][_-.+()&{}:#$*;=?@[]^|~]?
7. ストレージユニット名を入力します(この手順はストレージユニットがすでに存在することを前提としています)。
8. **[重複排除システム]**テキストボックスに、重複排除システム(重複排除ストレージユニットが置かれているホストマシン)のホスト名、IPアドレス、またはFCアドレスを入力します。

   > **注:** マルチインターフェイス機能を使用するにはIPアドレスまたはFQDNを使用することを推奨します。この機能の詳細については、マルチインターフェイスサポートを参照してください。

9. 必要に応じて**[ソース側重複排除]**を選択し、ソース側重複排除を有効にします。ソース側重複排除のプロパティウィンドウが表示されます。重複排除のプロパティを確認し、必要に応じて変更します。デフォルトのソース側ゲートウェイ名は「`DeviceName_Source_side`」です。各デバイスには、ソース側ゲートウェイを1つだけ作成できます。この(仮想)ゲートウェイは、バックアップ仕様でソース側重複排除が有効になっている場合、バックアップ済みシステム上で自動的に拡張されます。
10. ゲートウェイを選択し、**[追加]**をクリックしてプロパティダイアログを表示します。必要に応じてゲートウェイのプロパティを変更し、**[OK]**をクリックしてゲートウェイを追加します。

    ゲートウェイのプロパティを表示するには、目的のゲートウェイを選択して、**[プロパティ]**をクリックします。その他のゲートウェイオプションを設定する場合は、**[設定]**タブをクリックし、**[拡張]**をクリックして[拡張プロパティ]ウィンドウを開きます。

    各ゲートウェイのストリーム数を制限するには、**[ゲートウェイごとの並列ストリームの最大数]**を選択します。最大100のストリームを指定できます。このオプションを選択しなかった場合、ストリーム数は制限されません。このオプションはバックアップ仕様の作成時に設定することもできますが、この場合、B2Dデバイスの作成中に指定した値は上書きされるので注意してください。

    ゲートウェイが使用するネットワーク帯域幅を制限するには、**[ゲートウェイネットワーク帯域幅の制限(kbps)]**を選択して、制限値(kbps)を入力します。

重複排除ターゲットとしてIPアドレスまたはFQDNを構成した場合は、**[FUを使用]**と**[IPにフォールバック]**オプションが使用できます。これらはデフォルトで選択されています。

ソース側重複排除を有効にするには、**[サーバー側重複排除]**を選択します。

11. 接続を検証するには、**[チェック]**をクリックします。
12. **[次へ]**をクリックして、設定ウィンドウを表示します。ここでは、次のオプション指定できます。
    - **Max. ストレージユニットごとの最大接続数:** 物理接続を制限する書き込みおよび読み取りストリームの最大数の中央値を定義します。
    - **バックアップサイズのソフトクォータ(GB):** バックアップサイズのソフトクォータを入力します(GB)。
    - **ストアサイズのソフトクォータ(GB):** 1つのストレージユニットを作成する場合、または、データドメインオペレーティングシステム(DD OS)のクォータを手動で有効にする場合にサポートされ、ストレージユニットを作成するときに指定します。
    - **ストアメディアアイテムサイズのしきい値(GB)**: データドメインブーストデバイスのストアアイテムのサイズのしきい値を定義します。このサイズを超えると、オブジェクトは現在のストアアイテムに追加されません。デフォルトでは、ストアアイテムサイズは無制限になっています。
    - **ストアメディアごとのシングルオブジェクト**: データドメインブーストデバイスのストアアイテムごとに1つのオブジェクトを有効にする場合に選択します。
13. **[次へ]**をクリックして、構成済みのB2Dストレージユニットの詳細が含まれるサマリーウィンドウを表示します。
14. 設定を確認して、**[完了]**をクリックします。新しく構成されたB2DデバイスがScopingペインに表示されます。

AIXシステムでのデータドメインブーストの構成

AIXシステム上でファイバーチャネル(FC)プロトコルによってデータドメインブーストを構成するには、AIX DDdfcデバイスドライバーをインストールする必要があります。ドライバーのファイル名はDDdfc.1.0.0.x.bffで、xはバージョン番号です。

手順

1. AIXクライアントにルートユーザーとしてログインします。
2. `# smitty install`コマンドを入力します。
3. **[ソフトウェアのインストールと更新]**を選択します。
4. **[ソフトウェアのインストール]**を選択します。
5. DDdfc.1.0.0.x.bffファイルのインストール先のパス`/usr/omni/drv` を入力します。xはバージョン番号です。
6. **F4**を押して、インストールするDDdfc.1.0.0.xバージョンを選択します。
7. **Tab**を押して、[プレビューのみ]の値を[行]から[いいえ]に切り替えます。
8. **Enter**を押して、情報を受け入れてドライバーをインストールします。

ディスクへのバックアップデバイスを構成する - Smart Cache

ディスクへのバックアップ(B2D)デバイスを使用してバックアップを実行する前に、Data Protectorで使用できるようにデバイスを構成する必要があります。

Smart Cacheを構成する

前提条件

- Smart Cacheデバイスを作成するMedia Agentホストのユーザー資格情報が必要です。VMwareプラグインは、非段階的な復元中にこれらの資格情報を使用してネットワーク共有にアクセスします。

> **注:** 単一のMedia Agentホストでは、1つのオペレーティングシステムユーザー資格情報のみを使用してSmart Cacheデバイスを作成する必要があります。複数のユーザーが同じMedia Agentホスト上で同時にSmart Cacheデバイスを作成する場合、VMware Granular Recovery要求で「アクセスは拒否されました」というエラーが発生することがあります。

- Linuxオペレーティングシステムの場合、Data Protectorは復元中にSambaサーバーを使用して共有を作成するので、SambaサーバーをSmart Cacheクライアントにインストールして実行する必要があります。Sambaサーバーが実行されていることを確認するには、次のコマンドを実行します。`ps -ef | grep smbd`。Sambaサーバーのセキュリティのデフォルトのモードは*user-level*です。デフォルトのモードが変更された場合は、次のコマンドを使用して*user-level*に更新する必要があります。`[global] security = user`。
- Samba共有に読み取り書き込みのパーミッションがあることを確認してください。Security-Enhanced Linux (SELinux)カーネルセキュリティモードがLinuxシステムに展開されている場合、`# setsebool -P samba_export_all_rw on`コマンドを実行して、Samba共有の読み取り書き込みパーミッションを有効にします。
- Sambaサーバーで、次のコマンドを使用してMedia AgentホストのユーザーをSambaのパスワードデータベースに追加する必要があります。`smbpasswd –a <user>`。次のコマンドを使用して、ユーザーがパスワードデータベースに追加されているかどうかを確認できます。`pdbedit -w -L`。
- Samba構成ファイル(smb.conf)の定期的なクリーンアップを実行する必要があります。これにより、以前のSamba共有の構成情報が削除されます。
- Smart CacheストレージがWindows ReFSファイルシステム、CIFS、またはNFS共有である場合は、VMwareの非段階的な復元のエージェントとMedia Agentモジュールを同じホスト上に展開する必要があります。
- Smart Cacheストレージがローカルの固定ディスクまたはは SAN Storage LUNである場合は、VMwareの非段階的な復元のエージェントとMedia Agentモジュールを異なるものにできます。
- ファイルシステム全体を1つのSmart Cacheデバイス専用にする必要があります。このファイルシステムは、他のアプリケーションで使用しないようにし、さらに他のSmart Cacheデバイスまたはディスクへのバックアップデバイスで共有しないようにする必要があります。
- 1つのSmart Cacheデバイスに関連付けることができるのは、単一のメディアプールのみです。

制限事項

- Smart Cacheは、Windows x64およびLinux x64プラットフォームでのみ利用できます。
- ネットワーク共有上に置かれているWindows Smart Cacheデバイスの場合、非段階的なGREは

Windows Server 2008以降のシステムでのみサポートされます。

- Smart Cacheは、VMwareバックアップのターゲットとしてのみ使用できます。
- Linuxオペレーティングシステムでは、NDMP Media Agentパッケージがインストールされている場合、Smart Cacheへのバックアップはサポートされません。
- Smart Cacheデバイスへの暗号化またはAES 256ビット暗号化されたVMwareバックアップはサポートされていません。
- Cacheデバイスへの暗号化またはAES 256ビット暗号化されたソースのオブジェクトコピーはサポートされていません。ただし、ハードウェア暗号化されたテープデバイスとの間のオブジェクトコピーはサポートされています。
- Smart Cacheデバイスあたり1つのマウントポイントのみがサポートされます。
- スペースが不足している場合、Smart Cacheデバイスへのバックアップが失敗することがあります。Smart Cacheデバイス内の使用可能なディスクに余裕があることを確認してください。
- メディアのエクスポートおよびインポートは、Smart Cacheデバイスではサポートされません。
- Resilient File System (ReFS)ボリュームまたはネットワーク共有(CIFS/NFS)上にSmart Cacheデバイスを作成する場合、マウントプロキシコンポーネント(復元に使用します)を同じホストにインストールします。そのようにしないと非段階的な復元が失敗します。
- CIFSは、StoreOnce 4500のSmart Cacheデバイス構成ではサポートされません。

手順

1. ディスク上の必要な場所(たとえば`c:\SmartCache`)にSmart Cacheデバイス用のディレクトリを作成します。

   ローカルまたはネットワークドライブ(またはLinuxシステムの場合はNFSでマウントされたファイルシステム)にSmart Cacheデバイスを作成できます。ネットワークドライブを指定するには、次の形式を使用します。`\\hostname\share_name`。

   ホスト名、およびホストの共有名とネットワークドライブは、[ドライブのブラウズ]ダイアログには表示されません。UNC名へのパスを入力する必要があります。
2. **Windows**オペレーティングシステムで、Smart Cacheデバイスが含まれる共有ディスクにアクセスするためのパーミッションを取得するには、Media AgentでData Protector Inetアカウントを変更します。これを行うには、ローカルクライアントシステムとリモート共有ディスクの両方に対するアクセスパーミッションを付与します。また、このアカウントがシステムアカウントではなく、特定ユーザーのアカウントであることを確認します。Inetアカウントを設定した後に、共有ディスク上にあるSmart Cacheデバイスを構成して使用します。
3. コンテ**キストリストで**[デバイス/メディア]Data Protectorをクリックします。
4. Scopingペインで、**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックして、ウィザードを起動します。
5. デバイスの名前と説明(オプション)を指定します。
6. **ディスクへのバックアップ**デバイスタイプを選択し、**Smart Cache**インターフェイスタイプを選択します。
7. [クライアント]ドロップダウンリストで、デバイスの格納先のシステムを選択します。**[次へ]**をクリックします。
8. 非段階的な復元中に作成した共有にアクセスする必要があるユーザーのユーザー名とパスワードを入力します。
9. Smart Cacheデバイスのディレクトリを指定します。**[追加]**をクリックします。
10. ディレクトリのデフォルトプロパティを変更するには、ディレクトリを選択し、**[プロパティ]**をクリックします。

11. **[次へ]**をクリックしてサマリーウィンドウを表示します。設定を確認して、**[完了]**をクリックします。新しく構成されたB2DデバイスがScopingペインに表示されます。

クラウドデバイス(Helion)を構成する

クラウドオブジェクトストアへのオブジェクトコピーを実行する準備のためにクラウド(Helion)デバイスを構成します。

準備では、次の手順を実行する必要があります。

- HPE Public Cloudプロジェクト名を取得する
- 認証サービスURLを取得する
- アクセスキーを作成する

次に、Data Protectorで、クラウド(Helion)デバイスをディスクへのバックアップデバイスとして構成できます。

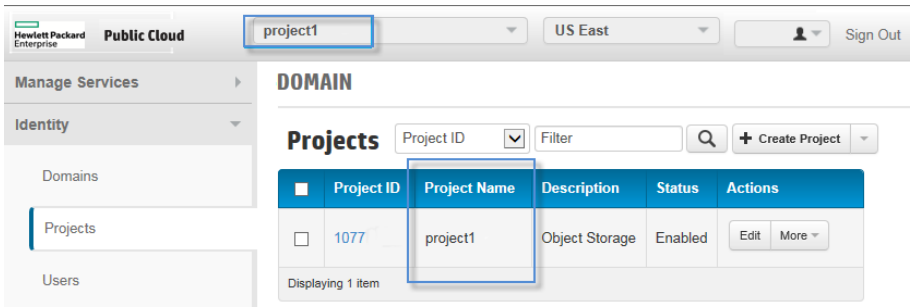
ディスクへのバックアップデバイスを構成する - クラウド(Helion)

HPE Public Cloudプロジェクト名を取得する

手順

1. HPE Public Cloudの資格情報を使用してHPE Public Cloudコンソール(https://horizon.hpcloud.com)にログインします。
2. プロジェクトリストから適切なプロジェクトを選択します。
3. HPE Data Protector GUIで後で使用するためにプロジェクト名をメモします。プロジェクト名は、デバイスの作成中に[テナント/プロジェクト]フィールドで指定します。

   HPE Public Cloudのプロジェクト



認証サービスURLを取得する

手順

1. [ユーザー]メニューから**[役割およびAPIエンドポイント]**を選択します。[ユーザーの役割およびAPIエンドポイント]ページが表示されます。
2. **[サービスAPIエンドポイント]**タブをクリックします。サービスAPIエンドポイントのリストが表示されます。
3. 自社のデータセンターに最も近い地域のサービスタイプ**ID**のサービスAPIエンドポイントURLをメモします。

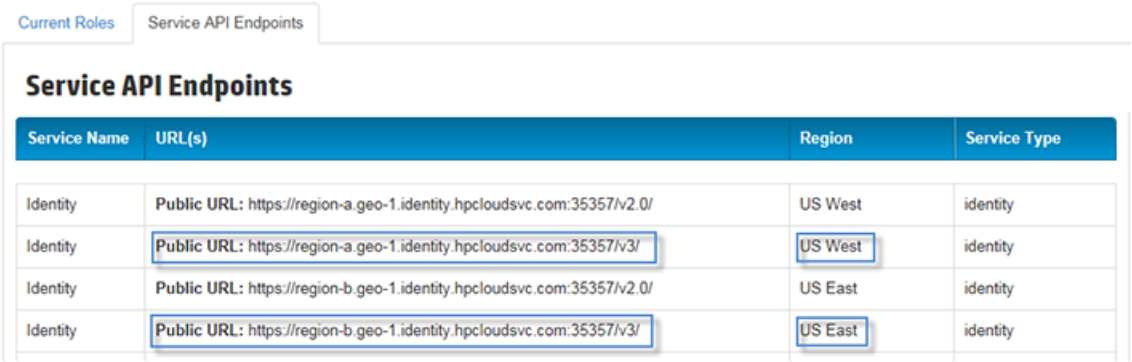
このURLは、後でクラウド(Helion)デバイスを作成するときに、HPE Data Protector GUIの[認証サービス]フィールドで指定します。

アクセスキーを使用して認証を行う場合は、末尾に**/v3/**サフィックスが付いている認証サービスURLをメモします。

例:

https://region-b.geo-1.identity.hpcloudsvc.com:35357**/v3/**

HPE Public CloudのサービスAPIエンドポイント

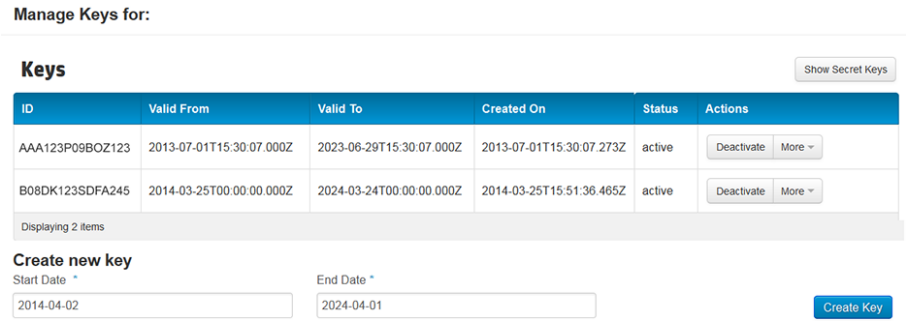


アクセスキーを作成する

手順

1. [ユーザー]メニューから**[アクセスキーの管理]**を選択します。[アクセスキーの管理]ページが表示されます。
2. 新しいキーを作成するには、新しいキーの**[開始日]**と**[終了日]**を指定し、**[キーの作成]**をクリックします。新しいキーが作成されます。

   HPE Public Cloudでのアクセスキーの作成



3. **[秘密キーの表示]**をクリックして、新しいキーのIDと秘密キーを表示します。

   HPE Public Cloudの秘密キー

Manage Keys for:

Keys

ID	Valid From	Valid To	Created On	Secret Key	Status	Actions
ABC1DEF242CCCC	2013-07-01T15:30:07.000Z	2023-06-29T15:30:07.000Z	2013-07-01T15:30:07.273Z	1o43z2ABC09C1DWfQasb30odiL42ABC09C1D	active	Deactivate
1432ABC09CDWQ4	2014-03-25T00:00:00.000Z	2024-03-24T00:00:00.000Z	2014-03-25T15:51:36.465Z	A1bC1D6Fdh2ABC09C1D242CmlC1C9dpaz2C	active	Deactivate

Displaying 2 items

4. 後で使用するためにキーIDと秘密キー情報をコピーします。これらは、クラウド(Helion)デバイスを作成するときにHPE Data Protector GUIで指定します。

ディスクへのバックアップデバイスを構成する - クラウド(Helion)

HPE Data Protectorで、インターフェイスタイプとしてクラウド(Helion)デバイスを使用してディスクへのバックアップデバイスを構成します。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックして、ウィザードを起動します。
3. デバイスの名前と説明(オプション)を指定します。
4. **[ディスクへのバックアップ]**デバイスタイプを選択し、インターフェイスの種類として**クラウド(Helion)**を選択します。**[次へ]**をクリックします。
5. **認証サービスURL**を指定します。これは、「認証サービスURLを取得する」で取得したサービスAPIエンドポイントURLです。
6. **[認証モード]**リストで、認証のモードを選択します。
   a. ユーザー名とパスワードによる認証を使用するには、**[ユーザー名とパスワード]**を選択し、HPE Public Cloudの資格情報を入力します。
   b. アクセスキーを使用して認証を行うには、**[アクセスキー]**を選択し、**[アクセスキーID]**と**[秘密キー]**に入力します。これらは、「アクセスキーを作成する」でメモしたキーです。

   > **注:**
   > アクセスキーを使用して認証を行う場合、認証サービスURLに**/v3/**サフィックスが含まれている必要があります。例:
   >
   > https://region-b.geo-1.identity.hpcloudsvc.com:35357/**v3/**

7. **[テナント/プロジェクト]**を指定します。これは、「プロジェクト名を取得する」で取得したプロジェクト名です。
8. **[コンテナーの選択/作成]**をクリックして、既存のストアのリストからコンテナーを選択するか、新しいコンテナーを作成します。
9. データソースのローカルのゲートウェイを指定します。
   a. ゲートウェイを選択し、**[追加]**をクリックしてプロパティダイアログを表示します。必要に応じてゲートウェイのプロパティを変更し、**[OK]**をクリックしてゲートウェイを追加します。
10. **[次へ]**をクリックしてサマリーウィンドウを表示します。設定を確認して、**[完了]**をクリックします。新しく構成されたデバイスがScopingペインに表示されます。

ディスクへのバックアップデバイスを構成する - クラウド(Azure)

Data Protectorで、**インターフェイスの種類**としてクラウド(Azure)を使用してディスクへのバックアップデバイスを構成します。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックして、ウィザードを起動します。
3. **[デバイス名]**フィールドにデバイス名を指定します。**[説明]**はオプションです。
4. **ディスクへのバックアップ**デバイスタイプを選択し、**インターフェイスタイプ**としてクラウド(Azure)を選択します。**[次へ]**をクリックします。

   [管理コンソールのURL]は、デフォルトで入力されています。
5. **[ストレージアカウント名]**、**[秘密キー]**、**[秘密キー2]**の情報をフィールドに入力します。**[追加]**をクリックして、データをクラウド(Azure)に送信するためのゲートウェイを追加します。[コンテナーの選択]ウィンドウが表示されます。
6. データをアップロードするための既存のコンテナーを選択するか、新しいコンテナーを作成します。ゲートウェイは、デフォルト値を使用して追加できます。

   オブジェクトコピーにはブロックサイズの制限があります。ローカルデバイスからクラウドにオブジェクトコピーを行ってから、復元のために同じデバイスにコピーする場合、ローカルデバイスとクラウドデバイスのブロックサイズは同じでなければなりません。
7. **[チェック]**をクリックして、ゲートウェイがクラウド(Azure)に接続していることを確認します。正常に接続されている場合、ステータスは**[OK]**と表示されます。デバイスが作成され、使用する準備が整います。

ファイルライブラリデバイスを構成する

ファイルライブラリデバイスの格納先ディスクは、Media Agentが存在するシステムのローカルディスクにする必要があります。そうしないと、デバイスのパフォーマンスが低下する可能性があります。

前提条件

- ファイルライブラリデバイスが存在するディスクは、ファイルライブラリデバイスが存在するファイルシステムで表示できなければなりません。
- ファイルライブラリデバイスの内容が作成されるディレクトリは、ファイルライブラリデバイスが存在するディスク上に存在しなければなりません。
- ファイルライブラリデバイスをWindowsシステム上で作成する場合、ファイルライブラリデバイスとして使用するファイルに対しWindowsの圧縮オプションを無効にします。

制限事項

- ファイルライブラリデバイスには、1つまたは複数のディレクトリを格納することができます。1つのファイルシステムに存在し得るディレクトリは、1つだけです。

- ファイルライブラリタイプのデバイスの構成に使用するディレクトリのパス名の長さは、46文字を超えることはできません。

手順

1. ファイルライブラリデバイスを格納するディスクに、`c:\FileLibrary`のようなファイルライブラリデバイス用のディレクトリを作成します。

   ファイルライブラリデバイスは、ローカルドライブかネットワークドライブ(UNIXシステムの場合はNFSマウントファイルシステム)上に作成できます。ネットワークドライブは、`\\hostname\share_name`の形式で指定することも、ドライブ文字(`S:\datastore\My_FileLibrary`)に割り当てることもできます。

   共有名またはネットワークドライブを伴うホスト名は、パスを入力する[ドライブのブラウズ]ダイアログには表示されません。UNC名またはネットワークドライブへのパスは自分で入力する必要があります。

   Windowsオペレーティングシステムで、ファイルライブラリデバイスのある共有ディスクにアクセスするための正しいパーミッションを取得するため、Media Agent上でData Protector Inetアカウントを変更します(ローカルクライアントシステムとリモート共有ディスクの両方にアクセスできるパーミッションを設定します)。また、このアカウントがシステムアカウントではなく、特定ユーザーのアカウントであることを確認します。Inetアカウントを設定すると、共有ディスク上にあるファイルライブラリデバイスの構成および使用が可能になります。

   > **重要:**
   > ファイルライブラリ用に作成したディレクトリはディスクから削除しないよう注意してください。このディレクトリを削除すると、ファイルライブラリデバイス内のデータが消失してしまいます。

2. Data Protector Managerのコンテキストリストで[デバイス/メディア]をクリック**します。**
3. Scopingペインで、**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックして、ウィザードを起動します。
4. [デバイス名]テキストボックスにファイルライブラリデバイスの名前を入力します。
5. 必要に応じて、[説明]テキストボックスにライブラリの説明を入力します。
6. [デバイスの種類]ドロップダウンリストで、**[ファイルライブラリ]**を選択します。
7. [クライアント]ドロップダウンリストで、デバイスの格納先のシステムを選択します。**[次へ]**をクリックします。
8. ファイルライブラリを格納するディレクトリ、またはディレクトリのセットを指定します。**[追加]**をクリックします。
9. ディレクトリのデフォルトプロパティを変更するには、ディレクトリを選択し、**[プロパティ]**をクリックします。
10. ファイルライブラリに対するライターの数を入力します。追加したディレクトリの数がデフォルトになります。デバイス内のディレクトリ数より多いライターを追加すると、デバイスのパフォーマンスを向上できます。この点は、使用しているハードウェア構成によって異なります。使用している環境で、結果をテストする必要があります。**[次へ]**をクリックします。
11. ファイルライブラリデバイスの[メディアの種類]は、[ファイル]です。このファイルライブラリ内で仮想フルバックアップを有効にするには、**[分散ファイルメディア形式を使用する]**を選択します。**[次へ]**をクリックします。
12. ファイルライブラリデバイスの構成のサマリーを確認します。**[完了]**をクリックしてウィザードを終了します。

デバイス名が構成済みデバイスのリストに表示されます。デバイス名は、そのデバイスが割り当てられたメディアプールにも表示されます。

ファイルデポは、初めて使用されるまで、そのデバイスには表示されません。

デバイスを初めて使用した後にスキャンを行うことにより、構成を検証することができます。

ファイルライブラリで使用するメディアプールのメディアの使用法は、デフォルトで追加不可能です。このポリシーにより、期限切れになったメディアの自動再利用などのファイルライブラリのメリットを得られるため、このポリシーを使うことをお勧めします。また、ファイルライブラリを使ってオブジェクトコピーやオブジェクト集約を実行するには、追加不可能なメディアの使用法が必要です。

デバイスに対する複数パスの構成について

通常、SAN環境のデバイスは複数のクライアントに接続されているため、複数のパス、つまり、クライアント名とSCSIアドレス(UNIXシステム上ではデバイスファイル)の組み合わせからアクセスが可能です。Data Protectorでは、これらのパスのいずれかを使用できます。同一物理デバイスに対するすべてのパスをまとめて、1つの論理デバイスとして構成することも可能です。これを、*マルチパスデバイス*と呼びます。

たとえば、あるテープデバイスが、client1に接続されて`/dev/rs1`および`/dev/rs2`として構成されており、client2では`/dev/r1s1`、client3では`scsi1:0:1:1`として構成されているとします。このため、`client1:/dev/rs1`、`client1:/dev/rs2`、`client2:/dev/r1s1`、および`client3:scsi1:0:1:1`という4つの異なるパスを通してデバイスにアクセスすることができます。マルチパスデバイスには、このテープデバイスへの4つのパスすべてが含まれています。

複数のパスを使う理由

Data Protectorの以前のバージョンでは、デバイスは1つのクライアントからしかアクセスできませんでした。この問題を回避するには、複数の論理デバイスを、ロック名を使用して単一の物理デバイスとして構成する必要がありました。このようにして、複数のシステムから単一の物デバイスへのアクセスの構成にロック名を使用する場合は、各システムですべてのデバイスを構成する必要がありました。たとえば、単一のデバイスに接続されているクライアントが10個あった場合は、同じロック名のデバイスを10個構成する必要がありました。Data Protectorの今回のバージョンでは構成が簡略化され、すべてのパスについて単一のマルチパスデバイスを構成するだけで済むようになっています。

マルチパスデバイスを採用すると、システムが障害に強くなります。Data Protectorは、最初に定義されているパスを試します。クライアント上のすべてのパスがアクセス不可能だった場合、Data Protectorはその次に定義されているクライアント上のパスを試します。リストされているパスがすべて利用不可能だった場合にのみ、セッションは中断されます。

パスの選択

バックアップセッション中、デバイスパスはそのデバイスの構成中に定義された順序で選択されます。ただし、バックアップ仕様で優先クライアントが選択されている場合を除きます。その場合は、選択されている優先クライアントが最初に使用されます。

復元セッション中、パスは次の順序で選択されます。

1. すべてのオブジェクトが同じターゲットクライアントに復元される場合は、オブジェクトの復元先クライアント上のパス
2. バックアップに使用されたパス
3. その他の利用可能なパス

複数のパスが構成されたデバイスの場合は、ローカルパスが優先されます。利用可能なローカルパスがない場合は、利用可能な任意のパスが事前に定義された順序で使用されます。

直接ライブラリアクセスが有効な場合は、構成されている順序に関係なく、最初にローカルパス(あて先クライアント上のパス)がライブラリ制御に使用されます。

マルチパスSAN環境では、Data Protectorバックアップセッションマネージャー(BSM)は、できる限りローカルデバイスを使用します。この動作は、LANfreeグローバルオプションを使って調整できます。

LANfreeグローバルオプションには次の2つの値を指定できます。

- 0 – デフォルトでは、この値が指定されます。HPE Data Protectorバージョン8.11以前の場合、変更する必要はありません。
- 1 – マルチパス環境で適用できます。この環境では、HPE Data Protectorは、優先されるホストまたはマルチパスリストの最初のホストを選択する代わりに、オブジェクトが存在していた元のホストを選択します(そのようなパスが使用可能な場合)。

  以下に、LANfreeグローバルオプションが1に設定された場合の、実際のマルチパスデバイスの割り当ての効率向上について説明します。

  - HPE Data Protectorは、ホストへのパスが構成されているデバイスについて、データが存在していた元のホストを優先します。

  - HPE Data Protectorは、ホストへのパスが構成されているデバイスについて、データが存在していた元のホスト上で新しいMedia Agent (MA)を起動します。この処理は、空いている同時スロットを使用してターゲットデバイス用のリモートMAが既に起動されている場合でも行われます。

次のシナリオでは、HPE Data Protectorは、デバイスのローカルパスを使用しない場合があります。

- ユーザーが負荷調整(MINまたはMAXパラメーター)を指定されている場合、BSMは、データの提供元のどのホストに対してもローカルではないデバイスを選択してロックすることがあります。
- マルチパスデバイスを制御しているMAが1つのホスト上で実行され、そのデバイスへのパスが構成されている別のホストからオブジェクトが取得される場合、Data ProtectorはMAをローカルホストに移行しませんがん、既に起動されているローカルホストにLAN経由でデータをストリーミングします。これは、負荷調整のMAX値に既に達している場合に発生します。
- IgnoreObjectLocalityForDeviceSelectionグローバルオプションが設定されているとLANfreeの設定が無効になります。デフォルトでは、IgnoreObjectLocalityForDeviceSelectionは設定されません。

次の場合は、LANフリーなバックアップを実現するためにユーザーによるデバイスパスの追加が必要になることがあります。

- バックアップクライアントに複数のネットワークインターフェイスとホスト名が設定されている場合。この場合、DNSの構成によっては、HPE Data Protectorのバックアップが複数のインターフェイスを介して転送される可能性があります。この場合は、各インターフェイスのローカルパスを追加することが推奨されます。
- WindowsクラスターリソースであるWindowsファイルサーバーのファイルシステムのバックアップを実行する場合。このような設定では、各Windowsクラスターリソースに専用のホスト名が指定され、そのための個別のデバイスパスエントリを作成する必要があります。

以前のバージョンとの互換性

Data Protectorの以前のバージョンで構成されたデバイスはアップグレード時に再構成されず、変更を行わずに以前のリリースのData Protectorと同じように使うことができます。新しいマルチパス機能を活用するには、デバイスをマルチパスデバイスとして再構成します。

制限事項

以下の制限事項が適用されます。

- マルチパスは、NDMPデバイスとジュークボックスライブラリではサポートされていません。
- デバイスチェーンはマルチパスデバイスではサポートされていません。

[デバイス/メディア]の拡張オプションを設定する

新しいデバイスの構成時やデバイスプロパティの変更時には、デバイスやメディアの拡張オプションを設定できます。利用可能な拡張オプションは、デバイスの種類によって異なります。

これらのオプションの一部は、バックアップの構成時に設定することもできます。バックアップ仕様で設定されたオプションは、デバイス全般に設定されているオプションより優先して適用されます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[デバイス]**を展開します。
3. オプションを変更するデバイス(ライブラリデバイスの場合はドライブ)を右クリックし、**[プロパティ]**をクリックします。
4. **[設定]**タブをクリックし、**[拡張]**ボタンをクリックして、拡張オプションのページを開きます(**[設定]**, **[サイズ]**、**[その他]**)。
5. 目的のオプションを指定し、**[OK]**をクリックして変更内容を適用します。

VTLデバイスを構成する

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[環境]**を展開して**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックしてウィザードを起動します。
3. [デバイス名]テキストボックスにVTLの名前を入力します。
4. [説明]テキストボックスに必要に応じて説明を入力します。
5. 必要に応じて、**[マルチパスデバイス]**を選択します。
6. [デバイスの種類]リストで、**[SCSIライブラリ]**を選択します。これにより、**[SCSI]**が[インターフェイスの種類]リストで自動的に選択されます。
7. **[マルチパスデバイス]**オプションが選択されて*いない*場合は、[クライアント]リストでクライアント名を選択します。
8. 必要に応じて、ライブラリ管理コンソールの有効なURLを**[管理コンソールのURL]**テキストボックスに入力します。**[次へ]**をクリックします。
9. ライブラリSCSIアドレスおよびドライブの処理に関する必要な情報を指定して、**[次へ]**をクリックしま

す。

10. Data Protectorで使用するスロットを指定し、**[次へ]**をクリックします。
11. デバイスで使用するメディアの種類を選択します。
12. **[完了]**をクリックしてウィザードを終了します。

> **注:** RedHat Linux (RHEL) 7.1システムでVTLデバイスを使用している場合は、ジェネリックSCSIドライバーを手動でロードする必要があります。これは、コマンド`modprobe -vs sg`を実行して行うことができます。また、システム始動時にこのコマンドが開始されるように、このコマンドをRHEL `init scripts`または`cron job`に追加することをお勧めします。

スタッカーデバイスを構成する

バックアップデバイスをシステムに接続し、デバイスファイル(SCSIアドレス)が存在することを確認したら、そのデバイスをData Protectorで使用できるように構成することができます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックして、ウィザードを起動します。
3. [デバイス名]テキストボックスにデバイスの名前を入力します。
4. [説明]テキストボックスに必要に応じて説明を入力します。
5. 必要に応じて、**[マルチパスデバイス]**を選択します。
6. **[マルチパス デバイス]**オプションを選択していない場合は、クライアントの名前を選択します。
7. **[次へ]**をクリックします。
8. [デバイスの種類]リストで、デバイスの種類として**[スタッカー]**を選択し、**[次へ]**をクリックします。
9. [データのデバイス]テキストボックスに物理デバイスのSCSIアドレス(Windowsシステムの場合)またはデバイスファイル名(UNIXシステムの場合)を入力します。また、ドロップダウン矢印をクリックすると、ドライブのアドレスまたはファイル名を自動検出できます。

   マルチパスデバイスの場合は、クライアント名を選択し、**[追加]**をクリックして、構成済みパスのリストにパスを追加します。
10. 変更されたSCSIアドレスの自動検出を有効にする場合は、**[変更されたSCSIアドレスの自動検出]**を選択します。
11. **[次へ]**をクリックします。
12. 構成するデバイスのメディアの種類を[メディアの種類]ドロップダウンリストから選択します。
13. 選択したメディアの種類に対応するメディアプールを指定します。既存のプールを[メディアプール]ドロップダウンリストから選択するか、新しいプール名を入力します。新しいプール名を入力した場合は、プールが自動的に作成されます。
14. **[完了]**をクリックしてウィザードを終了します。

デバイス名が構成済みデバイスのリストに表示されます。デバイスをスキャンすると、構成を確認できます。デバイスが正しく構成されていれば、Data Protectorはメディアのロード、読み込み、スロットへのアンロードができるようになります。

スタッカーデバイスメディアの管理

スタッカーデバイスを構成した後で、このデバイスの管理メディアの特別な点について考慮してみてください。たとえば、オペレーションスキャン、検証、フォーマットはスタッカーデバイス内の各メディアで個別に実行しなければなりません。Data Protectorセッションが実行できるように正しくメディアをロードする必要があります。

ジュークボックスデバイス(光磁気ライブラリ)を構成する

バックアップデバイスをシステムに接続し、デバイスファイル(SCSIアドレス)が存在することを確認したら、そのデバイスをData Protectorで使用できるように構成することができます。

ジュークボックスデバイスの構成

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックして、ウィザードを起動します。
3. [デバイス名]テキストボックスにデバイスの名前を入力します。
4. [説明]テキストボックスに必要に応じて説明を入力します。
5. [デバイスの種類]リストで、デバイスの種類として**[ジュークボックス]**を選択します。
6. [クライアント]リストでクライアントの名前を選択します。
7. 必要に応じて、ライブラリ管理コンソールの有効なURLを**[管理コンソールのURL]**テキストボックスに入力します。
8. **[次へ]**をクリックします。
9. ジュークボックスのファイル/ディスクのセットを指定します。複数のファイルやディスクを指定する場合は、`/tmp/FILE 1-3`のように、ダッシュで区切ります。指定し終えたら、**[追加]**をクリックします。光磁気のジュークボックスの場合、ディスク名の最後は`A/a`または`B/b`とする必要があります。**[次へ]**をクリックします。
10. 構成するデバイスのメディアの種類を[メディアの種類]リストから選択します。
11. **[完了]**をクリックして、このウィザードを終了します。ライブラリドライブを構成するかどうかを確認するメッセージが表示されます。**[はい]**をクリックすると、ドライブ構成ウィザードが表示されます。

ジュークボックスデバイス内のドライブの構成

手順

1. [デバイス名]テキストボックスにデバイスの名前を入力します。
2. [説明]テキストボックスに必要に応じて説明を入力します。
3. 選択したメディアの種類に対応するメディアプールを指定します。既存のプールを[メディアプール]リストから選択するか、新しいプール名を入力します。新しいプール名を入力した場合は、プールが自

動的に作成されます。すべてのドライブを1つのメディアプールに含めることも、各ドライブを個別のメディアプールに割り当てることもできます。**[次へ]**をクリックします。

4. オプションで、**[デバイスを復元で使用可]**および**[デバイスをオブジェクトコピーのソースデバイスとして使用可]**を選択し、**[デバイスタグ]**を指定します。
5. **[完了]**をクリックしてウィザードを終了します。

ドライブ名が構成済みドライブのリストに表示されます。ドライブをスキャンすると、構成を確認できます。

SCSIライブラリデバイスまたはマガジンデバイスを構成する

バックアップデバイスをシステムに接続し、デバイスファイル(SCSIアドレス)が存在することを確認したら、そのデバイスをData Protectorで使用できるように構成することができます。

ライブラリとマガジンデバイスの構成手順は同じですが、マガジンデバイスを構成する場合には**[マガジンのサポート]**オプションが設定されているメディアプールを指定する必要があります。

バックアップデバイスの構成には、Data Protectorの自動構成機能を使用することをお勧めします。

SCSIライブラリロボティクスの構成

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックして、ウィザードを起動します。
3. [デバイス名]テキストボックスにデバイスの名前を入力します。
4. [説明]テキストボックスに必要に応じて説明を入力します。
5. 必要に応じて、**[マルチパスデバイス]**を選択します。
6. [デバイスの種類]リストで、デバイスの種類として**[SCSIライブラリ]**を選択します。
7. [インターフェイスの種類]リストで、インターフェイスの種類として**[SCSI]**を選択します。
8. **[マルチパスデバイス]**オプションが選択されていない場合は、[クライアント]リストでクライアント名を選択します。
9. 必要に応じて、ライブラリ管理コンソールの有効なURLを**[管理コンソールのURL]**テキストボックスに入力します。
10. **[次へ]**をクリックします。
11. ライブラリロボティクスのSCSIアドレスを入力するか、またはドロップダウン矢印をクリックして、ドライブのアドレスまたはファイル名を自動検出します。

    マルチパスデバイスの場合は、クライアント名を選択し、**[追加]**をクリックして、構成済みパスのリストにパスを追加します。
12. **[ビジードライブの処理]**リストで、ドライブがビジーの場合にData Protectorが実行する操作を選択します。
13. 変更されたSCSIアドレスの自動検出を有効にする場合は、**[変更されたSCSIアドレスの自動検出]**を選択します。

14. 必要に応じて、**[SCSI予約/解除(ロボティクス制御)]**を選択します。**[次へ]**をクリックします。
15. デバイスのスロットを指定します。スロット範囲を指定するには、ダッシュを使って指定し、**[追加]**をクリックします。たとえば、スロット1、2、3を同時に追加する場合なら、1-3と入力し、**[追加]**をクリックします。文字を使ったり先頭にゼロを付加したりしないでください。**[次へ]**をクリックします。
16. 構成するデバイスのメディアの種類を[メディアの種類]ドロップダウンリストから選択します。
17. **[完了]**をクリックして、このウィザードを終了します。ライブラリドライブを構成するかどうかを確認するメッセージが表示されます。**[はい]**をクリックすると、ドライブ構成ウィザードが表示されます。

ライブラリ内のドライブの構成

手順

1. [デバイス名]テキストボックスにデバイスの名前を入力します。
2. [説明]テキストボックスに必要に応じて説明を入力します。
3. 必要に応じて、**[マルチパスデバイス]**を選択します。
4. **[マルチパスデバイス]**オプションが選択されて*いない*場合は、[クライアント]リストでクライアント名を選択します。

   > **ヒント:**
   > Data Protector Media Agentが動作している異なるシステムから各ドライブがデータを受信できるよう、ライブラリを構成することができます。これにより、ハイエンド環境での性能が向上します。各ドライブを使用するクライアントシステムは[クライアント]ドロップダウンリストから選択してください。

   [次へ]をクリックします。
5. [データドライブ]テキストボックスにデータドライブのSCSIアドレスまたはファイル名を入力します。

   マルチパスデバイスの場合は、クライアント名を選択し、**[追加]**をクリックして、構成済みパスのリストにパスを追加します。
6. 変更されたSCSIアドレスの自動検出を有効にする場合は、**[変更されたSCSIアドレスの自動検出]**を選択します。
7. [ドライブのインデックス]テキストボックスに、ライブラリ内のドライブのインデックスを入力します。**[次へ]**をクリックします。
8. 選択したメディアの種類に対応するメディアプールを指定します。既存のプールを[メディアプール]ドロップダウンリストから選択するか、新しいプール名を入力します。新しいプール名を入力した場合は、プールが自動的に作成されます。デフォルトのメディアプールを使用することをお勧めします。

   > **注:**
   > すべてのドライブをData Protectorで使用できるよう構成する必要はありません。すべてのドライブを1つのメディアプールに含めることも、各ドライブを個別のメディアプールに割り当てることもできます。

   マガジンデバイス用のメディアプールを指定する場合は、**[マガジンのサポート]**オプションが設定されているメディアプールを選択してください。

   [次へ]をクリックします。
9. オプションで、**[デバイスを復元で使用可]**および**[デバイスをオブジェクトコピーのソースデバイスとして使**

用可]を選択し、**[デバイスタグ]**を指定します。

10. **[完了]**をクリックしてウィザードを終了します。

ドライブ名が構成済みドライブのリストに表示されます。ドライブをスキャンすると、構成を確認できます。デバイスが正しく構成されていれば、Data Protectorはメディアのロード、読み込み、スロットへのアンロードができるようになります。

SAN環境でデバイスを構成する

SAN環境は、1つのライブラリを使用する1つのクライアントから、複数のライブラリを使用する複数のクライアントまで、多岐にわたります。また、その複数のクライアントが、異なるオペレーティングシステムを採用していることもあります。Data Protectorから見た場合、SAN環境を構成する目的は次のとおりです。

- ライブラリロボティクスを共有する各ホストにおいて、それぞれのホストのロボティクス定義を作成する。ロボティクスを制御するホストが1つしかない場合は、デフォルトのロボティクス制御ホストに対してのみライブラリ定義が作成されます。
- ライブラリで同じ(テープ)ドライブを共有する各ホストにおいて
  - 使用するデバイスごとにデバイスの定義を作成する。
  - (物理)デバイスが別のホストからも使用される場合(共有デバイス)、ロック名を使用する。
  - 必要に応じて、ダイレクトアクセス機能を使用する場合はこの機能を選択する。使用する場合には、`libtab`ファイルがそのホスト上に設定されている必要があります。

考慮事項

- Microsoft Cluster Server:ドライブのハードウェアパスが両方のクラスターノードで同じことを確認します。デバイスを構成したら、フェイルオーバーを実行して検証します。

構成方法

SAN構成に参加するプラットフォームによって、3つの構成方法があります。

GUIを使ったデバイスの自動構成

Data Protectorの自動構成機能では、SAN環境内の複数のホストにあるデバイスおよびライブラリを自動構成することができます。自動構成は、以下のオペレーティングシステムでサポートされています。

- Windows
- HP-UX
- Solaris
- Linux
- AIX

制限事項

SAN環境内の以下のデバイスに対しては、自動構成を使用できません。

- 混合メディアライブラリ
- DASライブラリまたはACSLSライブラリ
- NDMPデバイス

環境に接続されているバックアップデバイスは、Data Protectorが検出します。ライブラリデバイスの場合、Data Protectorは、スロット数、メディアの種類、およびライブラリに属するドライブを認識します。Data Protectorは次に、ドライブやスロットを構成する他に、デバイスについても論理名、ロック名、メディアの種類、およびデバイスファイルまたはSCSIアドレスを設定して構成します。

> **注:**
> SAN環境に新しいホストを導入した場合、構成済みのライブラリとデバイスは自動的に更新されません。
>
> - 既存のライブラリを新しいホストで使用するには、このライブラリを削除し、同じ名前を指定して新しいホスト上で新しいライブラリを自動構成します。
> - 既存のライブラリにデバイスを追加するには、ライブラリを削除し、同じ名前を指定して新しいホスト上で新しいライブラリを自動構成するか、またはドライブをライブラリに手動で追加します。

CLI(sanconfコマンド)を使用したデバイスの自動構成

sanconfコマンドを使ってSAN環境内のデバイスとライブラリを構成することができます。sanconfコマンドは、集中型メディア管理データベース(Centralized Media Management Database)(CMMDB)によって、単一Data ProtectorセルでのSAN環境およびMoM環境においてライブラリ構成を容易にするユーティリティです。このコマンドは、複数のクライアントからドライブに関する情報を収集して単一ライブラリにすることによって、SAN環境内でライブラリを自動的に構成できます。MoM環境では、sanconfを実行しているセルでCMMDBが使用されていれば、sanconfはCMMDBを使用する任意のData Protectorセル内の任意のライブラリを構成できます。sanconfは次のオペレーティングシステムで使用できます。

- Windows
- HP-UX
- Solaris

sanconfでは、以下のオペレーティングシステム上で実行されているクライアントに接続されたサポートしているデバイスを検出し、構成することができます。

- Windows
- HP-UX
- Solaris
- Linux
- AIX

このコマンドを使用して、以下の作業を行うことができます。

- 指定のData Protectorをスキャンして、ドライブのSCSIアドレスと、SAN環境内のクライアントに接続されているロボティクス制御に関する情報を収集します。
- Data Protectorクライアントのスキャンで収集した情報をもとに、指定のクライアントのライブラリおよびドライブの設定を構成または修正します。
- すべてのクライアントまたは指定のクライアントのドライブをライブラリから削除します。

デバイスのロック

sanconfコマンドは、構成対象ドライブのロック名を自動生成します。ロック名は、ドライブのベンダーID文字列、製品ID文字列、製品シリアル番号で構成されます。

たとえば、ベンダーIDが「HP」、製品IDが「DLT8000」、シリアル番号が「A1B2C3D4E5」のHPE DLT 8000ドライブのロック名は「HP:DLT8000:A1B2C3D4E5」となります。

ロック名は手動で追加することもできます。ロック名は論理デバイスごとに固有です。

sanconfコマンドが作成したロック名は変更してはなりません。手動で作成し、sanconfコマンドで構成した物理ドライブを表す他のすべての論理ドライブも、sanconfで作成したロック名を必ず使用しなければならないからです。

制限事項

- sanconfでサポートされるライブラリの一覧については、https://softwaresupport.hpe.com/にある最新のサポート一覧を参照してください。
- sanconfは以下の機能をサポートしません。
  - ドライブスロットに予備のドライブを置くこと。
  - ドライブの種類を混在させること(たとえば、DLT、9840、LTOドライブの組み合わせ)。
  - 現在、利用できないクライアントを構成すること。このようなクライアントの構成は、クライアントのスキャンで収集された情報が含まれている構成ファイルがライブラリの構成に使用される場合にのみ可能です。

推奨事項

システムの個々のデバイスについてドライバーはそれぞれ1つだけ構成するようにしてください。

sanconfコマンドの使用法については、sanconfmanページまたは『*HPE Data Protector Command Line Interface Reference*』を参照してください。

UNIXシステムでの手動構成

SAN環境でUNIXシステムに接続された共有デバイスを手動で構成する場合、以下の作業を行う必要があります。

- 使用するデバイスごとにデバイスの定義を作成する。
- ロック名を使用する。
- 必要に応じて、ダイレクトアクセス機能を使用したい場合はダイレクトアクセスを選択する。使用する場合には、そのホスト上のlibtabファイルが適切に設定されている必要があります。

構成の段階

1. デバイスを手動で構成する
2. libtabファイルを手動で構成する

SAN環境でデバイスを手動で構成する

この手順では、ドライブとロボティクスが複数のシステムに使用され、ドライブがData Protectorを含めた複数のアプリケーションに使用される場合を想定しています。さらに、すべてのシステムがロボティクス制御コマンドを送信する(直接ライブラリアクセス)ことを前提としています。実際の環境がこれと異なる場合もあるので、ここでは、環境に応じた手順の違いも適宜示してあります。

ロボティクス制御には、SAN内の任意のクライアントを使用できます。まず、デフォルトのロボティクス制御システムの役割を果たしているクライアント上で、ライブラリロボティクス制御を構成する必要があります。どのクライアントがメディアの移動を要求しているかに関わらず、このクライアントが、メディアの移動を管理するために使用されます。これは、複数のホストが同時にメディアの移動を要求した場合に、ロボティクスで競合が発生するのを回避するためです。ホストが失敗し、かつダイレクトアクセスが有効化されている場合にのみ、ロボティクス制御がメディアの移動を要求しているローカルのホストで実行されます。

前提条件

Data Protector Media Agent(General Media AgentまたはNDMP Media Agent)が、共有ライブラリと通信する必要がある各クライアントにインストールされていること。

構成の段階

SAN環境内のライブラリの構成

ライブラリ内のドライブの構成

SAN環境内の**ライブラリ**の構成

> **注:**
> ロボティクス制御をクラスターに管理させる場合は、以下のことを確認する必要があります。
>
> - ロボティクス制御が各クラスターノード上に存在すること。
> - 仮想クラスター名がライブラリロボティクス構成に使用されていること。
> - ロボティクスおよびデバイスの共通ファイル名が、`mksf`コマンドまたは`libtab`ファイルのいずれかを使用してインストールされていること。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックして、ウィザードを起動します。
3. [デバイス名]テキストボックスにデバイスの名前を入力します。
4. [説明]テキストボックスに必要に応じて説明を入力します。
5. 必要に応じて、**[マルチパスデバイス]**を選択します。
6. [デバイスの種類]ドロップダウンリストで、デバイスの種類として**[SCSIライブラリ]**を選択します。
7. [インターフェイスの種類]ドロップダウンリストで、インターフェイスの種類として**[SCSI]**を選択します。
8. **[マルチパスデバイス]**が選択されていない場合は、クライアント(バックアップシステム)の名前を[クライア

ント]ドロップダウンリストから選択します。

9. 必要に応じて、ライブラリ管理コンソールの有効なURLを**[管理コンソールのURL]**テキストボックスに入力します。
10. **[次へ]**をクリックします。
11. ライブラリロボティクスのSCSIアドレスを入力するか、またはドロップダウン矢印をクリックして、ドライブのアドレスまたはファイル名を自動検出します。

    マルチパスデバイスの場合は、[クライアント]ドロップダウンリストでクライアントの名前を選択します。**[追加]**をクリックして、構成済みパスのリストにパスを追加します。
12. **[ビジードライブの処理]**リストで、**[メディアの取り出し]**を選択します。
13. 変更されたSCSIアドレスの自動検出を有効にする場合は、**[変更されたSCSIアドレスの自動検出]**を選択します。**[次へ]**をクリックします。
14. デバイスのスロットを指定します。複数のスロットを指定するには、ダッシュを使います。指定し終えたら、**[追加]**をクリックします。たとえば、スロット1、2、3を同時に追加する場合なら、1-3と入力し、**[追加]**をクリックします。**[次へ]**をクリックします。
15. 構成するデバイスのメディアの種類を[メディアの種類]ドロップダウンリストから選択します。
16. **[完了]**をクリックして、このウィザードを終了します。ライブラリドライブを構成するかどうかを確認するメッセージが表示されます。**[はい]**をクリックすると、ドライブ構成ウィザードが表示されます。この後は、下記の手順のとおり、ウィザードの指示に従ってください。

ライブラリ内のドライブの構成

使用するクライアントから各ドライブを構成します。

手順

1. [デバイス名]テキストボックスにドライブの名前を入力します。

   以下の命名規則を使用することをお勧めします。

   - `LibraryLogicalName_DriveIndex_Hostname`例: SAN_LIB_2_hotdog (非マルチパスデバイスの場合)
   - `LibraryLogicalName_DriveIndex`例: SAN_LIB_2 (マルチパスデバイスの場合)
2. [説明]テキストボックスに必要に応じて説明を入力します。
3. 必要に応じて、**[マルチパスデバイス]**を選択します。
4. **[マルチパスデバイス]**が選択されていない場合は、クライアント(バックアップシステム)の名前を[クライアント]ドロップダウンリストから選択します。
5. **[次へ]**をクリックします。
6. [データドライブ]テキストボックスにデータドライブのSCSIアドレスまたはファイル名を入力します。

   マルチパスデバイスの場合は、[クライアント]ドロップダウンリストでクライアントの名前を選択します。**[追加]**をクリックして、構成済みパスのリストにパスを追加します。
7. [ドライブのインデックス]テキストボックスに、ライブラリ内のドライブのインデックスを入力します。
8. 変更されたSCSIアドレスの自動検出を有効にする場合は、**[変更されたSCSIアドレスの自動検出]**を選択します。**[次へ]**をクリックします。

9. 選択したメディアの種類に対応するメディアプールを指定します。既存のプールを[メディアプール]ドロップダウンリストから選択するか、新しいプール名を入力します。新しいプール名を入力した場合は、プールが自動的に作成されます。

   すべてのドライブを1つのメディアプールに含めることも、各ドライブを個別のメディアプールに割り当てることもできます。

10. **[拡張]**ボタンをクリックします。**[設定]**タブで、**[ダイレクトライブラリアクセスを使用]**オプションを選択します。

    単一のシステムからのみData Protectorによるロボティクス制御コマンドを送信する場合は、**[ダイレクトライブラリアクセスを使用]**オプションを選択しないでください。Data Protectorで使用するライブラリ/ドライブを構成するときに選択したクライアントシステムがライブラリロボティクスを制御することになります。

11. マルチパスドライブの場合は、この手順は*必要ありません*。**[次へ]**をクリックします。
    - Data Protectorがドライブにアクセスする唯一のアプリケーションの場合は、**[その他]**タブをクリックし、**[ロック名を使用]**オプションをオンにし、名前を入力します。この名前は、他のクライアント上で同じドライブを構成するときに必要になるので、メモしておいてください。以下の命名規則を使用することをお勧めします。

      `LibraryLogicalName_DriveIndex`例: SAN_LIB_D2

    - ドライブにアクセスするアプリケーションがData Protectorの他にもある場合は、**[ロック名を使用]**オプションを選択して、すべてのデバイスについて、一度にアクセスするのは1つのアプリケーションからという排他的アクセスを、操作上のルールで保証します。

    - ドライブを単一のシステムでのみ使用する場合は、**[ロック名を使用]**オプションをオンにしないでください。

12. オプションで、**[デバイスを復元で使用可]**および**[デバイスをオブジェクトコピーのソースデバイスとして使用可]**を選択し、**[デバイスタグ]**を指定します。
13. **[完了]**をクリックしてウィザードを終了します。

ドライブは複数のシステムおよび複数のアプリケーション(Data Protectorだけとは限らない)によって使用されます。デバイスのロック機能(ロック名を定義)を使用して、すべてのデバイスについて、一度にアクセスするのは1つのアプリケーションからという排他的アクセスを、操作上のルールで保証します。

ドライブ名が構成済みドライブのリストに表示されます。ドライブをスキャンすると、構成を確認できます。

SAN環境でlibtabファイルを構成する

`libtab`ファイルの目的は、ライブラリのロボティクス制御アクセスを"ダイレクトアクセスを要求しているシステム"上でも機能するようマッピングすることです。これは、ローカル制御パスがデフォルトのライブラリロボティクス制御システムで使用されている制御パスとは異なっている可能性が高いためです。

`libtab`ファイルは、各WindowsおよびUNIXクライアント上に1つ配置されている必要があります。各クライアントは、ライブラリロボティクスへの"直接アクセス"を必要とし、デフォルトのライブラリロボティクス制御システムとして構成されたシステムとは異なっています。

手順

1. 直接アクセスを要求する各システム上の以下のディレクトリ内に、テキスト形式で`libtab`ファイルを作成します。

   Windowsシステムの場合: *`Data_Protector_home`*`\libtab`

   HP-UXおよびSolarisシステムの場合: `/opt/omni/.libtab`

   その他のUNIXシステムの場合: `/usr/omni/.libtab`

2. `libtab`ファイルには以下の情報を入力します。

   `FullyQualifiedHostname DeviceFile | SCSIPath DeviceName`

   - *`FullyQualifiedHostname`*は、ライブラリロボティクス用の直接アクセス制御を要求しているクライアントの名前です。このクライアントがクラスターの一部である場合、ノード名が使用されます。

   - *`DeviceFile | SCSIPath`*は、このクライアント上のライブラリロボティクスドライバーへの制御パスです。

   - *`DeviceName`*は、このクライアント上で使用されるデバイス定義の名前です。

   デバイス用に直接アクセスを要求する場合、デバイスごとに1行使用する必要があります。

システムがクラスターの一部になっている場合は、*`FullyQualifiedHostname`*に仮想サーバー名を指定し、*`DeviceFile | SCSIPath`*でローカルノード(物理システム)を参照する必要があります。

ADIC/GRAU DASライブラリデバイスを構成する

Data Protectorには、ADIC/GRAUライブラリをData Protectorバックアップデバイスとして構成するための専用ADIC/GRAUライブラリポリシーが用意されています。

Media Agentソフトウェアをインストールし、DASサーバーを通じてライブラリロボティクスにアクセスする各システムは、DASクライアントと呼ばれます。

以下に追加情報を示します。

- ADIC/GRAU機能は、個々のData Protectorライセンスの対象となります。詳細は、『*HPE Data Protectorインストールガイド*』を参照してください。
- このライブラリでは異なるアプリケーションに使用されるメディアを管理するので、どのメディアとドライブをData Protectorで使用し、どのメディアを追跡するかを定義する必要があります。
- Data Protectorは専用の独立したメディア割り当てポリシーを持ち、スクラッチプールは使用しません。

構成の段階

1. ライブラリドライブの接続
2. Media Agentのインストールを準備する
3. Media Agentのインストール
4. ADIC/GRAU DASライブラリデバイスの構成
5. ADIC/GRAU DASライブラリデバイス内のドライブの構成

ライブラリドライブを接続する

手順

1. Media Agentソフトウェアをインストールするシステムにライブラリドライブとロボティクスを物理的に接続します。

   UNIXシステムおよびWindowsシステムにバックアップデバイスを物理的に接続する方法の詳細は、『*HPE Data Protectorインストールガイド*』を参照してください。

2. ADIC/GRAUライブラリを構成します。詳しい手順の説明については、ADIC/GRAUライブラリ付属のマニュアルを参照してください。

   サポートされているADIC/GRAUライブラリについては、https://softwaresupport.hpe.com/にアクセスしてください。

Media Agentのインストールを準備する

手順

1. DASサーバーがOS/2をベースに稼動している場合は、Data ProtectorのADIC/GRAUバックアップデバイスを構成する前に、DASサーバーコンピューター上の`C:\DAS\ETC\CONFIG`ファイルを作成または更新します。

   このファイルには、すべてのDASクライアントのリストを記述する必要があります。Data Protectorの場合、Media Agentがインストールされる各Data Protectorクライアントをこのファイルで定義しなければなりません。

   各DASクライアントは、たとえば`OMNIBACK_C1`のように、スペースを含まない一意のクライアント名で定義されています。この例の場合、`C:\DAS\ETC\CONFIG`ファイルの内容は次のようになります。

   ```
   client client_name = OMNIBACK_C1,
   # hostname = AMU,"client1"
   ip_address = 19.18.17.15,
   requests = complete,
   options = (avc,dismount),
   volumes = ((ALL)),
   drives = ((ALL)),
   inserts = ((ALL)),
   ejects = ((ALL)),
   scratcHPools = ((ALL))
   ```

   これらの名前は、各Data Protector Media Agentクライアント上で、`omnirc`オプション`DAS_CLIENT`として構成する必要があります。`omnirc`ファイルは、*`Data_Protector_home`*ディレクトリの`omnirc`ファイル(Windowsシステムの場合)または`.omnirc`ファイル(UNIXシステムの場合)です。たとえば、IPアドレスが19.18.17.15のシステムでは、`omnirc`ファイルの該当行は`DAS_CLIENT=OMNIBACK_C1`になります。

2. ADIC/GRAUライブラリスロットの割り当てポリシーが静的または動的のいずれの方法で構成されているかを確認します。割り当てポリシーの種類をチェックする方法については、『`AMU Reference`

Manual』を参照してください。

静的割り当て方針では各volserごとにスロットがあらかじめ指定されていますが、動的割り当て方針ではスロットがランダムに割り当てられます。すでに設定されているポリシーに応じてData Protectorを構成してください。

静的割り当てポリシーが構成されている場合は、ライブラリのロボティクスを制御するシステムに次のomnircオプションを追加します。

```
OB2_ACIEJECTTOTAL = 0
```

これは、HP-UXとWindowsの場合に適用されます。

ADIC/GRAUライブラリの構成の詳細は、ADIC/GRAUサポート窓口に連絡するか、ADIC/GRAUのドキュメントを参照してください。

Media Agentのインストール

ADIC/GRAUライブラリ内のバックアップドライブに接続することになるシステム、およびDASサーバーを使ってライブラリロボティクスにアクセスするシステムに、General Media AgentまたはNDMP Media Agentをインストールすることができます。

> **注:**
> メディアのレポジトリのサイズやADIC/GRAUライブラリ内で使用するドライブおよびスロットの数によっては、特殊なライセンスが必要になります。詳細については、『*HPE Data Protectorインストールガイド*』を参照してください。

前提条件

- ADIC/GRAUライブラリがすでに構成されており、稼動していること。ADIC/GRAUライブラリの構成方法については、ADIC/GRAUライブラリに付属のドキュメントを参照してください。
- DASサーバーが正常に稼動しており、DASクライアントが正しく構成されていること。

  ADIC/GRAUライブラリを制御するには、DASソフトウェアが必要です。このソフトウェアは、DASサーバーと複数のDASクライアントからなります。DASソフトウェアの詳細は、ADIC/GRAUライブラリに付属のドキュメントを参照してください。
- Media Agentをインストールする前に、以下の情報を取得してください。
  - DASサーバーのホスト名。
  - 使用可能なデバイスおよび対応するドライブのDAS名のリスト。

    ADIC/GRAUシステムのDASクライアントをすでに定義し終えている場合は、以下のコマンドを実行すると、これらの情報を取得できます。

    `dasadmin listd2 [client]` または

    `dasadmin listd [client]`、ここで、`[client]`は予約済みのドライブを表示するDASクライアントの名前です。

    `dasadmin`コマンドは、`C:\DAS\BIN`ディレクトリ(OS/2ホストの場合)またはDASクライアントがインストールされているディレクトリにあります。

    Windowsシステムの場合: *%SystemRoot%*`\system32`

    UNIXシステムの場合: `/usr/local/aci/bin`

- 使用可能な挿入/取り出し領域および対応するフォーマット仕様のリスト。

  このリストは、OS/2ホスト上のAMS (AML Management Software)のグラフィカル構成で取得できます。

  [Admin]メニューの**[Configuration]**をクリックして構成を開始します。**[I/O]**をダブルクリックして[EIF-Configuration]ウィンドウを開き、**[Logical Ranges]**をクリックします。使用可能な挿入/取り出し領域のリストがテキストボックスに表示されます。

  1つのData Protectorライブラリデバイスで扱えるメディアの種類は1つだけです。挿入/取り出し領域のそれぞれに所属するメディアの種類を把握しておくことが重要です。このデータは、後でData Protectorライブラリ用の挿入/取り出し領域を構成するときに必要になります。

- **Windowsシステムの場合:**ドライブのSCSIアドレスのリスト(例: `scsi4:0:1:0`)。

- **UNIXシステムの場合:**ドライブのUNIXデバイスファイルのリスト

  この情報を表示するには、システムコマンドの`ioscan -fn`を実行します。

手順

1. Data Protectorグラフィカルユーザーインターフェイスとインストールサーバーを使ってMedia Agentコンポーネントをクライアントに配布します。
2. クライアントインターフェイス用のADIC/GRAUライブラリファイルをインストールします。

   Windowsシステムの場合:

   - `aci.dll`、`winrpc32.dll`、および`ezrpc32.dll`の各ライブラリを*`Data_Protector_home`*`\bin`ディレクトリにコピーします。(これらの3つのライブラリは、ADIC/GRAUライブラリに付属するDASクライアントソフトウェアの一部です。インストールメディア、またはAMU-PCの`C:\DAS\AMU\`ディレクトリに含まれています。)

   - この3つのライブラリは、*`%SystemRoot%`*`\system32`ディレクトリにもコピーしてください。

   - `Portinst`サービスおよび`Portmapper`サービスをDASクライアントにコピーします。なお、これらはADIC/GRAUライブラリとともに出荷されているDASクライアントソフトウェアの要件です。これらのファイルは、インストールメディアに収録されています。

   - [コントロールパネル]から**[管理ツール]**、**[サービス]**の順に移動し、`portinst`を起動して、`portmapper`をインストールします。

   - DASクライアントを再起動して`portmapper`サービスを開始します。

   - [コントロールパネル]から**[管理ツール]**、**[サービス]**の順に移動し、`portmapper`サービスおよび両方の`rpc`サービスが稼動しているかどうかをチェックします。

   HP-UX、Linux、およびAIXシステムの場合:

   共有ライブラリ`libaci.sl` (HP-UXシステム)、`libaci.so` (Linuxシステム)、または`libaci.o` (AIXシステム)を、ディレクトリ`/opt/omni/lib` (HP-UXおよびLinuxシステム)または`/usr/omni/lib` (AIXシステム)にコピーします。このディレクトリにアクセスするためのパーミッションが必要です。共有ライブラリの読み取りと実行が全ユーザー(root、グループ、その他)に対して許可されていることを確認してください。なお、共有ライブラリ`libaci.sl`および`libaci.o`は、ADIC/GRAUライブラリに付属しているDASクライアントソフトウェアの一部です。これらのファイルは、インストールメディアに収録されています。

3. DASソフトウェアを正しくインストールし終えたら、`devbra -dev`コマンドを実行して、ライブラリドライブがシステムに適切に接続されているかどうかをチェックします。コマンドは、デフォルトのData Protector管理コマンドディレクトリに存在します。

   ライブラリドライブおよび対応するデバイスファイル/SCSIアドレスのリストが表示されます。

ADIC/GRAU DASライブラリデバイスの構成

ADIC/GRAUライブラリをシステムに物理的に接続し、Media Agentをインストールし終えたら、Data Protector GUIからADIC/GRAUライブラリデバイスを構成できます。DASクライアントは、特定のメディア管理操作(Query、Enter、Eject)中にADIC/GRAUロボティクスにアクセスします。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックします。
3. [デバイス名]テキストボックスにデバイスの名前を入力します。
4. [説明]テキストボックスに必要に応じて説明を入力します。
5. 必要に応じて、**[マルチパスデバイス]**を選択します。
6. [デバイスの種類]リストで、**[GRAU DASライブラリ]**を選択します。
7. **[マルチパスデバイス]**オプションが選択されていない場合は、ADIC/GRAUロボティクスにアクセスするMedia Agentの名前を選択します。
8. 必要に応じて、ライブラリ管理コンソールの有効なURLを**[管理コンソールのURL]**テキストボックスに入力します。
9. **[次へ]**をクリックします。
10. [DASサーバー]テキストボックスにDASサーバーのホスト名を入力します。

    マルチパスデバイスの場合は、クライアント名を選択し、**[追加]**をクリックして、構成済みパスのリストにパスを追加します。
11. **[ビジードライブの処理]**リストで、ドライブがビジーの場合にData Protectorが実行する操作を選択し、**[次へ]**をクリックします。
12. ライブラリのインポート用およびエクスポート用の領域を指定し、**[追加]**をクリックします。**[次へ]**をクリックします。
13. [メディアの種類]リストから、デバイスに適したメディアの種類を選択します。
14. **[完了]**をクリックしてウィザードを終了します。ライブラリドライブを構成するかどうかを確認するメッセージが表示されます。**[はい]**をクリックすると、ドライブ構成ウィザードが表示されます。

ADIC/GRAU DASライブラリデバイス内のドライブの構成

手順

1. [デバイス名]テキストボックスにドライブの名前を入力します。
2. [説明]テキストボックスに必要に応じて説明を入力します。
3. 必要に応じて、**[マルチパスデバイス]**を選択します。

4. **[マルチパスデバイス]**オプションが選択されていない場合は、ADIC/GRAUロボティクスにアクセスするMedia Agentの名前を選択します。
5. **[次へ]**をクリックします。
6. [データドライブ]テキストボックスでデバイスのSCSIアドレスを指定します。

   マルチパスデバイスの場合は、ADIC/GRAUロボティクスにアクセスするMedia Agentクライアントの名前を選択し、**[追加]**をクリックして、構成済みパスのリストにパスを追加します。
7. 変更されたSCSIアドレスの自動検出を有効にする場合は、**[変更されたSCSIアドレスの自動検出]**を選択します。
8. [ドライブ名]テキストボックスに、Media Agentのインストール中に知ったADIC/GRAUドライブ名を指定します。**[次へ]**をクリックします。
9. ドライブの**デフォルトメディアプール**を選択します。
10. **[拡張]**をクリックし、**[同時処理数]**などのドライブの拡張オプションを設定します。**[OK]**をクリックします。**[次へ]**をクリックします。
11. オプションで、**[デバイスを復元で使用可]**および**[デバイスをオブジェクトコピーのソースデバイスとして使用可]**を選択し、**[デバイスタグ]**を指定します。
12. **[完了]**をクリックしてウィザードを終了します。

StorageTek ACSライブラリデバイスを構成する

Data Protectorには、StorageTek ACSライブラリ専用のポリシーがあります。これは、StorageTek ACSライブラリをData Protector バックアップデバイスとして構成するためのポリシーです。

Media Agentソフトウェアをインストールし、ライブラリロボティクスにアクセスするACSLSを通じてライブラリロボティクスにアクセスする各システムを、ACSクライアントと呼びます。

以下に追加情報を示します。

- STK機能は、個々のData Protectorライセンスの対象となります。詳細については、『HPE Data Protectorインストールガイド』を参照してください。
- このライブラリでは異なるアプリケーションに使用されるメディアを管理するので、どのメディアとドライブをData Protectorで使用し、どのメディアを追跡するかを定義する必要があります。
- Data Protectorは専用の独立したメディア割り当てポリシーを持ち、スクラッチプールは使用しません。

構成の段階

1. ライブラリドライブの接続
2. Media Agentのインストール
3. StorageTek ACSライブラリデバイスの構成
4. StorageTek ACSライブラリデバイス内のドライブの構成

ライブラリドライブを接続する

手順

1. Media Agentソフトウェアをインストールするシステムにライブラリドライブとロボティクスを物理的に接続します。

   UNIXシステムおよびWindowsシステムにバックアップデバイスを物理的に接続する方法の詳細は、『*HPE Data Protectorインストールガイド*』を参照してください。
2. StorageTek ACSライブラリを構成します。詳しい手順の説明については、STK ACSライブラリ付属のドキュメントを参照してください。

   サポートされているStorageTekライブラリについては、https://softwaresupport.hpe.com/にアクセスしてください。

Media Agentのインストール

StorageTekライブラリ内のバックアップドライブに物理的に接続する予定のシステムおよびACSLSを使ってライブラリロボティクスにアクセスするシステムに、General Media AgentまたはNDMP Media Agentをインストールできます。

> **注:**
> メディアのレポジトリのサイズやStorageTekライブラリ内で使用するドライブおよびスロットの数によっては、特殊なライセンスが必要になります。詳細については、『*HPE Data Protectorインストールガイド*』を参照してください。

前提条件

- StorageTekライブラリがすでに構成されており、稼動していること。StorageTekライブラリの構成方法については、StorageTekライブラリに付属のドキュメントを参照してください。
- Media Agentソフトウェアのインストールを開始する前に、以下の情報を取得する必要があります。
  - ACSLSが稼動しているホストの*hostname*。
  - Data Protectorで使用するACSドライブIDのリスト。リストを表示するには、ACSLSが稼動しているホストにログインし、次のコマンドを実行します。

    ```
    rlogin “ACSLS hostname” -l acssa
    ```

    端末の種類を入力して、コマンドプロンプトが表示されるまで待ちます。ACSSAプロンプトが表示されたら、次のコマンドを入力します。

    ```
    ACSSA> query drive all
    ```

    ACSドライブのフォーマット仕様は、次のように指定する必要があります。

    ```
    ACS DRIVE: ID:#,#,#,# - (ACS num, LSM num, PANEL, DRIVE)
    ```
  - Data Protectorで使用するドライブがonline状態になっていることを確認します。ドライブがonline状態になっていない場合は、ACSLSホスト上で次のコマンドを実行して状態を切り替えます。

    ```
    vary drive drive_id online
    ```

- 使用できるACS CAP IDおよびACS CAPフォーマットの仕様。リストを表示するには、ACSLSが稼動しているホストにログインし、次のコマンドを実行します。

  `rlogin "ACSLS hostname" -l acssa`

  端末の種類を入力して、コマンドプロンプトが表示されるまで待ちます。ACSSAプロンプトが表示されたら、次のコマンドを入力します。

  `ACSSA> query cap all`

  ACS CAPのフォーマット仕様は、次のように指定する必要があります。

  `ACS CAP: ID:#,#,# (ACS num, LSM num, CAP num)`

- Data Protectorで使用するCAPが`online`状態になっており、操作モードが`manual`になっていることを確認します。

  CAPが`online`状態になっていない場合は、次のコマンドを実行して状態を切り替えます。

  `vary cap cap_id online`

  CAPが`manual`操作モードになっていない場合は、次のコマンドを実行してモードを切り替えます。

  `set cap manual cap_id`

- **Windowsシステムの場合:**ドライブのSCSIアドレスのリスト(例: `scsi4:0:1:0`)。

- **UNIXシステムの場合:**ドライブのUNIXデバイスファイルのリスト

  この情報を表示するには、システムコマンドの`ioscan -fn`を実行します。

手順

1. Data Protector GUIとWindows用インストールサーバーを使ってMedia Agentコンポーネントをクライアントに配布します。
2. ライブラリ上のロボティクスにアクセスするすべてのライブラリホスト(Media Agentクライアント)で、ACS `ssi`デーモンを起動します。

   Windowsシステムの場合:

   `LibAttach`サービスをインストールします。詳細は、ACSのドキュメントを参照してください。`LibAttach`サービスの構成時には、必ず適切なACSLSホスト名を入力してください。構成が正常に完了すると、`LibAttach`サービスが自動的に開始されます。それ以降は、システムを再起動すると、必ずこのサービスが自動的に開始されます。

   > **注:**
   > `LibAttach`サービスをインストールし終えたら、`libattach\bin`ディレクトリがシステムパスに自動的に追加されていることを確認します。追加されていない場合は、手動で追加してください。

   このサービスの詳細は、StorageTekライブラリに付属のドキュメントを参照してください。

   HP-UXおよびSolarisシステムの場合:

   次のコマンドを実行します。

   `/opt/omni/acs/ssi.sh start ACS_LS_hostname`

   AIXシステムの場合:

   次のコマンドを実行します。

```
/usr/omni/acs/ssi.sh start ACS_LS_hostname
```

3. デフォルトのData Protector管理コマンドディレクトリから、`devbra -dev`コマンドを実行して、ライブラリドライブがMedia Agentクライアントに正しく接続されているかどうかをチェックします。

   ライブラリドライブおよび対応するデバイスファイル/SCSIアドレスのリストが表示されます。

StorageTek ACSライブラリデバイスを構成する

StorageTekライブラリをシステムに物理的に接続し、Media Agentをインストールし終えたら、Data Protector GUIからStorageTekライブラリデバイスを構成できます。ACSクライアントは、特定のメディア管理操作(Query、Enter、Eject)中にStorageTekロボティクスにアクセスします。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックします。
3. [デバイス名]テキストボックスにデバイスの名前を入力します。
4. [説明]テキストボックスに必要に応じて説明を入力します。
5. 必要に応じて、**[マルチパスデバイス]**を選択します。
6. [デバイスの種類]リストで、**[StorageTek ACSライブラリ]**を選択します。
7. **[マルチパスデバイス]**を選択していない場合は、StorageTekロボティクスにアクセスするMedia Agentクライアントを選択します。
8. 必要に応じて、ライブラリ管理コンソールの有効なURLを**[管理コンソールのURL]**テキストボックスに入力します。
9. **[次へ]**をクリックします。
10. [ACSLMホスト名]テキストボックスにACSサーバーのホスト名を入力します。

    マルチパスデバイスの場合は、クライアント名を選択し、構成済みパスのリストにパスを追加します。
11. **[ビジードライブの処理]**リストで、ドライブがビジーの場合にData Protectorが実行する操作を選択し、**[次へ]**をクリックします。
12. ライブラリの**CAP**を指定し、**[追加]**をクリックします。**[次へ]**をクリックします。
13. [メディアの種類]リストから、デバイスに適したメディアの種類を選択します。
14. **[完了]**をクリックしてウィザードを終了します。ライブラリドライブを構成するかどうかを確認するメッセージが表示されます。**[はい]**をクリックすると、ドライブ構成ウィザードが表示されます。

StorageTek ACSライブラリデバイス内のドライブの構成

手順

1. [デバイス名]テキストボックスにドライブの名前を入力します。
2. [説明]テキストボックスに必要に応じて説明を入力します。
3. 必要に応じて、**[マルチパスデバイス]**を選択します。
4. **[マルチパスデバイス]**を選択していない場合は、StorageTekロボティクスにアクセスするMedia Agentク

ライアントを選択します。

5. **[次へ]**をクリックします。
6. [データドライブ]テキストボックスでデバイスのSCSIアドレスを指定します。

   マルチパスデバイスの場合は、StorageTekロボティクスにアクセスするMedia Agentクライアントを選択し、**[追加]**をクリックして、構成済みパスのリストにパスを追加します。
7. [ドライブのインデックス]テキストボックスに、Media Agentのインストール中に取得したStorage Tek**ドライブインデックス**を指定します。ドライブインデックスは、カンマで区切られた4つの数字の組み合わせです。**[次へ]**をクリックします。
8. ドライブの**デフォルトメディアプール**を選択します。
9. **[拡張]**をクリックし、**[同時処理数]**などのドライブの拡張オプションを設定します。**[OK]**をクリックします。**[次へ]**をクリックします。
10. オプションで、**[デバイスを復元で使用可]**および**[デバイスをオブジェクトコピーのソースデバイスとして使用可]**を選択し、**[デバイスタグ]**を指定します。
11. **[完了]**をクリックしてウィザードを終了します。

バックアップデバイスの使用について

バックアップデバイスの使用が必要とされるタスクには、デバイス内のメディアを特定するためのデバイススキャン、仮想ロック名を指定することによるデバイスのロック、スケジュールに基づくメディアの取り出しの実施、汚れたドライブの自動または手動によるクリーニング、バックアップデバイスの名前の変更、必要なメディアがデバイス内にあることを確認するためのマウント要求への応答などがあります。

Data Protectorには、デバイスおよびメディア用の拡張オプションがデバイスの種類に応じて用意されています。これらは、デバイスとメディアの管理に役立ちます。

さらに、同じライブラリ内で種類の異なる複数のドライブを使用することもできます。ただし、使用するメディアの特性を考慮する必要があります。

デバイスが何らかの理由で動作不能になった場合は、そのデバイスをバックアップから除外して、デバイスのリストから別の利用可能なデバイスを自動で選択することができます。今後使用しないデバイスがある場合は、そのデバイスをData Protectorの構成から削除できます。

[デバイス/メディア]の拡張オプション

Data Protectorには、デバイスおよびメディアに適用する拡張オプションが用意されています。利用可能な拡張オプションは、デバイスの種類によって異なります。たとえば、ライブラリの構成の方がスタンドアロンデバイスより利用できるオプション数が多くなっています。

これらのオプションは、新しいデバイスの構成時やデバイスプロパティの変更時に設定できます。これらのオプションは、それぞれのデバイスに全般的に適用されます。ここで示すオプションのサブセットを特定のバックアップ仕様に合わせてチューニングすることもできます。これらのオプションは、デバイスに対して全般的に設定されているオプションより優先して適用されます。これらは、バックアップ仕様の構成時や変更時にアクセスできます。

拡張オプションの詳細については、『HPE Data Protectorヘルプ』を参照してください。

拡張オプション - 設定

同時処理数

オプション

- CRCチェック
- 汚れたドライブの検出
- ドライブベースの暗号化
- セッション終了後メディアを取り出し
- 再スキャン
- [ダイレクトライブラリアクセスを使用] (SAN固有のオプション)

拡張オプション - サイズ

- ブロックサイズ(KB)
- Disk Agentバッファー
- セグメントサイズ(MB)

拡張オプション - その他

マウント要求

- 遅延(分)
- スクリプト

デバイスのロック名

- ロック名を使用

複数の種類のドライブを使用するライブラリ

ドライブの種類が複数でも、DLT 4000/7000/8000 (DDSファミリも同じ)のように同様のテクノロジを使用していれば、同じライブラリで使用できます。このため、すべてのメディアが同一フォーマットかどうか確かではない状態でいずれかのドライブでメディアを使用した場合に問題が発生するおそれがあります。たとえば、DLT-4000は復元時に、DLT-8000(最高密度)で書き込んだテープを読み込めません。また、圧縮メディアと非圧縮メディアには互換性がありません。

このような問題は、同じ書き込み密度を設定するか、メディアプールをドライブの種類ごとに作成します。

同一密度に設定

この方法では、全メディア共通のフォーマットを使用して、ドライブを問わず、すべてのメディアに互換性を持たせるようにします。Windowsシステムで使用するデバイスの場合、特定の書き込み密度の使用についてはドライブに付属のマニュアルを参照する必要があります。UNIXシステムの場合、ドライブの密度は、デバイスファイル名の作成中に、または、関連するデバイスファル名を選択してデバイス定義で使用することにより、設定できます。密度は同一の値を設定する必要があります。たとえば、DLT 4000とDLT 7000の場合にはDLT 4000の密度を設定します。また、使用デバイスのブロックサイズ設定が同一であることも確認する必要があります。メディアのフォーマットにはデバイス定義の設定を使用します。すべてのメディアの密度設定を同じにすると、必要に応じてフリープールを使用できます。復元時には、ドライブを問わずすべてのメディアを使用できます。

ドライブの種類ごとにメディアプールを設定

この方法では、あるドライブグループで使用するメディアを別のドライブグループで使用するメディアとはっきり区別するので、ドライブやメディアを最適化して使用できます。ドライブのグループ別にメディアプールを設定できます。これにより、ドライブの種類ごとに異なる密度の設定を使用できます。たとえば、DLT-4k-pool、および、DLT-8k-poolを作成するとします。メディアのフォーマットにはデバイス定義の設定を使用します。たとえば、DLT-8000の最高密度のプールに属するメディアは、DLT-8000の最高密度の設定でフォーマットする必要があります。

フリープールサポート

このように個別設定した「プール間」で1つのフリープールを使用することはできません。フリープールは、別のプールに属するメディアを正しく識別できないため、このようなメディアは「外部」メディアとみなされます。フリープールの概念は、*ドライブの種類ごとに1つのプール*(DLT-8kプールなど)にのみ適用できます。これは同種のメディア(DLT)に互換性のない方法で書き込みが行なわれてはいけないからです。あるプールに属するメディアは、関連するデバイスでしか使用できないため、復元時には注意が必要です。

スキャンについて

スキャン処理では、ドライブに挿入されているメディアのフォーマットがチェックされ、デバイスのレポジトリの内容が表示されます。さらに、IDB内の対応する情報が更新されます。

- スタンドアロンデバイスでは、ドライブ内のメディアがスキャンの対象になります。
- ライブラリデバイスでは、選択したスロット内のメディアがスキャンの対象になります。
- バーコードをサポートしているライブラリデバイスの場合は、バーコードを使ってメディアをスキャンできます。
- ファイルライブラリデバイスでは、ファイルデポに関するIDB内の情報を更新します。
- ADIC/GRAU DASライブラリまたはSTK ACSライブラリを使用する場合は、Data ProtectorによってADIC/GRAU DASサーバーまたはSTK ACSLMサーバーが照会され、IDB内の情報がサーバーから返された情報と同期されます。

スキャンを実行するタイミング

デバイス内のメディアに関するData Protector情報を更新する必要があれば、随時にデバイスをスキャンできます。メディアの収納場所を手動で変更した場合は、デバイスを必ずスキャンしておいてください。手動で変更した収納場所(スロットやドライブ)はData Protectorに認識されません。このため、デバイスをスキャンしておかないと、IDB内の情報との間に食い違いが生じます。スキャンを実行すると、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。

セル内のすべてのメディアに一意なバーコードラベルが割り当てられていることを確認してください。スキャン中に既存のバーコードが検出されると、IDBに登録されているメディアが論理的に移動されます。

ファイルデポのひとつを別の場所に移動した場合は、ファイルライブラリデバイス内でスキャンを実行します。

制限事項

レポジトリでADIC/GRAUライブラリに3970を超えるVOLSERが構成されている場合、VOLSERスキャンが正常に完了しないことがあります。この問題を回避するには、スロットを大きなレポジトリから複数の小さなレポジトリに分割するために、複数の論理ADIC/GRAUライブラリを構成します。

> **重要:**
> 同じ物理ライブラリ用に複数の論理ライブラリが構成されている状況でADIC/GRAU DASライブラリおよびSTK ACSライブラリを使用する場合、DASまたはSTK ACSLM Serverを照会することはお勧めしません。手動でVOLSERを追加するようにしてください。ただし、ADIC/GRAU DASライブラリを使用する場合に、論理ライブラリがData ProtectorではなくADIC/GRAU DASユーティリティを使って構成されている場合は、Data Protectorで問題なくADIC/GRAU DASライブラリを照会できます。

ドライブクリーニング

Data Protectorには、汚れたドライブをクリーニングすることを目的として次のような方法が用意されています。

- ライブラリの組み込みクリーニングメカニズム

  一部のテープライブラリには、ドライブからヘッドクリーニングが要求されたときにドライブを自動的にクリーニングする機能が内蔵されています。この場合、ライブラリ内で汚れたドライブが検出されると、Data Protectorに対する通知なしに、クリーニングテープが自動的にロードされます。このため、アクティブなセッションが中断されて失敗することになります。このようなハードウェア固有のクリーニング手順は、Data Protectorとの互換性がないため、使用しないことをお勧めします。代わりに、Data Protectorによって管理される自動ドライブクリーニング機能を使用してください。

- Data Protectorによって管理される自動ドライブクリーニング機能

  Data Protectorでは、クリーニングテープを使用するほとんどのデバイスに対して自動クリーニングがサポートされています。SCSIライブラリおよびマガジンデバイスの場合は、どのスロットにクリーニングテープが格納されているかを定義することができます。汚れたドライブからクリーニング要求が送信されると、Data Protectorがクリーニングテープを使用してドライブをクリーニングします。自動ドライブクリーニングでは、バックアップ用の適切なメディアが用意されていれば、汚れたドライブが検出されてもセッションが

失敗することはありません。自動ドライブクリーニングは、バーコードサポートのあるライブラリ、バーコードサポートのないライブラリのどちらにも対応しています。

- 手動クリーニング

  自動ドライブクリーニングが構成されていない場合は、汚れたドライブを手動でクリーニングする必要があります。Data Protectorが汚れたドライブを検出すると、セッションモニターウィンドウにクリーニング要求が表示されます。この要求に対して、ドライブにクリーニングテープを手動で挿入する必要があります。

ヘッドのクリーニングには、若干の研磨作用を持つテープが装填された専用テープクリーニングカートリッジが使用されます。このテープカートリッジは、ドライブにロードしたときに自動的に検出され、ヘッドのクリーニングが開始されます。

制限事項

- クリーニングテープカートリッジ専用の格納スロットのいずれかに格納されているクリーニングテープをドライブクリーニングに使用する場合は、ベンダー固有のSCSIコマンドを使用する必要がありますが、これらのコマンドはData Protectorではサポートされていません。これらのクリーニングテープ専用格納スロットは、通常のSCSIコマンドではアクセスできないため、Data Protectorが管理する自動ドライブクリーニングでは使用できません。標準のスロットをクリーニングテープの格納スロットとして構成してください。
- クリーニングテープの検出と使用は、Media Agentが稼働しているシステムによって異なります。詳細は、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。
- Data Protectorによって管理される自動ドライブクリーニングを使用する場合は、他の種類のデバイス管理アプリケーションと併用しないでください。併用すると、予期せぬ結果を招く可能性があります。これは、デバイスの種類とベンダーによっては、`cleanme`要求が読み取り時にクリアされることがあるためです。
- 共通クリーニングテープを使用した論理ライブラリの自動ドライブクリーニングはサポートされていません。論理ライブラリには必ず、固有のクリーニングテープの構成が必要です。

自動クリーニングの条件

- バーコードサポートなしのライブラリの場合は、Data Protectorのデバイス定義でクリーニングテープスロットがすでに構成されており、そのスロットにクリーニングテープカートリッジが格納されます。クリーニングテープスロットは、他のライブラリスロットとともに構成する必要があります。
- バーコードサポート付きのライブラリの場合、自動ドライブクリーニングを有効にするにはバーコードサポートをアクティブにする必要があります。クリーニングテープには、プレフィックス`CLN`の付いたバーコードラベルがあります。Data Protectorでは、これに基づいてクリーニングテープのバーコードを自動的に認識することができます。
- 構成済みのドライブでは、[汚れたドライブの検出]オプションが有効になります。

Data Protectorは、ドライブのクリーニング要求通知を受け取ると、クリーニングテープを自動的にロードし、ドライブをクリーニングします。クリーニングが完了すると、セッションが再開されます。クリーニングに関するすべての活動状況は、Data Protectorサーバーログファイルディレクトリに存在する`cleaning.log`ファイルに記録されます。

スケジュールに基づいたメディアの取り出し

Data Protectorでは、スクリプトとレポート機能を使い、スケジュールに基づいてメディアを取り出すことができます。

メディアの取り出しを実行するためには、プログラムまたはスクリプトはCell Manager上に作成しなければならず、対応するインタープリターもCell Manager上にインストールされている必要があります。

レポートが作成されスクリプトへの入力として送られるように、レポートグループを設定しスケジュールすることができます。このようなレポートグループには、取り出すメディアのみをリストするレポートが含まれている必要があります(たとえば、[メディアのリスト]レポートが使えます)。(スケジュールの結果として、または、[セッションの完了]通知のような通知として)レポートグループが起動されると、Data Protectorはレポートの結果をスクリプトへの入力として送り、スクリプトを開始します。このスクリプトはレポートを解析し、Data Protector CLIの`omnimm`コマンドを使って、指定されたメディアを取り出します。

取り出し処理を続けるためにメールスロットからメディアを取り出す必要がある場合、デフォルトでは、イベントログビューアーの中で通知を受けます(たとえば、ライブラリ内の空のメールスロットよりも、取り出すべきメディアの数が多い場合)。デフォルトの時間になっても、取り出されるべきメディアがメールスロットから取り出されずに残っている場合、`omnimm`コマンドで処理が中止されます。`omnirc`ファイル内のデフォルトのタイムスパンは変更することができます。

デバイスのロック

バックアップデバイスでは、同じ物理デバイスに異なる特性を定義して、複数のデバイスのように扱うことができます。すなわち、1つの物理デバイスを複数のData Protectorバックアップデバイスに構成し、複数のバックアップセッションに使用できます。論理デバイスの内部ロックは、2つのData Protectorセッションが同じ物理デバイスに同時にアクセスするのを防止する仕組みです。たとえば、あるバックアップセッションで特定のデバイスを使用している場合、他のバックアップ/復元セッションは、そのデバイスが利用可能になるまで待機した上で、そのデバイスを使用します。バックアップセッションまたは復元セッションを開始すると、そのセッションで使用するデバイス、ドライブ、およびスロットがData Protectorによってロックされます。

初期化、スキャン、検証、コピー、またはインポートなどのメディア操作を実行するメディアセッションも、デバイスをロックします。デバイスがロックされている間、そのデバイスを他の操作でロックしたり使用したりすることはできません。メディアセッションがロックを取得できなければ、操作が失敗します。その場合は、後で操作を再試行する必要があります。

バックアップまたは復元セッションがマウント要求を発行した場合は、ロックが開放され、メディア管理操作のみ実行可能になります。この状態では、デバイスがまだ予約されたままになっているので、他のバックアップセッションや復元セッションからそのデバイスを使用することはできません。さらに、最初のメディア操作中に同じドライブに対して他のメディア管理操作を実行することはできません。マウント要求が確認されると、バックアップセッションまたは復元セッションがデバイスを再度ロックし、セッションが続行されます。

内部ロックは物理デバイスよりも論理デバイスに作用するため、1つのバックアップ仕様で1つのデバイス名を指定し、別のバックアップ仕様で同じ物理デバイスに対するもう1つのデバイス名を指定すると、競合が発生する可能性があります。バックアップのスケジュールによっては、複数のバックアップセッション内Data Protectorで同じ物理デバイスを同時に使用しようとすることがあるため、その結果、競合が発生する場合があります。こうしたことは、2つのデバイス名が別の操作、たとえばバックアップと復元、またはバックアップとスキャンといった組み合わせで使用されたときにも発生する可能性があります。Data Protectorが複数のバックアップセッションで同じ物理デバイスを同時に使おうとしたときの競合を防ぐため、デバイス構成に仮想ロック名を指定します。Data Protectorがこのロック名を使用してデバイスが利用可能かどうかを

チェックして、競合を回避します。同じ物理デバイスに対しては、どのバックアップデバイス構成においても、常に同じロック名を使用する必要があります。

> **注:**
> デバイスフローレポート内の物理デバイスに関する情報は、現在構成されているデバイスから得られるため、デバイスが実際に使用された時点の情報とは異なる可能性があります(たとえば、デバイスの論理名が最近変更された場合、内部データベース内のセッションには以前のデバイス名が含まれる可能性があります)。
>
> デバイスフローレポートは常に現在の情報を表示します。すなわち、現在の論理デバイス名による現在の物理情報です。

バックアップデバイスを無効化する

バックアップデバイスを手動で無効化する

バックアップデバイスを無効化すると、それ以降のバックアップセッションでは、そのデバイスが使用されなくなります。その場合、負荷調整が選択されていれば、バックアップ仕様のデバイスリストで次に挙げられている利用可能なデバイスが代わりに使用されます。無効化されたデバイスと同じロック名を使用するデバイスはすべて無効化されます。

そのデバイスを無効化し、他のデバイスを引き続きバックアップに利用可能(かつバックアップ用に構成済み)にしておくと、特定のデバイスで損傷が発生したり保守の必要が生じたりしたことが原因のバックアップの失敗を回避することができます。

バックアップデバイスの無効化は、デバイスが損傷したときや保守作業を実施するときに役立つ機能です。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**をクリックします。[結果エリア]に、構成済みデバイスのリストが表示されます。
3. 無効化するデバイスを右クリックし、**[プロパティ]**をクリックします。
4. **[設定内容]**タブをクリックし、**[デバイスを使用不可能にする]**オプションを選択します。
5. **[適用]**をクリックします。

以上の手順により、デバイスが無効化されます。そのデバイスをバックアップに利用できるようにするには、**[デバイスを使用不可能にする]**オプションをオフにする必要があります。

バックアップデバイスを自動で無効化する

不明なエラーが所定の回数だけ発生したデバイスを自動で無効にするようにData Protectorを構成することができます。このしきい値を指定するには、`SmDeviceErrorThreshold`グローバルオプションを`SmDeviceErrorThreshold=MaxNumberOfUnknownErrors`に設定します。

修復後にデバイスをバックアップに利用できるようにするには、デバイスを右クリックし、**[デバイスを有効にする]**をクリックします。

バックアップデバイス名を変更する

バックアップデバイスの名前を変更すると、そのデバイスでのバックアップや復元を古い名前で実行することができなくなります。

> **重要:**
> デバイスの古い名前を、そのデバイスを使ったことがあるすべてのバックアップ仕様から削除してください。そうしないと、Data Protectorがバックアブまたは復元を存在しないデバイスで実行しようとして、セッションが失敗します。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**をクリックします。[結果エリア]に、構成済みデバイスのリストが表示されます。
3. 名前を変更するデバイス名を右クリックし、続いて**[プロパティ]**をクリックします。
4. [一般]プロパティページで、[デバイス名]テキストボックスに表示されている名前を修正します。
5. **[適用]**をクリックします。

デバイスが構成済みデバイスのリストに新しい名前で表示されます。

バックアップデバイスを削除する

バックアップデバイスをData Protector構成から削除すると、そのデバイスはバックアップや復元に使えなくなります。

> **重要:**
> デバイスの古い名前を、そのデバイスを使ったことがあるすべてのバックアップ仕様から削除してください。そうしないと、Data Protectorがバックアブまたは復元を存在しないデバイスで実行しようとして、セッションが失敗します。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**をクリックします。構成されているデバイスのリストが[結果エリア]に表示されます。
3. 削除するデバイスを右クリックし、**[削除]**をクリックします。確認メッセージが表示されたら、操作を続行してよいことを確認してください。

構成済みデバイスのリストからデバイスが削除されます。

> **ヒント:**
> Data Protectorで特定のバックアップデバイスを使うことがなくなった場合は、Media Agentソフトウェアコンポーネントをシステムから削除してかまいません。この削除はクライアントコンテキストで実行できます。

マウント要求に応答する

マウント要求への応答では、必要なメディアがデバイス内にロードされていることを確認します。バックアップ対象のメディアがどのように選択されているかを知っておく必要があります。

前提条件

Adminユーザーグループに追加されているか、[モニター]のユーザー権限が付与されていることが必要です。

手順

1. コンテキストリストで**[モニター]**を選択します。
2. 必要なメディアをデバイスに挿入します。ライブラリデバイスがある場合は、マウント要求で要求されたスロットを使用しなくてもかまいません。
3. [結果エリア]で、ステータスが[マウント要求]になっているデバイスをダブルクリックして、セッションに関する情報を表示します。
4. ステータスが[マウント要求]になっているデバイスを選択します。
5. **[アクション]**メニューの**[マウント要求の確認]**を選択するか、ステータスが[マウント要求]になっているデバイスを右クリックして**[マウント要求の確認]**を選択します。

セッションとデバイスのステータスが[実行中]に変わります。

Storage Area Network (SAN)について

SANとは

Storage Area Network (SAN)は、高速のファイバーチャネル技術に基づく、データストレージ専用のネットワークです。SANは、ストレージ処理を専用のネットワークで行うことによって、アプリケーションサーバーの負荷を軽減します。Data Protectorでもこの技術がサポートされており、SANで接続されたストレージデバイスを複数のホスト間で共有できるようになっています。これにより、複数のシステムと複数のデバイスとの間の接続が実現されています。この目的で、同じ物理デバイスが複数回定義されています。たとえば、該当デバイスへのアクセスが必要な全システム上で定義されています。

SAN環境でData Protectorを使用する場合は、以下の点を考慮してください。

- デバイスは、一般に、複数のシステム間で共有されます。各システムが共有デバイスをそのシステムの(疑似)ローカルデバイスとして使用します。これは、個々のドライブと、ライブラリ内のロボティクスのどちらにも該当します。
- 複数のシステムが同じデバイスに同時にデータを書き込まないように注意する必要があります。デバイスへのアクセスは、すべてのシステム間で同期化する必要があります。このためには、ロックメカニズムを使用します。
- SANは、複数のシステムからライブラリロボティクスを管理するための優れた方法です。ロボティクスへ送信される要求が関連するすべてのシステム間で同期化されていれば、ロボティクスを直接管理することが可能です。

FC-ALおよびLIP

FC-AL (Fibre Channel Arbitrated Loops)内のテープデバイスを使用すると、バックアップセッションを中断するような異常が発生することがあります。これは、新しいFCリンクが接続/切断される時、およびFC-ALに接続されているシステムが再起動される時に、必ずFC-ALによってLIP (Loop Initialization Protocol)が実行されるためです。このFC-ALの再初期化により、実行中のバックアップが中断されます。このように中断されたジョブは、再開させる必要があります。

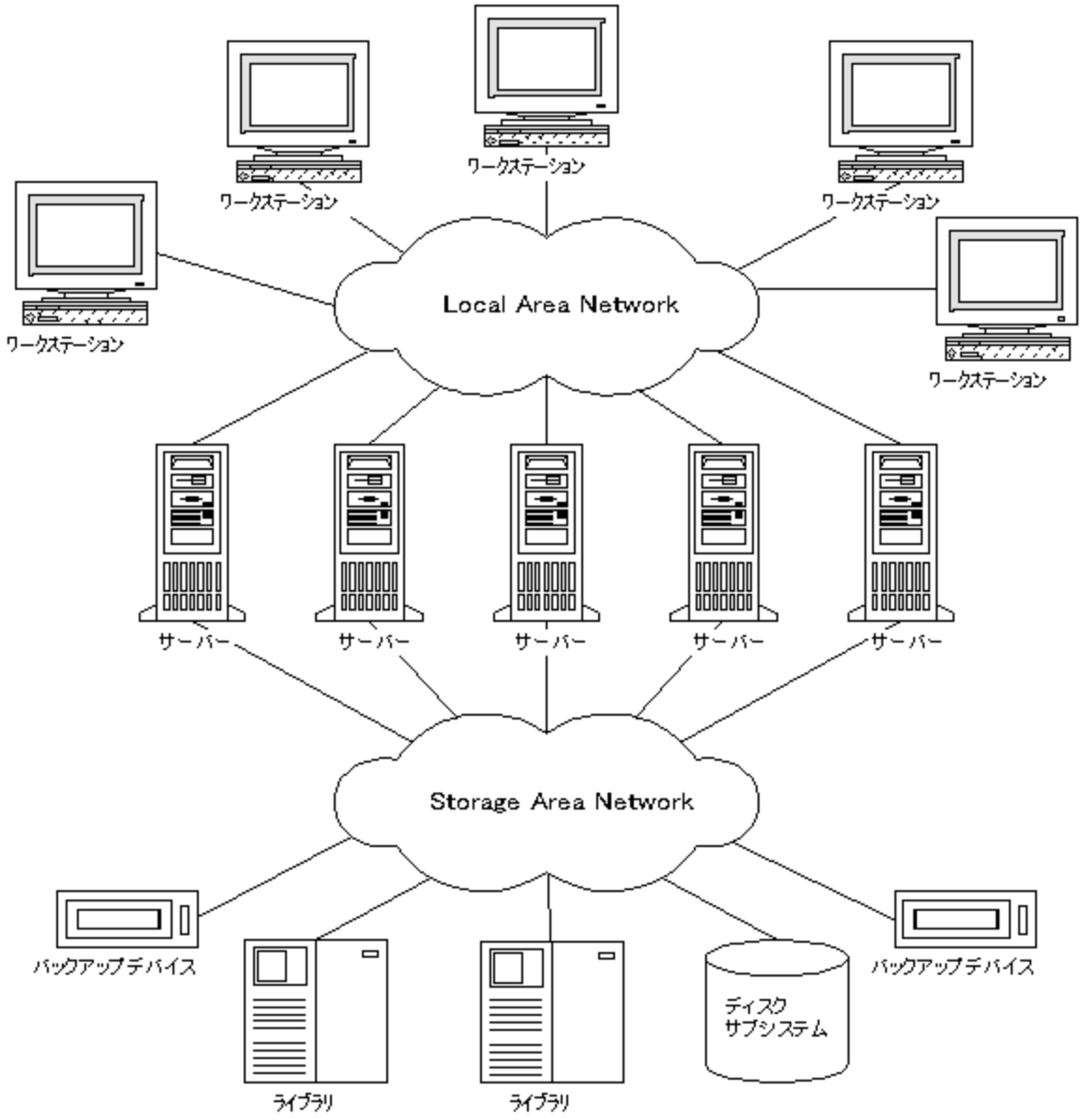
FC-ALループ上でLIPが実行される時は、アクティブなI/Oプロセスを伴うユーティリティでI/Oエラーが発生します。バックアップユーティリティが共有テープを使おうとすると、I/Oエラーが発生し、現在のバックアップセッションは失敗します。

- テープは、巻き戻すか、アンロードされます。
- バックアップセッションが中断されます。

以下をお勧めします。

- バックアップセッションの実行中に、FC-ALに対する新しいデバイスの追加や削除をしないでください。
- バックアップセッションの実行中に、FCコンポーネントに触らないでください。静電荷によりLIPが起きる可能性があります。
- Windowsの`discovery`やHP-UXの`ioscan`も使用しないでください。同様にLIPが起きる可能性があるためです。

SANにおける複数システムと複数デバイス間の接続の例



SAN環境におけるデバイスのロック

Data Protectorでは、SANのコンセプトがサポートされており、SAN環境内のバックアップデバイスを複数のシステムの間で共有できます。同じデバイスを複数のアプリケーションで共有することもできます。また、Data Protector環境内の複数のシステムの間で同じデバイスを共有することもできます。デバイスのロックは、複数のシステムの間で同じデバイスを共有している場合に、そのデバイスに対する複数のシステムからの同時アクセスを防ぐことを目的としています。

Data Protectorによって排他的に使用されるデバイスロックメカニズム

ドライブを使用しているアプリケーションがData Protectorだけであっても、同じドライブを複数のシステムから使用する必要があるときは、デバイスロックメカニズムを使うことができます。

複数のシステムからロボティクス制御を使っているアプリケーションがData Protectorだけであっても、Data Protectorはロボティクス制御を内部処理するようになっています。これは、ライブラリを制御する必要があるすべてのシステムとライブラリ制御とが同じセル内にあるという仮定に基づいています。このような場合、デバイスに対するアクセスの同期化すべてがData Protectorの内部制御によって管理されます。

複数のアプリケーションで使用されるデバイスロックメカニズム

複数のシステムでData Protectorが使われている場合は、同じ物理デバイスにアクセスするためにデバイスロックメカニズムを使う必要があります。

Data Protectorと少なくとも1つの以外のアプリケーションが同じデバイスを複数のシステムから使用する場合、すべてのアプリケーションで同じ(全般)デバイスロックメカニズムを使う必要があります。このメカニズムは、複数のアプリケーション間で機能しなければなりません。このモードは、現在Data Protectorではサポートされていません。このような必要が生じた場合、すべてのデバイスに対し、一時点においては1つのアプリケーションからの排他的アクセスしか受け付けないように、オペレーショナルルールで保証する必要があります。

間接ライブラリアクセスと直接ライブラリアクセス

SCSIライブラリデバイスまたはサイロライブラリ(ADIC/GRAUおよびStorageTek)を使用するようにData Protectorを構成した場合、クライアントシステムがライブラリロボティックにアクセスする方法には、以下の2つがあります。

間接ライブラリアクセス

間接ライブラリアクセスの場合、Data Protectorによって開始されたロボティクス制御コマンドを送るシステムは、1つだけです(デフォルトのロボティクス制御システム)。ロボティクス機能を要求するその他のシステムは要求をロボティクス制御システムに転送し、そこから実際にコマンドがロボティクスに送られます。これは、Data Protectorからの要求すべてに対し、Data Protectorの内部で透過的に行われます。

直接ライブラリアクセス

直接ライブラリアクセスの場合、どのシステムからでも直接ライブラリロボティクスに制御コマンドが送られます。そのため、どのシステムも他のシステムに依存することなく機能することができます。

直接ライブラリアクセスの場合、複数のシステムが同じライブラリにコマンドを送るときは、通信のシーケンスを調整する必要があります。

Data Protectorでは、どのライブラリの定義も、ライブラリロボティクスを制御しているホストと(デフォルトで)関連付けられています。他のホストからメディアを移動するよう要求があった場合、Data Protectorは、まずライブラリ定義で指定されたシステムにアクセスし、メディアの移動を行います。そのシステムが利用でき

ない場合は、libtabファイルを設定すれば、ローカルホストから直接ライブラリロボティクスにアクセスすることもできます。これはすべて、Data Protectorの内部で透過的に行われます。

マルチパスデバイスへの直接ライブラリアクセスが有効な場合は、構成されている順序に関係なく、最初にローカルパス(あて先クライアント上のパス)がライブラリ制御に使用されます。マルチパスデバイスの場合は、libtabファイルは無視されます。

SAN環境でデバイスを構成する

SAN環境は、1つのライブラリを使用する1つのクライアントから、複数のライブラリを使用する複数のクライアントまで、多岐にわたります。また、その複数のクライアントが、異なるオペレーティングシステムを採用していることもあります。Data Protectorから見た場合、SAN環境を構成する目的は次のとおりです。

- ライブラリロボティクスを共有する各ホストにおいて、それぞれのホストのロボティクス定義を作成する。ロボティクスを制御するホストが1つしかない場合は、デフォルトのロボティクス制御ホストに対してのみライブラリ定義が作成されます。
- ライブラリで同じ(テープ)ドライブを共有する各ホストにおいて
  - 使用するデバイスごとにデバイスの定義を作成する。
  - (物理)デバイスが別のホストからも使用される場合(共有デバイス)、ロック名を使用する。
  - 必要に応じて、ダイレクトアクセス機能を使用する場合はこの機能を選択する。使用する場合には、libtabファイルがそのホスト上に設定されている必要があります。

考慮事項

- Microsoft Cluster Server:ドライブのハードウェアパスが両方のクラスターノードで同じことを確認します。デバイスを構成したら、フェイルオーバーを実行して検証します。

構成方法

SAN構成に参加するプラットフォームによって、3つの構成方法があります。

GUIを使ったデバイスの自動構成

Data Protectorの自動構成機能では、SAN環境内の複数のホストにあるデバイスおよびライブラリを自動構成することができます。自動構成は、以下のオペレーティングシステムでサポートされています。

- Windows
- HP-UX
- Solaris
- Linux
- AIX

制限事項

SAN環境内の以下のデバイスに対しては、自動構成を使用できません。

- 混合メディアライブラリ
- DASライブラリまたはACSLSライブラリ
- NDMPデバイス

環境に接続されているバックアップデバイスは、Data Protectorが検出します。ライブラリデバイスの場合、Data Protectorは、スロット数、メディアの種類、およびライブラリに属するドライブを認識します。Data Protectorは次に、ドライブやスロットを構成する他に、デバイスについても論理名、ロック名、メディアの種類、およびデバイスファイルまたはSCSIアドレスを設定して構成します。

> **注:**
> SAN環境に新しいホストを導入した場合、構成済みのライブラリとデバイスは自動的に更新されません。
>
> - 既存のライブラリを新しいホストで使用するには、このライブラリを削除し、同じ名前を指定して新しいホスト上で新しいライブラリを自動構成します。
> - 既存のライブラリにデバイスを追加するには、ライブラリを削除し、同じ名前を指定して新しいホスト上で新しいライブラリを自動構成するか、またはドライブをライブラリに手動で追加します。

CLI(sanconfコマンド)を使用したデバイスの自動構成

sanconfコマンドを使ってSAN環境内のデバイスとライブラリを構成することができます。sanconfコマンドは、集中型メディア管理データベース(Centralized Media Management Database)(CMMDB)によって、単一Data ProtectorセルでのSAN環境およびMoM環境においてライブラリ構成を容易にするユーティリティです。このコマンドは、複数のクライアントからドライブに関する情報を収集して単一ライブラリにすることによって、SAN環境内でライブラリを自動的に構成できます。MoM環境では、sanconfを実行しているセルでCMMDBが使用されていれば、sanconfはCMMDBを使用する任意のData Protectorセル内の任意のライブラリを構成できます。sanconfは次のオペレーティングシステムで使用できます。

- Windows
- HP-UX
- Solaris

sanconfでは、以下のオペレーティングシステム上で実行されているクライアントに接続されたサポートしているデバイスを検出し、構成することができます。

- Windows
- HP-UX
- Solaris
- Linux
- AIX

このコマンドを使用して、以下の作業を行うことができます。

- 指定のData Protectorをスキャンして、ドライブのSCSIアドレスと、SAN環境内のクライアントに接続されているロボティクス制御に関する情報を収集します。
- Data Protectorクライアントのスキャンで収集した情報をもとに、指定のクライアントのライブラリおよびドライブの設定を構成または修正します。
- すべてのクライアントまたは指定のクライアントのドライブをライブラリから削除します。

デバイスのロック

sanconfコマンドは、構成対象ドライブのロック名を自動生成します。ロック名は、ドライブのベンダーID文字列、製品ID文字列、製品シリアル番号で構成されます。

たとえば、ベンダーIDが「HP」、製品IDが「DLT8000」、シリアル番号が「A1B2C3D4E5」のHPE DLT 8000ドライブのロック名は「HP:DLT8000:A1B2C3D4E5」となります。

ロック名は手動で追加することもできます。ロック名は論理デバイスごとに固有です。

sanconfコマンドが作成したロック名は変更してはなりません。手動で作成し、sanconfコマンドで構成した物理ドライブを表す他のすべての論理ドライブも、sanconfで作成したロック名を必ず使用しなければならないからです。

制限事項

- sanconfでサポートされるライブラリの一覧については、https://softwaresupport.hpe.com/にある最新のサポート一覧を参照してください。
- sanconfは以下の機能をサポートしません。
  - ドライブスロットに予備のドライブを置くこと。
  - ドライブの種類を混在させること(たとえば、DLT、9840、LTOドライブの組み合わせ)。
  - 現在、利用できないクライアントを構成すること。このようなクライアントの構成は、クライアントのスキャンで収集された情報が含まれている構成ファイルがライブラリの構成に使用される場合にのみ可能です。

推奨事項

システムの個々のデバイスについてドライバーはそれぞれ1つだけ構成するようにしてください。

sanconfコマンドの使用法については、sanconfmanページまたは『*HPE Data Protector Command Line Interface Reference*』を参照してください。

UNIXシステムでの手動構成

SAN環境でUNIXシステムに接続された共有デバイスを手動で構成する場合、以下の作業を行う必要があります。

- 使用するデバイスごとにデバイスの定義を作成する。
- ロック名を使用する。
- 必要に応じて、ダイレクトアクセス機能を使用したい場合はダイレクトアクセスを選択する。使用する場合には、そのホスト上のlibtabファイルが適切に設定されている必要があります。

構成の段階

1. デバイスを手動で構成する
2. libtabファイルを手動で構成する

ディスクへのバックアップについて

Data Protectorのディスクへのバックアップでは、テープではなく、ディスクにデータを保存します。Data Protectorでは、1つまたは複数のディスク上のディレクトリに書き込みが行われます。データは、ディスクのディレクトリに格納されるファイルに書き込まれます。

ディスクバックアップの場合、バックアップの作成前に実行する機械的な処理(テープのロードなど)がないため、テープへのバックアップより高速です。また、ディスクストレージは、急速に安価になっています。

重要なビジネスデータを処理する多くのアプリケーションでは、トランザクションの発生後、すぐにそのトランザクションをバックアップする必要があります。ディスクベースのバックアップを使用すると、営業時間中、継続してディスクにデータを書き込むことができます。

ディスクベースのバックアップデバイスとは

ディスクベースのバックアップデバイスは、概念的にテープドライブやテープスタックに似ています。ディスクベースのバックアップデバイスには、テープドライブのレポジトリに相当する1つまたは複数のディレクトリが存在します。バックアップの作成時には、テープにファイルを書き込む場合のように、ファイルデポにデータが書き込まれます。ディスクベースのバックアップデバイスは、ディスクに格納されるファイルにデータが書き込まれるため、'ファイルデバイス'とも呼ばれます。

ディスクベースのデバイスの構成方法

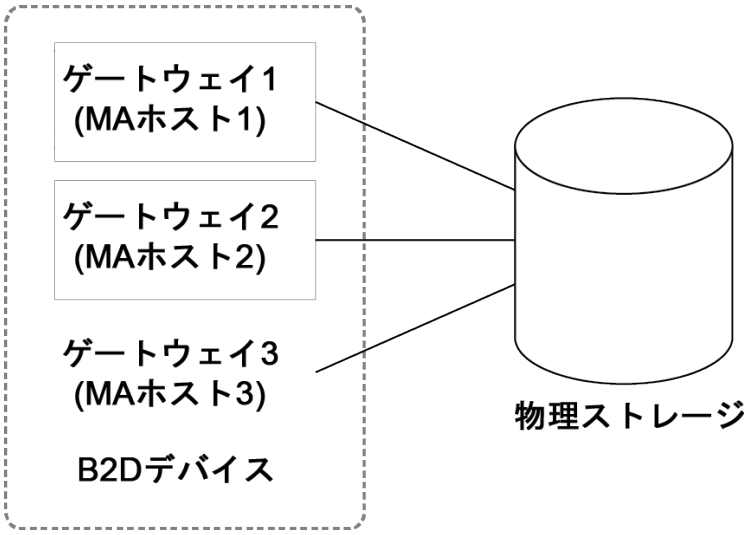
ディスクベースのバックアップデバイスは、Data ProtectorのGUIを使って構成され、Data Protectorのすべてのメディア管理機能、およびバックアップ/復元機能を使用します。

ディスクへのバックアップデバイスについて

ディスクへのバックアップ(B2D)デバイスは、データを物理ディスクストレージにバックアップするデバイスです。B2Dデバイスは、複数ホスト構成をサポートしています。これは、ゲートウェイと呼ばれる複数のホストを介して単一の物理ストレージにアクセスできることを意味します。各ゲートウェイは、Media Agentコンポーネントがインストールされているデータ Protectorクライアントです。物理ストレージは、特定のストレージセクションを表す個別のストアにパーティション分割することもできます(これは、ハードディスクのパーティション分割に似ています)。物理ストレージディスク上の個々のストアにアクセスできるのは1台のB2Dバイスのみですが、複数のB2Dデバイスが同じ物理ストレージ上の異なる複数のストアにアクセスすることはできます。

他のライブラリベースのデバイスと似ていますが、ゲートウェイで許容される柔軟性が高いため、B2Dデバイスの動作は異なります。ライブラリドライブと異なり、各ゲートウェイは単一または複数のセッションで複数のMedia Agentを同時に開始できるホストとして機能します。

B2Dデバイス(論理ビュー)



特定のゲートウェイで起動できるMedia Agentの数は、次によって定義されます。

- ゲートウェイ上限値。各B2Dゲートウェイは、並列ストリームの最大数までに制限されています。
- ストアでの接続制限値。この制限値は、B2Dデバイスの構成時にGUIで指定します。この値を指定しない場合、利用可能な最大値が使用されます。Data Protector
- 物理ストレージユニットの物理接続の制限。この値は物理ストアから取得されます。
- 実行中の動作によっては、次の入力パラメーターに従って、各Session Managerがゲートウェイ上のMedia Agentの数を調整します。
  - バックアップ対象のオブジェクトの数
  - オブジェクトの場所
  - 物理接続制限

B2Dデバイスは高速な読み取り/書き込みアクセスに対応した特殊なデータ形式を使用します。このデータ形式は、Data Protectorの従来のテープフォーマットと互換性がありません。B2Dを選択すると、データ形式が自動的に設定されます。

重複排除について

データの重複排除とは、重複するデータのバックアップを省略することでバックアップデータのサイズを縮小するデータ圧縮技術です。重複排除プロセスでは、データストリームを管理しやすいデータのチャンク(またはブロック)に分割します。次に、データチャンクの内容を相互に比較し、同じ内容のチャンクが見つかった場合に、そのチャンクを一意のチャンクへのポインターに置き換えます。つまり、同一内容のチャンクが20個見つかった場合は、一意のチャンクが1個だけ保持(バックアップ)され、残りの19個はポインターに置き換えられます。バックアップデータは重複排除ストアと呼ばれるディスクベースのあて先デバイスに書き込まれます。復元処理を実行すると、一意のチャンクが複製されて、ポインターで識別される正しい位置に挿入されます。重複排除型の復元処理では、復元プロセスをバックアップデータのリハイドレートと呼ぶこともあります。

重複排除を使用するタイミング

通常、電子メールシステムをバックアップする際にはデータの重複排除を使用します。この電子メールシステムには、たとえば、1 MBの同一の画像の添付ファイルが100件含まれている可能性があります。このシステムを従来のバックアップ技術でバックアップすると、100件の添付インスタンスがすべてバックアップされるため、約100MBのストレージスペースが必要になります。データの重複排除を使用した場合、実際に保存される添付ファイルは1件だけです。他のすべてのインスタンスは一意の格納済みコピーを参照します。この例では*重複排除率*が約100:1となります。この例はファイルレベルの重複排除と呼ばれるもので、ディスクへのバックアップデバイスと重複排除を使用する利点を理解するのに役立ちます。

重複排除の利点

一般的には、データの重複排除を行うとバックアップサービス全体の速度が上昇し、全体のストレージコストが減少します。また、ストレージに必要なディスクスペースも大幅に減少します。データの重複排除はディスクベースのシステムであるため、復元サービスのレベルが極めて高く、テープ(または他のメディア)処理のエラーも減少します。

重複排除テクノロジ

一般的に数種類の重複排除技術が利用でき、通常はハードウェアベースのソリューションとソフトウェアベースのソリューションに大別されます。これらのソリューションは、ファイル単位(シングルインスタンス)やブロック単位の重複排除といったサブグループに、さらに分類することができます。

Data Protectorでは、以下の重複排除バックエンドが利用できます。

StoreOnceソフトウェア重複排除

Data ProtectorのStoreOnceソフトウェア重複排除は、ソフトウェアベースのブロックレベルの重複排除ソリューションを提供します。

StoreOnceソフトウェア重複排除を使用する際には、以下の点に注意してください。

- 重複排除は、ディスクベースのデバイスへのバックアップのみを対象としており、テープドライブやライブラリといったリムーバブルメディアには使用できません。
- Data Protectorはソフトウェアのみの重複排除方式を使用するため(StoreOnceソフトウェア重複排除を使用する場合)、バックアップしたデータを保存する標準的なハードディスク以外のハードウェアは必要ありません。
- StoreOnceソフトウェア重複排除は、ハッシュベースのチャンク化技術を使用してデータストリームをまとまった大きさのデータチャンクに分割します。
- 重複排除処理では、重複するデータが削除され、データのコピーが1つと、一意のデータへの参照リンクだけが残されます。重複排除処理で格納するデータは一意のデータのみのため、必要なストレージ容量を削減することができます。
- バックアップ仕様でディスクターゲットデバイスへのバックアップを指定すると、Data Protectorは重複排除型のバックアップを実行します。

HPE StoreOnceバックアップシステムデバイス

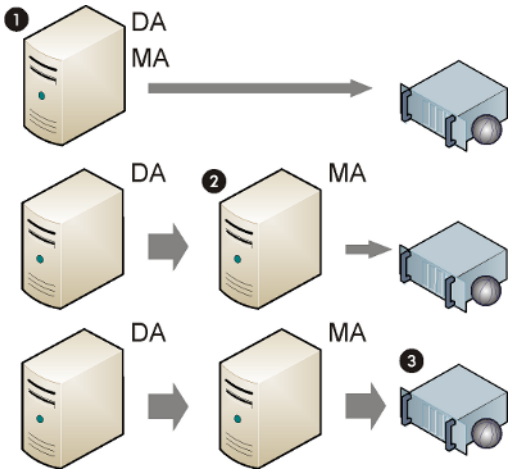
HPE StoreOnceバックアップシステムデバイスは、重複排除をサポートするディスク間(D2D)バックアップデバイスです。

重複排除の設定

Data Protectorは、次のような重複排除の設定をサポートしています。

- ソース側重複排除(1) - ソース側でデータの重複排除が行われます(バックアップされるシステム)。
- サーバー側重複排除(2) - Media Agentシステムでデータの重複排除が行われます(ゲートウェイ)。
- ターゲット側重複排除(3) - ターゲットデバイスでデータの重複排除が行われます(StoreOnceバックアップシステムまたはStoreOnceソフトウェアシステム)。

重複排除の設定



ソース側重複排除

ソース側重複排除(1)では、バックアップされるクライアントにDisk Agentと共にMedia Agentがインストールされ、クライアントがゲートウェイ(ソース側ゲートウェイ)になります。重複排除はクライアント上のMedia Agentが行い、重複排除済みデータのみをターゲットデバイスに送るため、ネットワーク全体のトラフィックが減少します。同時ストリームは、負荷調整設定によって数が制限されます。1つのMedia Agentによるローカルオブジェクトのバックアップが終了すると、次のクライアントシステムで別のMedia Agentが新たに起動します。ただし、バックアップされるシステムが重複排除をサポートしている必要があります。

サーバー側重複排除

サーバー側重複排除では、独立したMedia Agentクライアント(ゲートウェイ)上でMedia Agentによって重複排除が実行されます。このため、バックアップ済みシステムとターゲットデバイス上の負荷は低下しますが、Disk AgentとMedia Agent間のネットワークトラフィックの量は減少しません。

Media Agentクライアントが重複排除をサポートしている必要があります。サーバー側重複排除では、重複排除をローカルで行えないクライアントからのデータの重複排除が行えます。

ターゲット側重複排除

重複排除プロセスはターゲットデバイス上で実行されます。バックアップ対象のデータは、クライアント(ゲートウェイ)上にインストールされたMedia Agentから受け取ります。ターゲット側重複排除では、Media Agentと重複排除システム間のネットワークトラフィックの量が減少しません。

ファイルライブラリデバイスについて

ファイルライブラリデバイスは、ユーザーが定義する、内部ハードディスクドライブまたは外部ハードディスクドライブに格納されるデバイスです。ファイルライブラリデバイスは、ディレクトリのセットで構成されます。このデバイスに対してバックアップを実行すると、これらのディレクトリに自動的にファイルが作成されます。ファイルライブラリのディレクトリに格納されるファイルは、ファイルデポと呼ばれます。

Data Protectorによって設定されたファイルライブラリデバイスの容量には、上限はありません。ファイルライブラリデバイスの最大サイズは、ディレクトリが格納されているファイルシステムの最大サイズによって決まります。たとえば、Linux上で稼動しているファイルライブラリデバイスの最大サイズは、Linuxのファイルシステムに保存可能な最大サイズになります。

ファイルライブラリデバイス内の各ファイルデポの容量は、最初にデバイスを構成するときに指定します。デバイスの使用中に、ファイルライブラリのプロパティを使用してファイルデポのサイズプロパティを再設定できます。

ファイルライブラリデバイスは、Data Protectorの検索パスに登録されている任意のディレクトリに格納できます。格納先のハードドライブは、ローカルでもリモートでもかまいません。検索パスは、ファイルライブラリデバイスの構成時に指定できます。

ディスクベースのデバイスの管理方法

使用中のディスクベースのデバイスがすべてフル状態になりつつある場合、それらのバックアップを行う前に以下のいずれか処理を実行する必要があります。

- テープへのデータの移動を開始し、ファイルデバイスまたは1つ以上のファイルスロットを空にする。
- ファイルデポをリサイクルする。
- 新しいファイルデポをファイルデバイスに追加する。

ファイルデポ

ファイルデポは、バックアップからファイルライブラリデバイスへのデータを格納するファイルです。

ファイルデポの作成

ファイルライブラリデバイスを使用した初めてのバックアップを開始すると、Data Protectorによってファイルデポが自動的に作成されます。Data Protectorは、デバイスによって作成されるデータバックアップセッションごとに1つのファイルデポを作成します。バックアップ対象のデータ量がデフォルトの最大ファイルデポサイズより多い場合、Data Protectorは、1つのバックアップセッションに対して複数のファイルデポを作成します。

ファイルデポ名

各ファイルデポの名前は、システムによって自動生成される一意識別子です。

Data Protectorは、メディア識別子もファイルデポに追加します。メディア識別子は、メディアプールにおけるメディアとしてファイルデポを識別します。メディアに追加されるこの識別子によって、復元時に特定のバックアップセッションを識別することができます。この識別子は、ファイルデポのプロパティとともに表示されます。

ファイルデポをリサイクルした場合、ファイルデポのアイコンはGUIに表示されたままとなりますが、ファイルデポ名は消えることがあります。

ファイルデポサイズ

ファイルデポのサイズは、ファイルライブラリデバイスの作成時に定義します。サイズを定義する際は、ファイルデポの最大サイズをはじめ、デバイスのサイズプロパティをすべて指定します。ファイルデポのサイズプロパティを入力するのは一度だけですが、すべてのファイルデポにグローバルに適用されます。1つのセッションでバックアップするデータサイズが指定のファイルデポサイズより大きい場合、ファイルライブラリデバイスに割り当てられているディスクスペースがなくなるまで、Data Protectorが自動的にファイルデポを追加作成します。

デフォルトのファイルデポサイズは5GBです。この値を増やすことはできますが(最大2TB)、パフォーマンスが低下する可能性があります。

ファイルデポのスペース消費

Data Protectorは、デバイスに利用できるディスクスペースがなくなるまで、ファイルデポを自動的に作成します。ファイルライブラリデバイス用として確保しなければならない容量は、デバイスを最初にセットアップしたときのデバイスプロパティで定義します。

満杯ディスクの取り扱い

ファイルライブラリデバイスに利用できる総ディスクスペースがユーザー指定レベル未満となった場合、通知が行われます。

ディスク当たりのデバイス数

ファイルライブラリデバイスには、1つまたは複数のディレクトリを格納することができます。1つのファイルシステムに存在し得るディレクトリは、1つだけです。

多様なディスクにファイルデポが散在している場合、2つのファイルライブラリデバイスからのファイルデポを1つのディスクに入れることは好ましくありません。これは、プロパティが異なっているとData Protectorに矛盾が生じる可能性があるためです(一方のファイルライブラリデバイスのファイルデポのディスクスペースが20MBと指定されているが、他方のファイルライブラリデバイスでは10MBである、など)。

ファイルライブラリデバイスのプロパティを設定する

ファイルライブラリデバイスのプロパティは、ファイルライブラリデバイスの初期構成時に設定できます。また、ファイルライブラリデバイスの稼動後に変更することもできます。

プロパティの初期設定

手順

1. ファイルライブラリデバイスの構成中に、ファイルライブラリデバイスディレクトリを選択し、**[プロパティ]**をクリックします。

2. デバイスのサイズに関するプロパティを指定します。**[OK]**をクリックします。
3. **[次へ]**をクリックして、ファイルライブラリデバイスの構成を続けます。

デバイスプロパティを変更する

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を展開し、変更対象のファイルライブラリデバイス名をクリックします。
3. ファイルライブラリデバイス名を右クリックし、**[プロパティ]**をクリックします。
4. **[レポジトリ]**タブをクリックします。リストからファイルライブラリのパスを選択します。
5. **[プロパティ]**をクリックします。デバイスのサイズに関するプロパティをすべて指定し、**[OK]**をクリックします。

Data Protectorでは、デバイスのプロパティが変更された後にファイルライブラリデバイスで作成された各ファイルデポに対して、[プロパティ]ダイアログで指定されたプロパティが適用されます。デバイスのプロティの変更前に作成されたファイルデポのプロパティはそのまま維持されます。

ファイルライブラリデバイスを削除する

ファイルライブラリデバイスに保護されたデータが格納されていると、ファイルライブラリデバイスを削除できません。そのため、ファイルライブラリを削除する前に、そのデバイスに格納されている各ファイルデポのデータ保護レベルを変更する必要があります。

削除の段階

1. データ保護をチェックする
2. ファイルデポをリサイクルする
3. エクスポート済みのファイルデポのアイコンを削除する
4. ファイルライブラリデバイスを削除する

データ保護をチェックする

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、削除するファイルライブラリデバイスの名前を選択し、ファイルライブラリの[ディレクトリ]フォルダーを開きます。
3. [結果エリア]に、[保護]列が表示されているかどうかを調べます。保護レベルが[無期限]になっているファイルデポをチェックします。

ファイルデポをリサイクルする

ファイルデポやファイルライブラリデバイス全体をリサイクルし削除することによって、ディスクスペースを解放することができます。

個々のファイルデポ単位、またはファイルライブラリ内のファイルデポすべてを一括でリサイクルできます。つまり、リサイクルされた項目が占有するディスクスペースが回復され、次のバックアップ時に使用できるようになります。これは、保護されていないファイルデポを削除し、新しいファイルデポを作成することによって実現されます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、ファイルライブラリデバイスのファイルデポを展開します。
3. [結果エリア]で、個々のファイルデポをクリックして、リサイクルするファイルデポを選択します。
4. 選択したファイルデポを右クリックし、**[エクスポート]**をクリックします。

   ファイルデポをエクスポートすると、そのファイルデポに関する情報がIDBから削除されます。Data Protectorは以降、このファイルデポの存在を認識しなくなります。しかし、このファイルデポの情報は依然として保持されているため、後でファイルデポの回復が必要になったときにインポートすることができます。
5. 選択したファイルデポを右クリックし、**[リサイクル]**をクリックします。
6. ファイルライブラリ内のデータ保護レベルがフル'の各ファイルデポについて、この手順を繰り返します。

ファイルデポがリサイクル対象として指定されると、Data Protector GUIにはData Protectorによって自動的に生成されたファイルデポの名前が表示されなくなり、ファイルデポのアイコンだけが表示されます。エクスポート済みのファイルデポのアイコンは削除できます。

エクスポート済みのファイルデポのアイコンを削除する

ファイルデポがエクスポートされると、Data Protector Managerではその名前は表示されなくなり、ファイルデポのアイコンのみが表示されます。

手順

1. [結果エリア]で、削除対象のアイコンをクリックします。
2. 選択したアイコンを右クリックし、**[削除]**をクリックします。
3. 削除するすべてのエクスポート済みファイルデポのアイコンについて、この作業を繰り返します。

この作業によりGUIからアイコンが削除されますが、物理的にファイルはIDBから削除されません。

ファイルライブラリデバイスを削除する

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、削除するファイルライブラリの名前を選択します。

3. ファイルライブラリデバイスを右クリックし、**[削除]**をクリックします。

ファイルライブラリデバイスがIDBから削除されます。

ジュークボックスデバイスについて

ジュークボックス物理デバイス

ジュークボックスは、ライブラリデバイスです。ジュークボックスには、光磁気メディアまたはファイルメディアを格納できます。デバイスがファイルメディアの格納に使用された場合、その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。ファイルジュークボックスデバイスに格納するメディアの種類は、初期構成時に定義します。UNIX上でジュークボックス光磁気ライブラリを実行している場合は、エクスチェンジャースロットまたはプラッタのサイドごとに構成されたUNIXデバイスファイルが必要です。

ジュークボックスファイルデバイス

ファイルジュークボックスデバイスは、テープスタックと同じような論理デバイスです。ファイルジュークボックスデバイスには、初期デバイス構成でユーザーが定義したサイズのスロットが付いています。このデバイスの構成は、手動で行います。ファイルジュークボックスのプロパティは、使用中に変更することができます。ファイルジュークボックスデバイスをファイルメディアの格納に使用すると、テープではなく、ディスクに書き込みが行われます。ファイルジュークボックスデバイスは、データをファイルに保存します。ファイルは、テープデバイスのスロットに相当します。

このデバイスの標準の最大データ記憶容量は、ファイルジュークボックスを実行するオペレーティングシステムがファイルシステムに格納できるデータ量によってのみ制限されます。ジュークボックスデバイスの各スロットの最大容量は、2TBです。ただし、Windowsシステムでは100MBから50GBまで、UNIXシステムでは100MBから2TBまでのスロットサイズが推奨されます。たとえば1TBのデータをバックアップする場合には、次のようなデバイス構成が可能です。

Windowsシステムの場合: 各10GBのファイルスロット100個を備えたファイルジュークボックスデバイス1個

UNIXシステムの場合: 各4 GBのファイルスロット250個を備えたファイルジュークボックスデバイス1個

ジュークボックスファイルデバイスのパフォーマンスを高めるには、1つのディスクにつき1個のデバイスだけ、1つのデバイスにつき1個のドライブだけを使用するとよいでしょう。また、Data Protectorバックアップ/復元の実行中には、他のアプリケーションとディスクとの間で大量のデータ転送を行わないようにしてください。

WindowsとUnixにおける推奨スロットサイズ

利用可能なディスクスペース	スロット数	スロットサイズ
1TB	100	10
5TB	250	20
10TB	250	40

ファイルジュークボックスデバイスのメンテナンス方法

使用しているファイルジュークボックスデバイスの空き容量がなくなった場合には、バックアップを続ける前に以下のいずれかを行う必要があります。

- テープへのデータの移動を開始し、ファイルデバイスまたは1つ以上のファイルスロットを空にする。
- ジュークボックススロットをリサイクルする。
- 新しいジュークボックススロットをファイルデバイスに追加する。

ファイルジュークボックスデバイスを構成する

作成するデバイスは、IDBが置かれているディスク以外のディスクに置くことをお勧めします。そうすることで、データベースが使用するのに十分な量のディスクスペースが確保されます。このデバイスとIDBを別のディスクに置くことによっても、パフォーマンスは向上します。

ファイルジュークボックスデバイスの構成

> **重要:**
> 以下の点に注意してください。
>
> - ファイルジュークボックスデバイスを構成する際に、既存のデバイス名を使用しないでください。既存のデバイスが上書きされます。
> - 複数のデバイスを構成する際に、同じデバイス名を使用しないでください。同じ名前にした場合、デバイスがアクセスされるたびにそのデバイスは上書きされます。

前提条件

- Windowsシステムの場合は、デバイスとして使用するファイルのWindows圧縮オプションを無効にします。
- デバイスを作成する前に、デバイスが格納されるディレクトリをディスク上に作成しておく必要があります。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックして、ウィザードを起動します。
3. [デバイス名]テキストボックスにデバイスの名前を入力します。
4. [説明]テキストボックスに必要に応じて説明を入力します。
5. [デバイスの種類]リストで、デバイスの種類として**[ジュークボックス]**を選択します。
6. [クライアント]リストでクライアントの名前を選択します。
7. 必要に応じて、ライブラリ管理コンソールの有効なURLアドレスを[管理コンソールのURL]テキストボックスに入力します。
8. **[次へ]**をクリックします。
9. ジュークボックスのファイル/ディスクのセットを指定します。複数のファイルやディスクを指定する場合

は、/tmp/FILE 1-3のように、ダッシュで区切ります。指定し終えたら、**[追加]**をクリックします。光磁気のジュークボックスの場合、ディスク名の最後はA/aまたはB/bとする必要があります。**[次へ]**をクリックします。

10. [メディアの種類]リストで、構成するデバイス用に**[ファイル]**を選択します。
11. **[完了]**をクリックして、このウィザードを終了します。ライブラリドライブを構成するかどうかを確認するメッセージが表示されます。**[はい]**をクリックすると、ドライブ構成ウィザードが表示されます。

ファイルジュークボックスデバイス内のドライブの構成

手順

1. [デバイス名]テキストボックスにデバイスの名前を入力します。
2. [説明]テキストボックスに必要に応じて説明を入力します。
3. 選択したメディアの種類に対応するメディアプールを指定します。既存のプールを[メディアプール]リストから選択するか、新しいプール名を入力します。新しいプール名を入力した場合は、プールが自動的に作成されます。すべてのドライブを1つのメディアプールに含めることも、各ドライブを個別のメディアプールに割り当てることもできます。**[次へ]**をクリックします。
4. オプションで、**[デバイスを復元で使用可]**および**[デバイスをオブジェクトコピーのソースデバイスとして使用可]**を選択し、**[デバイスタグ]**を指定します。
5. **[完了]**をクリックしてウィザードを終了します。

ドライブ名が構成済みドライブのリストに表示されます。ドライブをスキャンすると、構成を確認できます。

ファイルジュークボックスのスロットをリサイクルする

データ保護はファイルジュークボックス内の個々のファイルスロットについて設定されるため、[保護]を**[なし]**に設定することで、個々のスロットをリサイクルすることができます。このため、小さなスロットが複数あると柔軟性が向上し、データ保護と記憶領域保持管理がより効率的になります。ファイルジュークボックスデバイス内のスロットをリサイクルすると、そのデータ保護がなくなり、スロットをバックアップに再利用できるようになります。スロット内のデータは、次に行われるバックアップセッションによって上書きされます。

> **重要:**
> この方法を使用すると、メディア上にすでに存在しているデータが上書きされ、失われます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、ファイルジュークボックスデバイススロットを展開します。
3. [結果エリア]で、リサイクルするスロットを選択します。
4. 選択したスロットを右クリックし、**[リサイクル]**をクリックします。

スタンドアロンデバイスについて

スタンドアロン物理デバイス

スタンドアロンデバイスは、一度に1つのメディアに対する読み取り/書き込みを行うドライブを持つ、DDSやDLTのようなシンプルなデバイスです。スタンドアロンデバイスは、小規模なバックアップに使用します。メディアが一杯になった場合、オペレーターはバックアップを継続するためにメディアをすぐに新しいものに手動で交換する必要があります。このため、スタンドアロンデバイスは大規模な無人バックアップには適していません。

スタンドアロンファイルデバイス

スタンドアロンファイルデバイスは特定のディレクトリに存在するファイルで、テープにデータを書き込む代わりに、このファイルにデータをバックアップすることができます。スタンドアロンファイルデバイスは、データをファイルに保存します。ファイルは、テープデバイスのスロットに相当します。スタンドアロンファイルデバイスは、小規模なバックアップを行う際に便利です。

ファイルデバイスの最大容量は2TBです。ただし、Windowsシステムでは100MBから50GBまで、UNIXシステムでは100MBから2TBまでのスタンドアロンファイルデバイスサイズが推奨されます。Data Protectorがファイルシステムの空き領域を測定することは一切なく、デフォルト容量または指定容量がファイルサイズの上限であるとみなされます。圧縮ファイルをファイルデバイスに使用することはできません。デフォルトのサイズは、`FileMediumCapacity`グローバルオプションを設定することによって変更できます。

スタンドアロンファイルデバイスのデフォルトの最大サイズは100 MBです。これを超えるサイズのバックアップを行う場合は、`FileMediumCapacity`グローバルオプションを設定することによってデフォルトのサイズを変更できます。グローバルオプションの設定の詳細については、「HPE Data Protectorのグローバルオプションをカスタマイズする」または「グローバルファイルの編集によるオプションのカスタマイズ」を参照してください。

たとえば、20GBが最大値である場合(20Gb = 20000 MB)、`FileMediumCapacity`グローバルオプションを次のように設定します。

```
# FileMediumCapacity=MaxSizeInMBytes

FileMediumCapacity=20000
```

ファイルデバイスの容量は、メディアを最初にフォーマットするときに指定します。メディアを再フォーマットするときに新しいサイズを指定しても、最初に指定したサイズが適用されます。ファイルデバイスの容量を変更するには、システムからファイルを削除する必要があります。

サイズを指定するときは、ファイルシステム上に少なくとも1MB以上の空き容量が残るようにしてください。ファイルデバイスがサイズの上限に達すると、マウント要求が発行されます。Data Protector

スタンドアロンファイルデバイスのパフォーマンスを高めるには、1つのディスクにつき1個のデバイスだけ、1つのデバイスにつき1個のドライブだけを使用することをお勧めします。また、Data Protectorバックアップ/復元の実行中には、他のアプリケーションとディスクとの間で大量のデータ転送を行わないようにしてください。

ファイルデバイスは、Data Protectorの検索パスに登録されている任意のディレクトリに格納できます。格納先のハードドライブは、ローカルでもリモートでもかまいません。検索パスは、ファイルデバイスの構成時に指定できます。

スタンドアロンファイルデバイスを構成する

作成するデバイスは、IDBが置かれているディスク以外のディスクに置くことをお勧めします。そうすることで、データベースが使用するのに十分な量のディスクスペースが確保されます。このデバイスとIDBを別のディスクに置くことによっても、パフォーマンスは向上します。

> **重要:**
> 以下の点に注意してください。
> - ファイルジュークボックスデバイスを構成する際に、既存のデバイス名を使用しないでください。既存のデバイスが上書きされます。
> - 複数のデバイスを構成する際に、同じデバイス名を使用しないでください。同じ名前にした場合、デバイスがアクセスされるたびにそのデバイスは上書きされます。

前提条件

- Windowsシステムの場合は、デバイスとして使用するファイルのWindows圧縮オプションを無効にします。
- デバイスを作成する前に、デバイスが格納されるディレクトリをディスク上に作成しておく必要があります。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックして、ウィザードを起動します。
3. [デバイス名]テキストボックスにデバイスの名前を入力します。
4. [説明]テキストボックスに必要に応じて説明を入力します。
5. [クライアント]リストでクライアントの名前を選択します。
6. [デバイスの種類]リストで、デバイスの種類として**[スタンドアロン]**を選択し、**[次へ]**をクリックします。
7. テキストボックスに、ファイルデバイスのパスとファイル名を入力します(例: `c:\My_Backup\file_device.bin`)。
8. **[追加]**をクリックし、**[次へ]**をクリックします。
9. [メディアの種類]リストで、メディアの種類として**[ファイル]**を選択します。
10. 選択したメディアの種類に対応するメディアプールを指定します。既存のプールを[メディアプール]ドロップダウンリストから選択するか、新しいプール名を入力します。新しいプール名を入力した場合は、プールが自動的に作成されます。
11. **[完了]**をクリックしてウィザードを終了します。

デバイス名が構成済みデバイスのリストに表示されます。デバイスをスキャンすると、構成を確認できます。

この時点で、Data Protectorがデバイスを特定できるようになりますが、実際にはまだディスク上には存在していません。ディスクをバックアップに使えるようにするには、フォーマットする必要があります。

第9章: メディア

メディア管理について

Data Protectorには、多数のメディアを簡単かつ効率的に管理できる強力なメディア管理機能があります。バックアップ、復元、およびメディア管理イベントに関する情報は、IDBを使用して保存されます。

Data Protectorのメディア管理には、以下の特長があります。

- データが誤って上書きされないようにデータを保護できます。
- メディアプールを使用することによって、個々のメディアを意識せずに多数のメディアをまとめて管理できます。
- メディアに物理的にアクセスすることなく、Data Protector Cell Manager間でメディア関連カタログデータすべてを転送する機能です。
- フリープール機能により、空きメディアが存在しない場合にバックアップが失敗するのを回避できます。
- すべてのメディアや各メディアの状態を追跡でき、その情報を複数のData Protectorセル間で共有できます(データ保護の有効期限、バックアップ時にそのメディアを使用できるかどうか、各メディアにバックアップされている情報に関するカタログ情報など)。
- 特定のバックアップに使用するメディアとデバイスを明示的に定義できます。
- Data Protectorメディアおよびその他の代表的なテープフォーマットの自動認識が可能です。
- バーコードをサポートしている大規模ライブラリおよびサイロデバイスに対して、バーコードの認識とサポートが可能です。
- メディア情報が集中管理されており、複数のData Protectorセル間で共有できます。
- メディアのボールティング(アーカイブ/オフサイト保管)をサポートしています。
- メディア上のデータの追加コピーを対話式または自動的に作成できます。
- フィルタリングとページングの詳細な設定を行えます。

[デバイス/メディア]ビューをカスタマイズする

グローバルオプション`MediaView`、`MagazineView`、`SCSIView`、`ExternalView`、`JukeboxView`、`ACSView`、`DASView`を構成して[デバイス/メディア]コンテキストのデフォルトビューをカスタマイズできます。ライブラリまたはメディア管理のコンテキストで表示される属性に対応するトークン文字列を指定して、これらの属性をカスタマイズします。詳細については、HPE Data Protectorのグローバルオプションをカスタマイズするを参照してください。

メディアプールについて

メディアプールには、同じ種類の複数のバックアップメディアが含まれます。通常のバックアップ用とアーカイブバックアップ用のメディアプールをそれぞれ別に作成したり、部署ごとにメディアプールを作成するなど、用途に応じて複数のメディアプールを使い分けることができます。各メディアプールは、メディア使用方針および割り当てポリシー、およびメディア状態要素を定義します。

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同じ種類の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。フリープールを使用することで、フリーメディアが存在しない場合にバックアップが失敗するのを回避できます。

保護されているメディアは、SAPプールなど、特定のプールに所属しますが、フリーメディアは他のいくつかのプールが使用しているフリープールに自動的に移動させることができます。この共通のフリープールは、このフリープールを使用しているすべてのプールのフリーメディアの割り当てに使用できます。各メディアプールについて、フリープールとリンクするかどうかを設定できます。

デフォルトのメディアプール

デフォルトのメディアプールは、デバイス定義の一部としてData Protectorが提供しているプールです。バックアップ仕様にメディアプールが指定されていない場合に、このプールが使用されます。

フリープールの特性

フリープールを使用すると、複数のメディアプールの間でフリーメディアを共有できます。これによって、マウント要求が発生してオペレーターの介入が必要になる頻度が低くなります。フリープールを使用するかどうかは、任意です。

フリープールの使用を検討する場合は、次の点に注意してください。

フリープールのプロパティ

フリープールには、以下のような特徴があります。

- メディアプールとリンクされている場合や空でない場合は削除できません。
- 通常のプールとは異なり、フリープールは保護されたメディアを保持できないため、割り当てに使用できません。このため、フリープールに対して割り当てポリシーオプション([厳格]/[緩和]、[追加可能]/[追加不可能])を設定することはできません。
- Data Protectorフリーメディアのみ(不明のメディアまたは空のメディアを含まない)で構成されます。

フリープールを使用するタイミング

通常のプールとフリープールの間でメディアが移動されるのは、以下の2つの場合です。

- 通常のプール内のフリーメディアがなくなると、Data Protectorによってフリープールからメディアが割り当てられます。このとき、メディアは自動的に通常のプールに移動されます。
- 通常のプール内のメディア上のデータがすべて期限切れになると、そのメディアはフリープールに自動的に移動されます。

メディア品質の計算

メディアの品質では、「リンクされた」プール間の平均値が計算されます。メディア状態要素は、フリープールに対してのみ構成可能であり、フリープールを使用するすべてのプールに継承されます。フリープールを使用しないプールの場合は、それらのプール用の計算ベースが別途使用されます。

フリープールの制限事項

- 保護されたメディアは、フリープールに移動できません。
- インポート、コピー、およびリサイクルのように、保護されたメディアを対象とする操作は、フリープール内のメディアに対して実行できません。
- マガジンサポートオプションが選択されたプールでは、フリープールを使用できません。
- フリープールの使用時には、プール間で一時的(1日)に不整合が生じることがあります(たとえば、保護されていないメディアが通常のプールに含まれている場合、そのメディアがフリープールに移動されるまでに待ち時間が生じることがあります)。
- フリープールに異なるデータ形式のメディアが含まれている場合、Data Protectorは必要があれば割り当てられたメディアを自動的に再フォーマットします。たとえば、NDMPメディアは通常メディアに再フォーマットされます。

メディアプールのプロパティ

メディアプールの属性は、メディアプールを構成するときに指定します。一部のプロパティは後で変更できます。

メディアプールプロパティの詳細については、『HPE Data Protectorヘルプ』を参照してください。

[メディアプールプロパティ - 一般]

- 説明
- プール名
- メディアの種類

メディアプールプロパティ - 割り当て

割り当て

メディア割り当てポリシーは、メディアプール内のすべてのメディアの使用頻度が均等になるようにメディアにアクセスする順序を定義します。以下のいずれかのオプションを選択します。

- 厳格
- 緩和
- フォーマットされていないメディアを先に割り当てる
- フリープールを使用

- フリーメディアをフリープールに移動
- マガジンのサポート

メディアプールプロパティ - 状態

メディア状態要素

メディア状態要素は、メディアの状態(バックアップメディアとしての信頼性)を判定するしきい値を定義します。たとえば、古いメディアや磨耗したメディアへのバックアップは読み書きエラーが発生する確率が高くなります。Data Protectorでは、このしきい値に基づいて、[良好]、[普通]、[不良]のいずれかの状態が検出されます。状態要素は、個々のメディアに対して設定されるのではなく、メディアプール全体に対して設定されます。

> **重要:**
> Data Protectorがメディアの状態を正確に算出できるようにするには、メディアをメディアプールに追加するときに新しいメディアを使用します。

> **注:**
> あるプールがフリープールオプションを使用する場合、そのメディア状態ファクターはフリープールから継承されます。

メディア状態要素として、以下の2通りのしきい値のいずれかを選択できます。

- 最大上書き数
- 有効期限(月)

メディアプールプロパティ - 使用法

メディア使用ポリシーは、既に使用されているメディアに新しいバックアップを追加する方法を制御します。以下のいずれかのオプションを選択します。

- 追加可能
- 追加不可能
- 増分のみ追加可能

メディアプールの品質

プールメディアプールの品質内で最も質が低いメディアは、メディアプールの質を決定します。たとえば、プール内のいずれかのメディアの状態が[不良]になると、メディアプール全体の状態も[不良]になります。

メディアの品質は、メディアへのデータの書き込み能力や、メディアからのデータの読み取り能力に影響するため、バックアップ用のメディアの選択方法を左右します。[良好]状態のメディアは、[普通]状態のメディアに優先して選択されます。[不良]状態のメディアは、選択対象から除外されます。

メディアの状態は、以下のメディア状態要素に基づいて判定されます。

- 良好
- 普通

- 不良

メディアの状態の計算に使用するメディア状態要素は、メディアプールの[条件]プロパティページで変更できます。メディア状態要素を変更すると、そのメディアプール内のすべてのメディアの状態が新しい要素に基づいて計算されるようになります。

デバイスエラーとメディア品質

バックアップ中にデバイスに障害が発生すると、このデバイスでバックアップに使用されているメディアは不良とマーキングされます。これによって、この問題が不良メディアが原因だった場合に将来のエラーの発生が防止されます。

このエラーがドライブの汚れによるものであった場合、ドライブをクリーニングし、そのメディアを検証して状態をリセットします。

不良とマークされたメディアがプールに表示されないかどうかを確認するようにしてください。各メディアの状態に関する詳細情報は、[検証]を使用して得ることができます。メディアを単にリサイクルする方法はお勧めできません。

メディアプールを作成する

Data Protectorにはデフォルトのメディアプールがありますが、ユーザーの要件に合わせてメディアプールを作成できます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開して**[プール]**を右クリックし、**[メディアプールの追加]**をクリックして、ウィザードを起動します。
3. [プール名]テキストボックスにメディアプールの名前を入力し、必要に応じて、[説明]テキストボックスに説明を入力します。バックアップデバイスと使用するメディアの種類を[メディアの種類]ドロップダウンリストから選択します。**[次へ]**をクリックします。
4. 以下のオプションを設定します。
   - 必要に応じて、メディアの使用法およびメディア割り当てポリシーのデフォルト設定を変更します。
   - フリープールを使用するには、**[フリープールを使用]**オプションを最初に選択し、次にドロップダウンリストからフリープールを選択します。
   - フリーメディアのフリープールへの自動的割り当て解除を無効にするには、**[フリーメディアをフリープールに移動]**オプションを選択します。
   - マガジンをサポートしているデバイスに対してメディアプールを構成する場合は、**[マガジンのサポート]**オプションを選択します。このオプションをフリープールと一緒に使用することはできません。

   [次へ]をクリックします。
5. 必要に応じて、[メディア状態要素]ダイアログの設定を変更します。
6. **[完了]**をクリックしてウィザードを終了します。これによって、メディアプールが作成されます。

> **ヒント：**
> 既に構成されているメディアプールを変更できます。ただし、メディアの種類は変更できません。

メディアプールを変更する

ユーザーの要件に合うようにメディアプールプロパティを変更できます。メディアプールの名前、その説明、メディアの使用法および割り当てポリシー、またはメディア状態要素を変更できます。メディアの種類は変更できません。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開し、**[プール]**をクリックします。構成済みのメディアプールのリストが[結果エリア]に表示されます。
3. プロパティを変更するメディアプールの名前を右クリックし、**[プロパティ]**をクリックします。[一般]プロパティページが表示されます。
4. [プール名]テキストボックスのメディアプール名や[説明]テキストボックスの説明を変更できます。
5. メディアの使用法およびメディアの割り当てポリシーの設定を変更するには、**[割り当て]**タブをクリックします。ここで、フリープールの使用を選択/選択解除するか、**[フリーメディアをフリープールに移動]**オプションを有効/無効にするか、**[マガジンのサポート]**オプションを選択します。
6. **[条件]**タブをクリックすると、[メディア状態要素]ダイアログの設定を変更できます。また、メディア状態要素をデフォルトに戻すこともできます。
7. **[適用]**をクリックして設定内容を確定します。

メディアプールを削除する

メディアプールをData Protector構成から削除すると、そのメディアプールはバックアップで使用されなくなります。バックアップデバイスのデフォルトプールとして使用されているメディアプールは削除できません。その場合は、すべてのデバイスに適用するメディアプールを変更するか、デバイスを削除してください。

メディアが含まれているメディアプールを削除しようとすると、プール内のすべてのメディアをエクスポートまたは移動するように促すメッセージが表示されます。

> **重要：**
> バックアップ仕様で使用されているメディアプールを削除すると、バックアップ仕様からメディアプールが削除されます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開し、**[プール]**をクリックします。構成済みメディアプールのリストが[結果エリア]に表示されます。
3. 削除するメディアプールを右クリックし、**[削除]**をクリックします。確認メッセージが表示されたら、操作を続行してよいことを確認してください。

このメディアプールは、構成済みメディアプールのリストに表示されなくなります。

メディアのライフサイクル

メディアのライフサイクルは、メディアが使用された時点で開始し、最大使用基準に達した時点で終了します。このライフサイクル中には、主に以下のような作業が行われます。

メディアをバックアップ用に準備する

これには、メディアをフォーマットまたは初期化し、それらのメディアをメディアプールへ割り当てる処理が含まれます(未使用のメディアと使用済みの非Data Protectorメディアの場合はフォーマット、使用済みのData Protectorメディアの場合はインポート)。使用済みメディアを扱う場合には、リサイクルや非保護およびエクスポート機能の使用を検討してください。

メディアのバックアップ用の使用

この作業では、バックアップ用メディアの選択方法、チェックするメディアの状態要素(上書きの回数など)、メディアに新しいバックアップを追加する方法、データ保護の期限などを決定します。

メディアを安全な場所に保管する

メディアのボールティングでは、メディアを安全に保管できるように準備した後、実際に保管します。ポリシーを適切に設定する必要があります。このとき、収納場所のリストの作成カタログ保護ポリシーを適切に設定する必要があります。メディアの収納場所の指定および変更、メディアの取り出しなどの作業を行います。デバイスのスキャンが必要になることもあります。

Data Protectorでは、以下のように、さまざまなレベルでボールティングをサポートしています。

- データ保護ポリシーおよびカタログ保護ポリシー。
- ライブラリからメディアを簡単に選択して取り出すことができます。
- メディア収納場所により、メディアの物理的な保管場所を識別できます。
- 指定した時間枠内のバックアップに使用されたメディアを示すレポートを作成できます。
- 指定したメディアをバックアップ中に使用したバックアップ仕様に関するレポートを作成できます。
- 特定の収納場所に保管されているメディアのうち、指定した日時にデータ保護の期限が切れるメディアを示すレポートを作成できます。
- 復元に必要なメディアをメディアの物理的な保管場所と共に示すリストを表示できます。
- メディアへの書き込み日時や保護期限が切れたメディアなどの条件を指定して、その条件を満たすメディアをメディアビューから抽出することができます。

バックアップデータのコピーをボールティング用に作成し、オリジナルのメディアは復元用としてオンサイトに残しておくことをお勧めします。Data Protectorでは、メディア上のデータの追加コピーを対話的または自動的に作成できます。

メディアの廃棄

最大使用基準を超過し、期限切れになったメディアは、不良のマークを付加され、今後のData Protectorセッションに使用されなくなります。

メディアの種類

メディアの種類とは、DDSやDLTなどメディアの物理的な種別を意味します。デバイスの構成時には、適切なメディアの種類を選択する必要があります。これにより、該当するメディアプールに含まれているメディア上の空き領域が自動的に見積もられます。

サポートされているメディアの種類

サポートされるメディアの種類の詳細は、https://softwaresupport.hpe.com/にある最新のサポート一覧を参照してください。

メディアの品質

メディアの品質は、メディアへのデータの書き込み能力や、メディアからのデータの読み取り能力に影響するため、バックアップ用のメディアの選択方法を左右します。[良好]状態のメディアは、[普通]状態のメディアに優先して選択されます。[不良]状態のメディアは、選択対象から除外されます。

メディアの状態は、以下のメディア状態要素に基づいて判定されます。

- 良好
- 普通
- 不良

メディア品質(状態)に関する情報は、メディアの[情報]プロパティページで確認できます。

メディアの状態の計算に使用するメディア状態要素は、メディアプールの[オプション]プロパティページで変更できます。メディア状態要素を変更すると、そのメディアプール内のすべてのメディアの状態が新しい要素に基づいて計算されるようになります。

メディア品質は、メディアの交換時期の判断材料として使えます。

デバイスエラーとメディア品質

バックアップ中にデバイスに障害が発生すると、このデバイスでバックアップに使用されているメディアは不良とマーキングされます。これによって、この問題が不良メディアが原因だった場合に将来のエラーの発生が防止されます。

このエラーがドライブの汚れによるものであった場合、ドライブをクリーニングし、そのメディアを検証して状態をリセットします。

メディアに不良のマーキングが付いているかどうかを確認するようにしてください。各メディアの状態に関する詳細情報は、[検証]を使用して得ることができます。メディアを単にリサイクルする方法はお勧めできません。

バックアップ用メディアの選択方法

Data Protectorのメディア管理機能では、バックアップに最も適したメディアが自動的に選択されます。基本的なメディア選択基準は、以下のとおりです。

- [不良]状態のメディアは、バックアップ対象から除外されます。
- [普通]状態のメディアは、[良好]状態のメディアを利用できない場合にのみ使用されます。
- [良好]状態のメディアが利用可能な場合は、[良好]状態のメディアが先に使用されます。
- メディアは、常に指定したプールから選択されます。保護されていないメディアがプールに含まれていない場合は、フリープールが構成されていればフリープールからメデData Protectorィアが選択されます。

さらに、メディアの選択には、以下の要因も反映されます。

メディア割り当てポリシー

メディア割り当てポリシーを使うと、バックアップ用メディアの選択方法を制御できます。任意の適切なメディアをバックアップに使用できる[緩和]ポリシーか、あらかじめ定義された順序で特定のメディアが利用できる必要がある[厳格]ポリシーを指定できます。

メディアの事前割り当て

メディアプール内のメディアをバックアップに使用する順序を指定できます。この順序を事前割り当てリストと呼びます。

メディアの状態

メディア状態も、バックアップ用メディアの選択方法に影響します。たとえば、[良好]状態のメディアは、[普通]状態のメディアより優先して使用されます。[不良]状態のメディアは、バックアップに使用されません。

[普通]のマークが付いたメディアがバックアップに使用されるのは、そのメディア上に保護されたオブジェクトが存在しない場合のみです。保護されたオブジェクトが存在する場合は、フリーメディアのマウント要求が発行されます。

メディアの使用方法

メディアの使用法は、既に使用されているメディアへのバックアップの追加方法を制御します。また、バックアップに使用するメディアの選択にも影響します。

制限事項

バックアップは、Travanデバイスで使用されているメディア上で追加することはできません。

追加可能メディアは、[良好]状態になっている必要があります。さらに、現在保護されているオブジェクトがいくつか含まれていて、かつ空き容量が残っていなければなりません。負荷調整を有効にして複数のデバイスを使用する場合、追加可能の概念はデバイス別に適用されます。つまり、各デバイスが追加可能メディアをセッションの最初のメディアとして使用します。同じメディアにデータを追加する複数のバックアップセッションの間で、バックアップ仕様が一致している必要はありません。

> **注:**
> 追加機能を使用しているときに、バックアップに複数のメディアが必要になった場合、前のセッションでバックアップしたデータは最初に使用したメディアだけに格納できます。その後は、空のメディアか保護Data Protectorされていないメディアだけが使用されます。

メディアの使用方法は、[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。

メディア上に1つのクライアント用の復元チェーンを作成できます。これらのメディアには、同じクライアントに関連する1つのフルバックアップと複数の増分バックアップのみ格納できます。

- **[増分のみ追加可能]**メディア使用状況ポリシーに基づいてクライアントごとに1つのプールを構成します。
- ひとつのバックアップ仕様で各クライアントに別々のプールをリンクするか、クライアントごとに別のバックアップ仕様を作成します。

なお、増分バックアップのみを格納するメディアが作成される場合があります。

メディアの選択に影響する要因

割り当てポリシー	フォーマットされていないメディアを先に割り当てる	Data Protector選択順序
緩和	OFF	1. 事前割り当てリスト(指定されている場合) 2. [追加可能](使用ポリシーの設定による) 3. 保護されていないData Protectorメディア 4. フォーマットされていないメディア 5. [普通]状態のメディア
緩和	ON	1. 事前割り当てリスト(指定されている場合) 2. [追加可能](使用ポリシーの設定による) 3. フォーマットされていないメディア 4. 保護されていないData Protectorメディア 5. [普通]状態のメディア
厳格	該当なし	1. 事前割り当てリスト(指定されている場合) 2. [追加可能](使用ポリシーの設定による) 3. 保護されていないData Protectorメディア 4. [普通]状態のメディア

各種メディアフォーマットの使用

Data Protectorでは、メディアへのデータ書き込みに以下の2種類のフォーマットを使用します。

- Data Protectorフォーマット(Data Protectorで直接制御しているバックアップデバイスの場合に使用)
- NDMPフォーマット(NDMPサーバーに接続されているバックアップデバイスの場合に使用)

この2種類のフォーマットは、2つの異なるData Protector Media Agentコンポーネント(General Media AgentまたはNDMP Media Agent)を使ってバックアップデバイスと通信します。

制限事項

- 各フォーマットを使用しているバックアップデバイスでは、異なるフォーマットでデータが書き込まれているメディアをブランクメディアまたは外部メディアとして認識します。
- 同じメディアに対して、異なるフォーマットでオブジェクトをバックアップすることはできません。
- 同じシステムに複数の種類のData Protector Media Agentコンポーネントをインストールすることはできません。
- メディアフォーマットごとに異なるメディアプールを使用することを強くお勧めします。

WORMメディア

WORM(Write Once, Read Many)は、情報を1回書き込んでドライブからデータが消去されないようにするデータストレージテクノロジです。WORMメディアは、誤って消去したくないデータを保存するためのものであるため、設計上再度書き込むことができません。

Data ProtectorでWORMメディアを使用する方法

WORMテープの検出は、Windowsプラットフォームのみでサポートされます。その他のプラットフォームでは、Data Protectorがテープを書き換え可能でないと認識せずに、その他のテープとして扱います。WORMメディア上のデータを上書きしようとすると、次のエラーメッセージが表示されます。

```
Cannot write to device ([19] The media is write protected.)
```

```
Tape Alert [ 9]: You are trying to write to a write-protected cartridge.
```

これを防ぐには、以下の手順に従ってください。

- WORMメディアのバックアップ保護期間を[無期限]に設定します。
- WORMメディアと書き換え可能メディアを別々のメディアプールに置きます。

サポートされているWORMメディア

サポートされるWORMメディアでは、すべてのData Protectorメディアの操作がサポートされます。サポートするWORMテープドライブとメディアの最新リストについては、https://softwaresupport.hpe.com/にある最新サポート一覧を参照してください。

メディアのフォーマットについて

フォーマット(初期化)すると、そのメディアに関する情報(メディアID、説明、および収納場所(位置))がIDBに保存され、メディアに関する情報(メディアヘッダー)も保存されて、Data Protectorで使用できるようになります。メディアをフォーマットするときには、所属先のメディアプールも指定する必要があります。

埋め込みブロックのフォーマット

メディアのヘッダーサイズを拡張して圧縮できないデータ(埋め込みブロック)を埋め込むことができます。これはメディアのコピーを作成する時に有効です。埋め込みブロックはターゲットメディアにはコピーされません。このため、ターゲットメディアがソースメディアよりも先にテープの終わりに到達するのを防ぐことができます。

オブジェクトコピー機能を使ってバックアップデータをコピーする場合は、テープの埋め込みは不要です。

テープの埋め込みは、デフォルトでは無効になっています。有効化するには、バックアップデバイスが接続されているシステムの`omnirc`ファイル内で`OB2BLKPADDING_n`オプションを設定します。

メディアをフォーマットするタイミング

バックアップに使用するメディアは、事前にフォーマットしておく必要があります。ただし、メディアプールに[緩和]メディア割り当てポリシーを使用している場合は、メディアのフォーマットを別途行う必要はありません。グローバルオプション`InitOnLoosePolicy`が1に設定されていると(デフォルトでは0)、新しいメディアがバックアップData Protector用に選択されている場合には自動的にフォーマットされます。

Data Protector以外のメディアは、バックアップを行う前に事前にフォーマットしておく必要があります。

Data Protectorメディア上のデータが保護されている場合、そのメディアはフォーマットされません。保護を解除すると、古いデータが上書きされます。

メディアラベル

Data Protectorでは、フォーマットの際に各メディアに一意のメディアラベルとメディアIDが割り当てられます。いずれもIDBに格納され、それによってData Protectorはそのメディアを管理できます。メディアラベルは、メディアのユーザー定義の説明とバーコード(**[初期化時にメディアラベルとしてバーコードを使用]**オプションがライブラリに選択されている場合)の組み合わせです。バーコードはメディアの説明のプレフィックスとして表示されます。たとえば、[CW8279]Default DLT_1は、Default DLT_1の説明とCW8279バーコードの付いたメディアラベルです。バーコードは、メディアの初期化時にテープ上のメディアヘッダーにメディアラベルとして任意に書き込むことができます。

フォーマットしたメディアには、ラベルと収納場所情報が書き込まれます。これらの情報を変更するには、メディアをもう一度フォーマットする必要があります(この場合は、既存のデータが上書きされることになります)。メディアのプロパティを変更することによって変わるのは、メディアそのものに書き込まれた情報ではなく、IDBに保存されている情報だけです。

ラベルを変更したりバーコード番号を省いたりすることもできますが、お勧めできません。これを行う場合は、メディアに割り当てた実際のバーコードやメディアラベルを手作業で記録しておく必要があります。

認識可能なメディアの形式

Data Protectorでは、メディアがほかのアプリケーションで既に使用されている場合、メディア上の一般的なフォーマットのデータを認識できます。ただし、プラットフォームによって認識可能なフォーマットに違いがあるため、Data Protectorではフォーマットを正しく認識できない場合もあります。

Data Protectorのメディアが上書きされるのを防止するには、[厳格]割り当てポリシーを選択する必要があります。

下の表に示すように、Data Protectorの動作は、認識したメディアフォーマットによって異なります。

Data Protectorのメディアフォーマットのカテゴリ

メディアフォーマット	バックアップ動作	実行可能な操作
不明または新規(ブランク)	[緩和]ポリシー:バックアップに使用 [厳格]ポリシー:バックアップに使用せず	メディアのフォーマット
圧縮付きで書き込まれたが、現在は圧縮なしで使用されているメディア	[緩和]ポリシー:バックアップに使用 [厳格]ポリシー:バックアップに使用せず	メディアのフォーマット
圧縮なしで書き込まれたが、現在は圧縮付きで使用されているメディア	[緩和]ポリシー:バックアップに使用 [厳格]ポリシー:バックアップに使用せず	メディアのフォーマット
外部Data Protector(ほかのセル)	バックアップに使用せず	メディアのインポートまたはメディアの強制フォーマット
tar、cpio、OmniBack I、ANSIラベル	バックアップに使用せず(保証不能)	メディアの強制フォーマット
Data Protector保護解除	バックアップに使用	メディアのエクスポート
Data Protectorで保護されているメディア	バックアップの追加	メディアのリサイクル(保護解除)

> **注:**
> ハードウェア圧縮をサポートしていないデバイスでハードウェア圧縮を使って書き込みが行われたメディアからデータを読み取ろうとしても、Data Protectorではメディアを認識できず、データを読み取ることはできません。したがって、このメディアは未知または新規のメディアとして扱われます。

メディアをフォーマットする

バックアップに使用するメディアは、事前にフォーマットしておく必要があります。Data Protectorメディア上のデータが保護されている場合、そのメディアはフォーマットされません。保護を解除すると、古いデータが上書きされます。

> **注:**
> ファイルライブラリデバイスに最初のバックアップが作成されるまで、ファイルライブラリデバイスをフォーマットすることはできません。バックアップが作成されるまで、デバイスにはファイルデポがなく、ファイルデポを手動で作成することができないためです。バックアップ中に作成されるファイルデポは、メディアに相当します。ファイルライブラリデバイスのメディアプールのメディア割り当てポリシーに従って、新しくフォーマットされたメディアが自動的に削除されます。

> **重要:**
> **[強制操作]**オプションを使用して、Data Protectorで認識されるその他のフォーマット(tar、OmniBack Iなど)でメディアをフォーマットするか、Data Protectorメディアを再フォーマットします。
>
> Data Protectorメディア上のデータが保護されている場合、そのメディアは保護が削除されるまでフォーマットされません。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開し、**[プール]**をクリックします。
3. [結果エリア]でメディアの追加先のメディアプールを右クリックし、**[フォーマット]**をクリックしてウィザードを起動します。
4. ターゲットメディアが格納されているデバイスを選択し、**[次へ]**をクリックします。
5. 必要に応じて新しいメディアの**[メディアの説明]**と収納場所を指定し、**[次へ]**をクリックします。
6. セッションに適用するその他のオプションを指定します。**[操作後メディアを取り出し]**オプションを選択することも、**[強制操作]**オプションを使用することもできます。また、**[メディアサイズを指定]**を使用することも、**[デフォルト]**オプションを選択したままにすることもできます。
7. **[完了]**をクリックして、ウィザードを終了します。これによって、フォーマット処理が開始されます。

フォーマットが完了したメディアの種類は[Data Protector]に設定されます。

マガジン内のすべてのメディアをフォーマットする

バックアップに使用するメディアは、事前にフォーマットしておく必要があります。Data Protectorメディア上のデータが保護されている場合、そのメディアはフォーマットされません。保護を解除すると、古いデータが上書きされます。

前提条件

マガジン内のすべてのメディアを一度にフォーマットするには、**[マガジンのサポート]**オプションを選択してデバイスを使用します。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開し、**[プール]**をクリックします。
3. [結果エリア]で、目的のメディアプールをダブルクリックします。
4. **[マガジン]**項目を右クリックし、**[マガジンのフォーマット]**をクリックしてウィザードを起動します。
5. 目的のライブラリドライブを選択し、**[次へ]**をクリックします。
6. 必要に応じて新しいメディアの説明と収納場所を指定し、**[次へ]**をクリックします。
7. セッションに適用するその他のオプションを指定します。**[強制操作]**オプションを使用して**[メディアサイズを指定]**オプションを選択することも、**[デフォルト]**オプションを選択したままにすることもできます。
8. **[完了]**をクリックして、ウィザードを終了します。これによって、フォーマット処理が開始されます。

フォーマットが完了したメディアの種類は[Data Protector]に設定されます。

マガジン内の単一のメディアをフォーマットする

バックアップに使用するメディアは、事前にフォーマットしておく必要があります。Data Protectorメディア上のデータが保護されている場合、そのメディアはフォーマットされません。保護を解除すると、古いデータが上書きされます。

前提条件

マガジン内のメディアをフォーマットするには、**[マガジンのサポート]**オプションを選択してデバイスを使用します。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開し、**[プール]**をクリックします。
3. [結果エリア]でメディアの追加先のメディアプールを右クリックし、**[フォーマット]**をクリックしてウィザードを起動します。
4. ターゲットメディアが格納されているデバイスを選択し、操作対象のメディアに対応するスロットを選択して、**[次へ]**をクリックします。
5. 必要に応じて新しいメディアの説明と収納場所を指定し、**[次へ]**をクリックします。
6. セッションに適用するその他のオプションを指定します。**[強制操作]**オプションを使用して**[メディアサイズを指定]**オプションを選択することも、**[デフォルト]**オプションを選択したままにすることもできます。
7. **[完了]**をクリックして、ウィザードを終了します。これによって、フォーマット処理が開始されます。

フォーマットが完了したメディアの種類は[Data Protector]に設定されます。

ライブラリデバイス内のメディアをフォーマットする

バックアップに使用するメディアは、事前にフォーマットしておく必要があります。Data Protectorメディア上のデータが保護されている場合、そのメディアはフォーマットされません。保護を解除すると、古いデータが上書きされます。

ライブラリデバイスを使用する場合は、[Ctrl]キーを使って複数のスロットを選択し、複数のメディアを一括でフォーマットできます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで[デバイス]を展開します。次に、ライブラリデバイスを展開し、**[スロット]**をクリックします。
3. [結果エリア]で目的のメディアの名前を右クリックし、**[フォーマット]**をクリックしてウィザードを起動します。
4. 目的のライブラリドライブを選択し、**[次へ]**をクリックします。
5. フォーマットしたメディアを追加するメディアプールを選択し、**[次へ]**をクリックします。
6. 必要に応じて新しいメディアの**[メディアの説明]**と収納場所を指定し、**[次へ]**をクリックします。

7. セッションに適用するその他のオプションを指定します。**[強制操作]**オプションを使用して**[メディアサイズを指定]**オプションを選択することも、**[デフォルト]**オプションを選択したままにすることもできます。
8. **[完了]**をクリックして、ウィザードを終了します。これによって、フォーマット処理が開始されます。

フォーマットが完了したメディアの種類は[Data Protector]に設定されます。

メディアのインポートについて

メディアのインポートとは、セルとは異質のData Protectorメディアをメディア上のデータを失うことなくメディアプールに追加することです。インポート対象となるのは、事前にエクスポートされたメディアか、他のData Protectorセルでデータを書き込まれたメディアです。

メディアのインポート時には、そのメディアにバックアップしたデータに関する情報がIDBに読み込まれます。後で復元を行う時には、データベースに読み込まれた情報を検索できます。

留意事項

- メディアのインポート中には、オブジェクトサイズやメディアサイズなどの属性情報が再構築されないので、インポートしたオブジェクトのサイズは0 kBと示されます。
- バックアップデバイスとメディアの種類によっては、インポート処理にかなり時間がかかることがあります。
- メディアは、フリープールにインポートできません。
- 削除したコピーをインポートしようとしたときにオリジナルメディアがIDBにない場合には、[強制操作]オプションを使用してオリジナルのメディアを最初にインポートするか、[コピーをオリジナルとしてインポート]オプションを使用してコピーをインポートしてください。
- データ保護が既に期限切れしたWORMメディアをData Protectorセルにインポートする場合、**[保護]**オプション(デフォルトで値は[無期限])を使用して、必ず新しいデータ保護値を指定してください。これにより、Data ProtectorでWORMメディアに追記できるようになります。

メディアをインポートするタイミング

インポート機能は、主に、複数のData Protectorセル間でメディアを移動する場合に使います。この場合、メディア上のスペースに関する情報は更新されません。

1つのバックアップセッションで使用されたメディアをすべて同時にインポートするようにしてください。バックアップセッションで使用したメディアをすべてインポートしなかった場合、他のメディアにまたがっているデータを復元できなくなります。

ファイルライブラリデバイスの場合、ファイルライブラリデバイスに以前に属していたファイルデポや、以前にエクスポートされたファイルデポのインポートのみ可能です。ターゲットホスト以外のホストに存在するファイルライブラリからメディアをインポートする場合、ジュークボックスデバイスへのインポートのみが可能です。

メディアをインポートする

Data Protectorで既に使用されているメディアをメディアプールに追加する場合、メディアをインポートすると、後で復元対象のデータを検索できます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**をクリックします。
3. [結果エリア]で、メディアのインポート先のデバイスを右クリックし、**[インポート]**をクリックしてウィザードを起動します。
4. インポートしたメディアの追加先となるメディアプールを選択し、**[次へ]**をクリックします。
5. **[コピーをオリジナルとしてインポート]**オプションを選択します。必要に応じて、**[ロギング]**オプションも選択できます。
6. **[完了]**をクリックして、ウィザードを終了します。これによって、インポート処理が開始されます。

[セッション情報]メッセージにインポート処理の進行状況が表示されます。インポートが完了したメディアの種類は[Data Protector]に設定されます。

マガジン内のすべてのメディアをインポートする

Data Protectorで既に使用されているメディアをメディアプールに追加する場合、メディアをインポートすると、後で復元対象のデータを検索できます。

前提条件

マガジン内のすべてのメディアを一度にインポートするには、**[マガジンのサポート]**オプションを選択してデバイスを使用します。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開し、**[プール]**をクリックします。
3. [結果エリア]で、マガジン内のメディアの所属先のメディアプールをダブルクリックします。[メディア]項目と[マガジン]項目が表示されます。
4. **[マガジン]**項目を右クリックし、**[マガジンのインポート]**をクリックしてウィザードを起動します。
5. 目的のライブラリドライブを選択し、**[次へ]**をクリックします。
6. 必要に応じて新しいメディアの説明を入力するか、**[自動生成]**オプションを設定したままにして**[次へ]**をクリックします。
7. **[コピーをオリジナルとしてインポート]**オプションを選択します。必要に応じて、**[ロギング]**オプションも選択できます。
8. **[完了]**をクリックして、ウィザードを終了します。これによって、インポート処理が開始されます。

[セッション情報]メッセージにインポート処理の進行状況が表示されます。インポートが完了したメディアの種類は[Data Protector]に設定されます。

マガジン内の単一のメディアをインポートする

メディアをメディアプールにインポートする場合、Data Protectorで使用されているメディアをインポートします。後で復元対象のデータを検索できます。

前提条件

マガジン内のメディアをインポートするには、**[マガジンのサポート]**オプションを選択してデバイスを使用します。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開し、**[プール]**をクリックします。
3. [結果エリア]で、マガジン内のメディアの所属先のメディアプールをダブルクリックします。[メディア]項目と[マガジン]項目が表示されます。
4. **[メディア]**項目を右クリックし、**[インポート]**をクリックしてウィザードを起動します。
5. ターゲットメディアが格納されているライブラリのドライブとスロットを選択し、**[次へ]**をクリックします。
6. **[コピーをオリジナルとしてインポート]**オプションを選択します。必要に応じて、**[ロギング]**オプションも選択できます。
7. **[完了]**をクリックして、ウィザードを終了します。これによって、インポート処理が開始されます。

[セッション情報]メッセージにインポート処理の進行状況が表示されます。インポートが完了したメディアの種類は[Data Protector]に設定されます。

ライブラリデバイス内のメディアをインポートする

Data Protectorで既に使用されているメディアをメディアプールに追加する場合、メディアをインポートすると、後で復元対象のデータを検索できます。

ライブラリデバイスを使用する場合は、[Ctrl]キーを使って複数のスロットを選択し、複数のメディアを一括でフォーマットできます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[デバイス]**を展開します。次に、ライブラリデバイスを展開し、**[スロット]**をクリックします。
3. [結果エリア]で、インポートするメディアが格納されているスロットを選択します。
4. 選択したスロットを右クリックし、**[インポート]**をクリックしてウィザードを起動します。
5. インポートするメディアがエクスチェンジャーによってロードされるライブラリドライブを選択し、**[次へ]**をクリックします。
6. インポートしたメディアの追加先となるメディアプールを選択し、**[次へ]**をクリックします。
7. **[コピーをオリジナルとしてインポート]**オプションを選択します。必要に応じて、**[ロギング]**オプションも選択できます。
8. **[完了]**をクリックして、ウィザードを終了します。これによって、インポート処理が開始されます。

[セッション情報]メッセージにインポート処理の進行状況が表示されます。インポートが完了したメディアの種類は[Data Protector]に設定されます。

暗号化されたバックアップを含むメディアのエクスポートとインポート

暗号化されたバックアップから別のData Protectorセルのクライアントにデータを復元するには、以下のセクションで説明するように、メディアと暗号化キーをあて先のCell Managerにインポートする必要があります。

> **注：**
> Data Protectorには、コマンドラインインターフェイス(CLI)を使用する暗号化キーの高度な手動の管理機能があります(キーの有効期限、再アクティベーション、エクスポート、インポート、削除など)。詳細については、`omnikeytool`のmanページまたは『*HPE Data Protector Command Line Interface Reference*』を参照してください。

CMMDBを含まないCell Manager環境またはMoM環境

Cell Manager環境またはローカルのMMDBを使用するMoM環境で以下の手順を実行し、暗号化されたバックアップを含むメディアをエクスポートおよびインポートします。

手順

1. 元のCell Managerで、IDBからメディアをエクスポートします。この操作では、キーストアから、暗号化キーがエクスポートされるデフォルトディレクトリの*mediumID*.csvファイルに関連暗号化キーもエクスポートします。
2. *mediumID*.csvファイルをエクスポート先のCell Managerに転送し、暗号化キーがインポートされるデフォルトディレクトリに配置します。
3. エクスポートしたメディアをあて先のCell Managerが使用するドライブに挿入します。
4. あて先のCell Managerで、メディアをインポートします。この操作によって、*mediumID*.csvファイルからキーもインポートされます。

> **注：**
> キーファイルがない場合にもメディアのインポートはできますが、復号化キーがないので、カタログインポートは中止されます。

CMMDBを含むMoM環境

CMMDBが使用されているMoM環境では、すべてのメディア情報がMoM Managerに保存されますが、メディアで使用される暗号化キーIDとCDBは、それぞれのCell Managerのローカルキーストアに保存されます。メディア管理のすべての操作は、MoM Cell Managerで実行する必要があることに注意してください。

CMMDBがMoM Managerにある場合に暗号化されたバックアップを含むメディアをエクスポートおよびインポートするには、以下の手順を実行します。

手順

1. CMMDBからメディアをエクスポートします。キーIDは、暗号化キーがエクスポートされるデフォルトディレクトリの*mediumID*.csvファイルにエクスポートされます。
2. *mediumID*.csvファイルをエクスポート先のCell Managerに転送し、暗号化キーがインポートされるデ

フォルトディレクトリに配置します。

3. MoM Managerで、ライブラリからメディアを取り出します。
4. メディアを元のメディアプールからあて先セルのドライブに関連付けられているメディアプールに移動します。この操作によって、カタログもインポートされます。
5. エクスポートしたメディアをあて先のCell Managerが使用するドライブに挿入します。
6. あて先のCell Managerで、メディアをインポートします。この操作によって、*mediumID*.csvファイルからキーもインポートされます。

メディアのコピーについて

Data Protectorにはバックアップの終了後にメディアをコピーするための機能が用意されています。メディアのコピーとは、バックアップが格納されているメディアの完全なコピーを作成するプロセスを指します。アーカイブやボールティングを目的として、コピーやオリジナルメディアを安全な場所に移し、もう一方のメディアセットを復元用としてサイトに置いておくことができます。

前提条件

2つのデバイス(1つはソースメディア用でもう1つはターゲットメディア用が必要です。複数のドライブがあるライブラリデバイス内のメディアをコピーすることもできます。その場合は、同じデバイス内の2つのドライブをそれぞれソースメディアとターゲットメディアに使います。

- ソースメディアとターゲットメディアは、同じメディアの種類でなければなりません。
- ターゲットメディアがデータ保護されたData Protectorメディアである場合、最初にメディアをリサイクルしてからメディアをフォーマットします。

制限事項

- 同一メディア(ソースメディア)のコピー(ターゲットメディア)を複数作成することができますが、コピーから別のコピーを作成することはできません。
- コピーできるのは、Data Protector常駐メディア(デバイス内のメディア)のみです。
- メディアのコピーは、通常は別の場所での保管用として、メディアの正確なコピーを作成するために設計されているため、ファイルライブラリではサポートされません。ファイルライブラリ内のデータのコピーを作成するには、オブジェクトコピー機能を使用します。
- メディアコピー操作は、フリープール内のメディアには実行できません。
- NDMPサーバーにより制御されているNASデバイスでは、デバイスの同時処理数は1つに制限されます。
- メディアコピーは、NDMP-Celerraバックアップセッションではサポートされていません。

メディアをコピーするタイミング

バックアップセッションが終了すると同時に、メディアをコピーできます。ただし、メディアのコピーに使用するデバイスがあるかどうかを考慮する必要があります。特定のデバイスをメディアのコピーに使う前に、そのデバイスが使用されるバックアップがすべて完了するまで待機することをお勧めします。

どのような結果が得られるか

メディアをコピーすると、オリジナルのメディアセットと同じメディアセットがもう1セット作成されます。どちらも復元に使用できます。

ソースメディアがコピーされると、新たなバックアップが付加されることを防止するため、Data Protectorがソースメディアを追加不可能にします これは元のメディアの内容がそのコピーと異ならないようにするためです。コピーも、追加不可能となります。

コピーからの復元

デフォルトの場合、Data Protectorは、オリジナルのメディアセットからデータを復元します。ただし、オリジナルのメディアセットが利用できずコピーが利用可能であるときには、コピーを使用して復元が行われます。

オリジナルもコピーも復元時のデバイスで利用できない場合、Data Protectorはマウント要求を出し、復元に必要なメディアとしてオリジナルとコピーの両方を表示しますが、いずれでも使用することができます。

スタンドアロンデバイスを使って復元する場合には、オリジナルではなくコピーからの復元を選べます。処理手順としては、復元に使用するデバイスにコピーを挿入するか、コピーが入っているデバイスを選択します。ライブラリにオリジナルが存在しているときにライブラリデバイスを使用して復元を行う場合、オリジナルが復元に使用されます。Data Protector

> **注:**
> メディアのコピー時には、ターゲットメディアがソースメディアよりも先にテープの終わりに到達する可能性があります。ソースメディアにストリーミングモードでデータが書き込まれた後、ビジー状態のシステムや負荷の高いネットワークを使用してコピーを作成すると、テープがいったん停止してから再び送られるときに空白のスペースが生じることがあり、この問題を招きます。この問題を防止するには、メディアのフォーマット時にテープに対する文字の埋め込みを行えるようにします。

メディアをコピーする

メディアをアーカイブまたはボールティングの目的でコピーできます。メディアのコピーセッションでは複数のメディアを同時にコピーできないため、各メディアのコピーを個別に開始する必要があります。

スタンドアロン デバイスのメディアをコピーする

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を展開し、コピーするメディアが格納されているデバイスを右クリックして、**[コピー]**をクリックします。
3. ターゲットメディアが格納されているデバイス(ライブラリのドライブとスロット)を選択し、**[次へ]**をクリックします。
4. メディアコピーの追加先となるメディアプールを選択し、**[次へ]**をクリックします。
5. 必要に応じて、メディアコピーの説明と収納場所を指定し、**[次へ]**をクリックします。
6. セッションに適用するその他のオプションを指定します。**[強制操作]**オプションを選択して、メディアの

サイズとメディア保護を指定できます。

> **ヒント:**
> ターゲットメディアがData Protectorで認識する形式(tar、OmniBack Iなど)以外の形式である場合や、保護されていないData Protectorメディアの場合は、**[強制操作]**オプションを使います。

7. **[完了]**をクリックして、ウィザードを終了します。これにより、コピー処理が開始します。

[セッション情報]メッセージにメディアコピーの進行状況が表示されます。

ライブラリデバイスのメディアをコピーする

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインの**[メディア]**で、**[プール]**を展開し、コピーするメディアが格納されているメディアプールを展開します。メディアを右クリックし、**[コピー]**をクリックしてウィザードを起動します。
3. コピー対象のメディアのドライブを選択し、**[次へ]**をクリックします。ライブラリにドライブが1つしかない場合、この手順はスキップされます。
4. ターゲットメディアが格納されているデバイス(ライブラリのドライブとスロット)を選択し、**[次へ]**をクリックします。
5. メディアコピーの追加先となるメディアプールを選択し、**[次へ]**をクリックします。
6. 必要に応じて、メディアコピーの説明と収納場所を指定し、**[次へ]**をクリックします。
7. セッションに適用するその他のオプションを指定します。**[強制操作]**オプションを選択して、メディアのサイズとメディア保護を指定できます。

> **ヒント:**
> ターゲットメディアがData Protectorで認識する形式(tar、OmniBack Iなど)以外の形式である場合や、保護されていないData Protectorメディアの場合は、**[強制操作]**オプションを使います。

8. **[完了]**をクリックして、ウィザードを終了します。これにより、コピー処理が開始します。

[セッション情報]メッセージにメディアコピーの進行状況が表示されます。

メディアの自動コピー

メディアの自動コピーとは、バックアップが格納されているメディアのコピーを作成する自動操作です。メディアのコピーを手動で開始する場合と比較すると、以下のような制限があります。

制限事項

- スタンドアロンデバイスはメディアの自動コピーに使用できません。ライブラリデバイスのみ使用できます。ディスクへのバックアップ(B2D)デバイスはメディアの自動コピーには使用できません。
- 自動メディアコピーは、NDMP-Celerraバックアップセッションではサポートされていません。

メディアの自動コピー

最初に、メディアの自動コピー仕様を作成します。自動メディアコピーセッションの開始時に、Data Protectorは、自動メディアコピー仕様内で指定したパラメーターに基づいて、メディアのリスト(ソースメディア)が生成されます。各ソースメディアでは、データのコピー先となるターゲットメディアが選択されます。ターゲットメディアは、ソースメディアと同じメディアプール、フリープール、またはライブラリ内の空きメディアの中から選択されます。

各コピー元メディアについて、ユーザーが自動メディData Protectorアコピー仕様内に指定したデバイスの中から、1組のデバイスが自動的に選択されます。自動メディアコピー機能には独自の負荷調整機能が備えられています。Data Protectorはできるだけ多くのデバイスを使用し、また可能であればローカルデバイスを使用することにより、使用可能なデバイスを最大限有効に活用しようとします。

各デバイスはセッションの開始時にロックされます。セッション開始後にデバイスをロックすることはできないため、セッション開始時に利用可能な状態になっていなかったデバイスはセッションに使用できません。セッション全体を正常に終了するには、少なくともデバイスのペアを各メディアの種類に使用できる必要があります。セッションに必要な最小限の数のデバイスをロックできなければ、セッションは失敗します。

ソースメディアでは、ターゲットメディアのあて先プールが定義されます。このため、コピーしたメディアは、オリジナルのメディアと同じプールに所属することになります。

コピーのデフォルトの保護期間は、オリジナルの保護期間と同じになります。メディアの自動コピー仕様を作成または修正するときに、異なる保護期間を設定することができます。

自動メディアコピー機能は、マウント要求やクリーニング要求には対応できません。マウント要求が受信されると、該当するメディアのペアに対してはコピーが中止されますが、セッションは続行されます。コピーされなかったメディアは、メディアの自動コピーセッションの完了後に手動でコピーできます。

メディアエラーが発生すると、そのメディアの自動コピーセッション内では、エラーの発生したデバイスが回避されます。ただし、他に使用できるデバイスがない場合は、エラーの発生したデバイスが再利用されます。

メディアの自動コピーの種類

メディアの自動コピーには、ポストバックアップのメディアコピーとスケジュール設定されたメディアコピーの2種類があります。

ポストバックアップのメディアコピー

ポストバックアップのメディアコピーは、バックアップセッションの完了後に実行されます。この場合は、特定のセッション内で使用されたメディアがコピーされます。

スケジュール設定されたメディアコピー

スケジュール設定されたメディアコピーは、ユーザー定義のタイミングで実行されます。この場合は、異なるバックアップ仕様に基づいて使用されている複数のメディアを、単一セッション内でコピーすることも可能です。どのメディアをコピーするかは、自動メディアコピー仕様を作成して指定します。

ポストバックアップのメディアコピーを構成する

ポストバックアップのメディアコピーは、特定のバックアップセッションの完了後に、そのセッションで使用したメディアのコピーを作成する操作です。

> **注:**
> バックアップセッションが中止された場合でも、ポストバックアップのメディアコピーセッションは開始されます。この場合は、一部のオブジェクトだけが正常にコピーされます。

制限事項

- 使用できるデバイスは、ライブラリデバイスのみです。
- ソースメディアとターゲットメディアは、同じ種類でなければなりません。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[自動操作]**を右クリックし、**[ポストバックアップのメディア操作を追加]**をクリックしてウィザードを起動します。
3. コピーするメディアが含まれているバックアップ仕様を[バックアップ仕様]ドロップダウンリストから選択します。[メディア操作の種類]ドロップダウンリストで、**[メディアコピー]**を選択し、**[次へ]**をクリックします。
4. 使用するソースデバイスとあて先デバイスを選択します。各メディアにつき、少なくとも1組のデバイスのペア(ソースデバイスとあて先デバイス)を指定する必要があります。**[次へ]**をクリックします。
5. コピーの数、操作後にメディアを自動的に取り出すかどうか、およびターゲットメディアの収納場所および保護を指定します。**[完了]**をクリックしてウィザードを終了します。

スケジュール設定されたメディアコピーを構成する

スケジュール設定されたメディアコピーは、特定のバックアップセッションで使用したメディアのコピーをスケジュールに基づいて作成する操作です。単一のセッション内で複数のコピー操作のスケジュールを設定できます。十分な数のデバイスが利用可能であれば、メディアが同時にコピーされます。それ以外の場合は、メディアが逐次的にコピーされます。

制限事項

- 使用できるデバイスは、ライブラリデバイスのみです。
- ソースメディアとターゲットメディアは、同じ種類でなければなりません。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[自動操作]**を右クリックし、**[スケジュールされているメディア操作を追加]**をクリックしてウィザードを起動します。
3. [メディア操作名]テキストボックスに操作の名前を入力します。[メディア操作の種類]ドロップダウンリ

ストで、**[メディアコピー]**を選択し、**[次へ]**をクリックします。

4. 使用するソースデバイスとあて先デバイスを選択します。各メディアにつき、少なくとも1組のデバイスのペア(ソースデバイスとあて先デバイス)を指定する必要があります。**[次へ]**をクリックします。
5. どの時間枠内のバックアップセッションを検索するかを指定します。**[次へ]**をクリックします。
6. コピーするバックアップに対応するバックアップ仕様を指定します。**[次へ]**をクリックします。
7. ソースメディアの状態と保護を指定します。**[次へ]**をクリックします。
8. コピーの数、操作後にメディアを自動的に取り出すかどうか、およびターゲットメディアの収納場所および保護を指定します。**[完了]**をクリックしてウィザードを終了します。必要に応じて、スケジューラーを使用してメディアのコピーをスケジュールできます。

   Data Protectorでスケジュールを作成および編集する方法の詳細については、「*スケジューラー、ページ 103*」を参照してください。

   > **重要:**
   > Data Protector10.00では、基本スケジューラーとアドバンストスケジューラーは廃止され、代わりに新しいWebベーススケジューラーが導入されました。特定の日時に実行するようバックアップセッションをスケジュールすることで、無人バックアップを構成できます。Data Protectorのアップグレード中に、すべての既存のData Protectorスケジュールが新しいスケジューラーに自動的に移行されます。

デバイスをスキャンする

デバイス内のメディアに関するData Protector情報を更新するには、デバイスをスキャンします。また、メディアの収納場所を手動で変更した後にも、デバイスをスキャンする必要があります。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**をクリックします。
3. [結果エリア]で、スキャンするデバイスを右クリックし、**[スキャン]**をクリックします。

[セッション情報]メッセージにスキャン処理の進行状況が表示されます。

ライブラリデバイス内のメディアをスキャンする

ライブラリの選択済みスロット内のメディアをスキャンし、デバイス内のメディアに関するData Protector情報を更新します。

スキャン処理中には、各スロットからメディアがドライブに挿入され、メディアヘッダーが読み込まれます。Data Protectorこのため、多数のスロットを選択した場合は、スキャンに時間がかかることがあります。

Ctrlキーを使用して複数のスロットを選択し、複数のメディアを一括でスキャンすることができます。ただし、使用できるのは1つのドライブのみです。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**をクリックします。

3. [結果エリア]で、ライブラリデバイスをダブルクリックして**[スロット]**をダブルクリックします。
4. [結果エリア]で、スキャンするメディアが格納されているスロットを選択します。
5. 選択したスロットを右クリックし、**[スキャン]**をクリックしてウィザードを起動します。
6. スキャンするメディアがエクスチェンジャーによってロードされるライブラリドライブを選択します。
7. **[完了]**をクリックして、ウィザードを終了します。これによって、スキャン処理が開始されます。

[セッション情報]メッセージにスキャン処理の進行状況が表示されます。

> **ヒント:**
> [バーコードリーダーのサポート]オプションを選択している場合は、**[バーコードのスキャン]**オプションを使ってSCSIライブラリをすばやくスキャンできます。

ライブラリデバイス内のドライブをスキャンする

ライブラリデバイスのドライブをスキャンし、ドライブ内のメディアに関するData Protector情報を更新します。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**をクリックします。
3. [結果エリア]で、ドライブをスキャンするライブラリデバイスをダブルクリックし、ターゲット**ドライブ**のアイコンをダブルクリックします。
4. スキャンするドライブを右クリックし、**[スキャン]**をクリックします。

[セッション情報]メッセージにスキャン処理の進行状況が表示されます。

バーコードリーダーサポートをアクティブ化する

バーコード付きのSCSIライブラリデバイスを使用する場合、Data Protectorでバーコードを使用できます。バーコードサポートの内容は、以下のとおりです。

- クリーニングテープをCLNプレフィックスで認識します。
- メディアをバーコードで参照します。Data Protectorメディアのバーコードは、メディアの説明の先頭に表示されます。
- メディアバーコードを使用して、ライブラリレポジトリのスロット内にあるメディアをすばやくスキャンします。

> **ヒント:**
> ライブラリプロパティで**[初期化時にメディアラベルとしてバーコードを使用]**オプションを選択すると、メディアの初期化中に**[バーコードを使用]**オプションが**[メディアの説明]**オプション内でデフォルトで有効になります。このオプションをオンにしなかった場合、デフォルトのオプションは[自動生成]です。このデフォルトのオプションは、Data Protectorでメディアが自動的にフォーマットされる場合に使用されます。

> **注:**
> セル内のバーコードはすべて、メディアのタイプや、複数のライブラリが存在するといったこととは関係なく、それぞれ一意でなければなりません。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、[デバイス]を展開し、ターゲットライブラリデバイスを右クリックして、**[プロパティ]**をクリックします。ライブラリデバイスの[プロパティ]ページが表示されます。
3. **[コントロール]**タブをクリックし、**[バーコードリーダーのサポート]**オプションを選択します。
4. このライブラリを使用してメディアを初期化するたびにテープのメディアヘッダーにバーコードを書き込む場合は、**[初期化時にメディアラベルとしてバーコードを使用]**オプションをオンにします。
5. **[適用]**をクリックして設定内容を確定します。

ライブラリデバイスをバーコードスキャンする

[バーコードのスキャン]オプションを使うと、SCSIライブラリをすばやくスキャンできます。バーコード機能なしでレポジトリをスキャンする場合よりも、かなり高速でスキャンできます。

前提条件

[バーコードリーダーのサポート]オプションを有効にしておく必要があります。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、[デバイス]を展開し、ターゲットライブラリデバイスを右クリックして、**[バーコードのスキャン]**をクリックします。

[セッション情報]メッセージにバーコードスキャン処理の進行状況が表示されます。

メディアを検索/選択する

メディアプールまたはライブラリデバイス内のメディアを検索および選択できます。[メディアのリスト]レポートを使ってメディアを絞り込むこともできます。この機能を使うと、メディアのリスト全体をブラウズしなくても、特定のメディアを検索して選択することができます。

メディアの選択操作は、先週書き込まれたすべてのメディアを保管場所に移動するなどのボールティングを行う場合に非常に便利です。

メディアプール内のメディアを検索/選択する

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開し、**[プール]**をクリックします。
3. [結果エリア]でメディアプールを右クリックし、**[メディアの選択]**をクリックします。[メディアの選択]ダイアログボックスが表示されます。

4. メディアの説明、収納場所、セッション、時間枠、保護の有無などに基づいてメディアを検索および選択できます。また、[選択の結合]オプションを使用することもできます。

ライブラリデバイス内のメディアを検索/選択する

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**をクリックします。
3. [結果エリア]で、ライブラリデバイスをダブルクリックします。**[スロット]**を右クリックして**[メディアの選択]**をクリックします。[メディアの選択]ダイアログボックスが表示されます。
4. メディアの説明、収納場所、セッション、時間枠、保護の有無などに基づいてメディアを検索および選択できます。また、[選択の結合]オプションを使用することもできます。

[メディアのリスト]レポートを使ってメディアを検索する

手順

1. コンテキストリストで**[レポート]**をクリックし、**[タスク]**タブをクリックします。
2. Scopingペインで**[プールとメディア]**を右クリックし、**[メディアのリスト]**をクリックしてウィザードを起動します。
3. ウィザードの指示に従って、検索条件を指定します。**[完了]**をクリックして検索結果を表示します。

バックアップ用メディアの事前割り当てリスト

メディアプール内のメディアをバックアップに使用する順序を指定できます。この順序を事前割り当てリストと呼びます。事前割り当てリストは、バックアップの構成時に定義できます。事前割り当てリストは、バックアップセッションに使用するメディアを制御するためのものです。各バックアップの実行前に、利用可能なメディアと事前割り当てリストを照合する必要があります。

オブジェクトコピー機能やオブジェクト集約機能の使用時には、メディアの事前割り当てを行うこともできます。

メディアプールの割り当てポリシーに応じて、以下のいずれかの処理が行われます。Data Protector

- 事前割り当てリストを**[厳格]**メディア割り当てポリシーと組み合わせて使用すると、バックアップデバイス内のメディアがその順序で使用できるものとみなされます。Data Protector メディアが使用できなければ、マウント要求が発行されます。Data Protector 事前割り当てリストに指定されているメディアをSCSI-IIエクスチェンジャーにロードすると、そのメディアが正しい順序で処理されます。Data Protector
- 事前割り当てリストを**[緩和]**メディア割り当てポリシーと組み合わせて使用すると、バックアップデバイス内のメディアがその順序で使用できるものとみなされます。メディアが利用可能でなければ、ライブラリ内の任意の適切なメディアが使用されます。

バックアップ用のメディアを事前に割り当てる

以下に追加情報を示します。

- オブジェクトコピー機能やオブジェクト集約機能の使用時には、メディアの事前割り当てを行うこともできます。
- ファイルライブラリメディアプールには、デフォルトで追加不可能のメディアの使用ポリシーがあります。このポリシーによってファイルライブラリのメリットを得られるため、このポリシーを変更してファイルライブラリデバイスメディアの事前割り当てリストを使用することはお勧めできません。

保存済みバックアップ仕様内でメディアを事前に割り当てるには、以下の手順に従ってください。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様([ファイルシステム]など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 適切なバックアップ仕様をダブルクリックし、**[あて先]**タブをクリックします。
4. [あて先]ページで、バックアップ用に選択されているデバイスを右クリックして**[プロパティ]**をクリックします。
5. [デバイスのプロパティ]ダイアログボックスで、[メディアプール]ドロップダウンリストから目的のメディアを選択します。
6. [事前割り当てリスト]の**[追加]**をクリックします。

   選択したメディアプールに含まれているメディアのリストが表示されます。
7. メディアを選択し、**[追加]**をクリックします。
8. すべての必要なメディアに対して手順6と7を繰り返します。操作が完了したら、**[OK]**をクリックして[あて先]プロパティページに戻ります。
9. バックアップに複数のデバイスを使用する場合は、手順4～8を繰り返します。
10. **[適用]**をクリックして変更内容を適用します。

メディアをリサイクルする

メディア上にバックアップされたすべてのデータの保護を解除し、以降のバックアップセッション中にメディアを上書きできるようにするには、メディアをリサイクル(保護解除)します。Data Protector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。そのデータの保護が解除されたことをData Protectorに認識させるだけです。

> **重要:**
> 以下の点に注意してください。
>
> - メディアをリサイクルすると、メディア上のすべてのオブジェクトの保護が解除されます。同じセッション中に同じオブジェクトが別のメディアにまたがって書き込まれた場合は、それらのデータもリサイクル対象となります。
> - リサイクル操作は、フリープール内のメディアには実行できません。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開し、**[プール]**をクリックします。構成済みのメディアプールのリストが

[結果エリア]に表示されます。

3. リサイクルするメディアが含まれているメディアプールをダブルクリックします。
4. ターゲットメディア名を右クリックし、**[リサイクル]**をクリックします。複数のメディアを同時に選択するには、[Ctrl]キーまたは[Shift]キーを使います。

処理が完了したメディアの[保護]は[なし]に設定されます。

メディアからカタログをインポートする

メディアからカタログをインポートすると、ファイル名やファイルバージョンなどの詳細情報がIDBに書き込まれ、復元対象のファイルとディレクトリを検索できるようになります。

特定のオブジェクトに対し、[カタログ保護]の期限が切れて、そのファイルやディレクトリをブラウズできなくなった場合にも、[カタログのインポート]を使用できます。指定したメディアの詳細情報が既にIDBに記録されている場合は、データが重複しないようになっています。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開し、**[プール]**をクリックします。
3. [結果エリア]で、カタログのインポート元となるメディアが含まれているメディアプールをダブルクリックします。
4. メディアを右クリックし、**[カタログのインポート]**をクリックします。
5. 他のドライブがある場合は、メディアのインポート先となるライブラリドライブを選択し、**[次へ]**をクリックします。
6. ユーザーの要件に合う**[ロギング]**オプションを選択します。
7. **[完了]**をクリックして、ウィザードを終了します。これによって、インポート処理が開始されます。

[セッション情報]メッセージにインポート処理の進行状況が表示されます。インポートが完了したら、復元するファイルおよびディレクトリを検索できます。

メディアを検証する

メディアの検証は、メディア上のデータフォーマットが有効かどうかをチェックして、IDB内のメディアに関する情報を更新します。検証できるのは、常駐Data Protectorメディアのみです。ただし、バックアップデバイスとメディアの種類によっては、検証処理にかなり時間がかかることがあります。

メディアコピーは、ボールティングする前に検証できます。バックアップ中にエラーが報告された場合には、メディアの検証が行われ、そのバックアップの使用の可否が確認されます。

Data Protectorは、以下の処理を通じてメディアを検証します。

- メディアに関する情報(メディアの識別情報、説明、および収納場所)を含むData Protectorヘッダーをチェックします。
- メディア上のすべてのブロックを読み取り、ブロックの形式を検証します。
- バックアップ中に**[CRCチェック]**オプションが使用された場合、CRCが再計算され、メディアに格納されているCRCと比較されます。この場合、バックアップデータ自体は各ブロック内で整合性がとれています。このレベルのチェックは高い信頼性があります。

CRCチェックオプションが使用されず、検証操作が行われなかった場合、メディア上のすべてのデータは読み取られたことになります。メディアには読み取りエラーはなく、テープのハードウェア状態は最小限の受け入れ可能レベルです。このレベルのチェックは、部分的とみなされます。

スタンドアロンデバイスのメディアを検証する

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を展開し、検証対象のメディアが格納されているデバイスを右クリックして、**[検証]**をクリックします。
3. [結果エリア]で**[操作後メディアを取り出し]**オプションを選択できます。**[完了]**をクリックしてメディアを検証します。

   スタンドアロンファイルデバイスの場合、この処理手順はスキップされます。

検証の状況がセッション情報メッセージとして表示されます。

ライブラリデバイスのメディアを検証する

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインの**[デバイス]**でライブラリデバイスを展開し、**[スロット]**を展開します。検証するメディアが格納されているスロットを右クリックし、**[検証]**をクリックします。
3. [結果エリア]で、検証を実行するライブラリドライブを選択して**[完了]**をクリックします。

検証の状況がセッション情報メッセージとして表示されます。

メディアを移動する

バックアップを再編成したり、各プールの目的を変更したりする場合、あるメディアプールから同じタイプの別のメディアプールにメディアを移動することができます。これは、別のメディアプールのデフォルトであるデバイス内のメディアを使用するときにも便利です。

> **注:**
> メディアをフリーメディアプールには移動できません。フリープールを使用している場合、メディアは2種類の方法で移動されます(選択されているフリープールオプションによってどちらの方法がとられるかが決まります)。
>
> - メディアがバックアップ用に選択され(割り当てられ)ている場合、メディアはフリープールから通常のプールに移動されます。
> - メディアの保護期限が満了している場合、メディアは通常のプールからフリープールに移動されます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開し、**[プール]**をクリックします。
3. [結果エリア]で、移動するメディアが含まれているメディアプールをダブルクリックします。各プール内のメディアのリストが表示されます。
4. 移動するメディアを右クリックしてから、**[プールへ移動]**をクリックして、ウィザードを起動します。複数のメディアを同時に選択するには、[Ctrl]キーまたは[Shift]キーを使います。
5. メディアの移動先となるメディアプールを選択します。
6. **[完了]**をクリックして、ウィザードを終了します。これによって、メディアが移動されます。

> **ヒント:**
> メディアを他のセルに移動するには、そのメディアを移動元のセルからエクスポートした後、移動先のセルにインポートします。

メディアをエクスポートする

メディアを他のData Protectorセルに移動するには、メディアをエクスポートします。エクスポートを行うと、メディアに関する情報とその内容がIDBから削除されます。Data Protectorは、エクスポートしたメディアの存在を認識しなくなります。メディア自体に格納されているデータは変更されません。

> **注:**
> すべてのメディアの手動によるエクスポートは大きな影響があるので、日時の保守でストレージがクリーンアップされるディスクへのバックアップデバイス(B2D)上でメディアを手動でエクスポートしないことをお勧めします。日次の保守でストレージがクリーンアップされるようにしてください。

オリジナルのメディアをエクスポートしてまだコピーがある場合、コピーのいずれかがオリジナルになります。

> **重要:**
> メディアをエクスポートする前に、メディアをリサイクルして保護を解除する必要があります。
>
> 同じバックアップセッションのメディアは、すべて同時にエクスポートしてください。セッションでバックアップしたデータが複数のメディアにまたがっている場合に1つのメディアだけをエクスポートすると、データを復元できなくなることがあります。Data Protector他のメディアにもデータが存在していることがわかっていても、一部のメディアが利用できない状態になるためです。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開し、**[プール]**をクリックします。
3. [結果エリア]で、エクスポート対象のメディアが含まれているメディアプールをダブルクリックします。メディアを右クリックし、**[エクスポート]**をクリックしてウィザードを起動します。
4. 確認メッセージが表示されたら、操作を続行してよいことを確認してください。

このエクスポートしたプールは、プール内のメディアのリストに表示されなくなります。

MCFファイルにカタログメディアデータをコピーする

メディア関連カタログデータをファイルにコピーすると、ファイル名およびファイルバージョンなどの詳細情報がCell Managerのディレクトリ*Data_Protector_program_data*`\Config\Server\export\mcf`(Windowsシステムの場合)、または`/var/opt/omni/server/export/mcf`(UNIXシステムの場合)に存在するメディアコンテナーフォーマット(MCF)ファイルに書き込まれます。これらのファイルを別のData Protector Cell Managerにインポートすると、メディア関連カタログデータが参照に利用可能になります。

制限事項

- 選択できるのは、Data Protectorメディアのみです。
- メディアをライブラリからエクスポートして別のライブラリにインポートすることができないというData Protectorのファイルライブラリの性質上、そのようなメディアに対して**[カタログをファイルにコピー]**および**[カタログをファイルからインポート]**は行わないでください。

推奨事項

- 1メディア当たりのカタログデータが大量になる場合があるので、別個のパーティションまたはマウントポイント上にファイルを保存することを推奨します。
- ファイルのサイズは、`EnableMCFCompression`グローバルオプションを`1`に設定することによって縮小できます。圧縮は、デフォルトでは無効になっています。

以下に追加情報を示します。

- メディア関連カタログデータは、オリジナルのCell Managerから削除されません。
- この操作によって、メディアごとにMCFファイルが作成されます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開してから、**[プール]**を展開します。
3. カタログをコピー対象にするメディアのメディアプールを展開します。
4. メディアを右クリックして、**[カタログをファイルにコピー]**をクリックします。
5. MCFファイルの出力ディレクトリを指定します。MCFファイルにメディア関連カタログデータが含まれます。
6. **[完了]**をクリックして、ウィザードを終了します。これにより、コピー処理が開始します。

エクスポートされたMCFファイルをあて先Cell Managerに転送できます。

> **ヒント:**
> 同じ結果を実現するには、**[デバイス]**を展開して、選択したデバイスのスロットを右クリックしてから、手順5および6を実行します。

MCFファイルからカタログメディアデータをインポートする

オリジナルCell Managerのメディアコンテナーフォーマット(MCF)ファイルからメディア関連カタログデータコピーをインポートすると、あて先Cell Manager上のファイルを参照できます。

前提条件

- インポート対象のMCFファイルがオリジナルのCell Managerから転送され、現在のCell Manager上でアクセスできることを確認します。

制限事項

- メディアがファイルからインポートされた後、メディアの物理的な存在を必要とする操作(復元、メディアコピーなど)によってメディアを使用することはできません。メディアをData Protector操作で完全に使用できるようにするためには、Data Protectorメディアスキャンの使用によってメディアが物理的にアクセスおよびスキャン可能である必要があります。それ以外の場合、マウント要求が発行されます。

以下に追加情報を示します。

- 多数のメディアカタログをMCFファイルからインポートする場合、復元チェーンの一部であるすべてのメディアを必ずインポートしてください。
- さまざまなメディアプールの複数の種類を1セッション内でインポートすることができます。
- Data Protector GUIでは、mcf拡張子のファイルのみを表示および選択できます。その他のファイルはディレクトリツリーでは非表示です。ただし、それらはコマンドラインインターフェイス(CLI)によって選択できます。詳細については、`omnimm`のmanページまたは『*HPE Data Protector Command Line Interface Reference*』を参照してください。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開して**[プール]**を右クリックし、**[カタログをMCFファイルからインポート]**をクリックして、ウィザードを起動します。
3. インポート対象のMCFファイルを指定します。
4. セッションに適用するその他のオプションを指定します。デフォルトで、**[可能ならば元のプールにインポート]**オプションが選択されます。[新規プールのプレフィックス]を選択するか、**[コピーをオリジナルとしてインポート]**オプションを選択できます。
5. **[完了]**をクリックして、ウィザードを終了します。これによって、インポート処理が開始されます。

メディアの説明を変更する

メディアの説明は、メディアの目的などを示すテキストです。説明は、メディアに書き込まれ、IDBに保存されます。新しいメディアをフォーマットするときはメディアの説明を追加します。バックアップ中にメディアを自動フォーマットした場合は、説明テキストが自動的に生成されますが、このテキストは必要に応じて変更できます。

ここでは、IDBに保存されているメディアの説明情報だけが更新されます。メデData Protectorィアに書き込まれている説明情報は更新されません。メディアをいったんエクスポートしてからインポートすると、IDB内の説明情報はメディアに書き込まれている説明情報に置き換えられます。

メディアラベルの説明部も変更されますが、バーコード部は元のまま変わりません。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開し、**[プール]**をクリックします。
3. [結果エリア]で、説明を変更するメディアが含まれているメディアプールをダブルクリックします。メディアプール内のメディアのリストが表示されます。
4. 説明を変更するメディアを右クリックし、**[プロパティ]**をクリックしてメディアの[一般]プロパティページを表示します。
5. [説明]テキストボックスにメディアの新しい説明を入力します。
6. **[適用]**をクリックして設定内容を確定します。

メディアの収納場所情報を変更する

メディアの収納場所情報は、デバイスから取り出したメディアを探すときに役立ちます。この情報は、メディアを初期化するときに入力します。このとき、場所情報がDB内に保存されます。この情報は、メディアを別の場所(収納棚など)に移動するたびに更新する必要があります。たとえば、"Shelf 4-Box 3"のような収納場所の名前を入力してください。

収納場所情報がメディアヘッダーに書き込まれることはありません。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開し、**[プール]**をクリックします。
3. [結果エリア]で、変更するメディアが含まれているメディアプールをダブルクリックします。メディアプール内のメディアのリストが表示されます。
4. 収納場所情報を変更するメディアを右クリックし、**[位置の変更]**をクリックしてウィザードを起動します。
5. 必要に応じて、メディアの新しい収納場所を指定します。
6. **[完了]**をクリックしてウィザードを終了します。

収納場所のリストを作成する

頻繁に使用する収納場所のリストを事前に定義しておくことができます。メディアのフォーマットなどの管理作業で対象となるメディアの収納場所を指定するときは、このリストから収納場所を選択できます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. [編集]メニューで、**[位置]**をクリックします。

3. 追加する収納場所を入力し、**[追加]**ボタンをクリックします。複数の収納場所を入力する場合は、この処理手順を繰り返します。
4. **[完了]**をクリックします。

メディアの位置の優先順位を設定する

復元、コピー、または集約の対象とするオブジェクトのバージョンが複数のメディアセットに存在する場合、いずれのメディアセットもその操作に使用できます。デフォルトでは、Data Protectorは自動的に最も適切なメディアセットを選択します。メディアの位置の優先順位を指定すると、メディアセットの選択を制御できます。

メディアの位置の優先順位を設定すると、メディアセットの選択アルゴリズムの条件に1複数のメディアセットが一致した場合に、最も優先順位が高いメディアセットが使用されます(優先順位Noneが最も高く、優先順位Data Protectorが最も低い)。

メディア位置の優先順位は、復元、オブジェクトコピー、オブジェクト集約、またはオブジェクト検証のセッションレベルで上書きできます。

以下に追加情報を示します。

- デフォルトの場合、メディアの位置の優先順位が考慮されるのは、複数のメディアセットの等級が同じであるときだけです。ほかのどの選択要素よりもメディアの位置の優先順位を優先させるには、グローバルオプションUserSpecifiedMediaPriorityHasHigherImportanceを1に設定します。
- メディアの位置の優先順位を適用するには、各メディアの位置を指定する必要があります。メディアごとに指定することも、複数のメディアに対して指定することもできます。
- メディアの位置の優先順位では、メディアコピー機能を使って作成されるコピーは反映されません。このようなコピーは、オリジナルのメディア(コピー元として使用されたメディア)が使用不可能な場合にのみ使用できます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで**[メディア]**を展開し、**[位置]**をクリックします。
3. [結果エリア]で位置をダブルクリックすると、その位置のプロパティが表示されます。
4. **[位置の優先順位]**ドロップダウンリストで、使用できる番号のどれか1つを選択します。優先順位が最も高いのは1です。
5. **[適用]**をクリックして設定内容を確定します。

メディアをボールティングする

バックアップデータのコピーをボールティング用に作成し、オリジナルのメディアは復元用としてオンサイトに残しておくことをお勧めします。Data Protectorでは、メディア上のデータの追加コピーを対話的または自動的に作成できます。

前提条件

- バックアップ仕様を構成する場合は、適切なデータ保護およびカタログ保護ポリシーが設定されていることが必要です。

- Data Protectorで保管場所を構成する必要があります。メディアが保管される物理的な場所を示す名前を使用します。

手順

1. Data Protector Managerで、メディアの保管場所を変更します。
2. メディアをデバイスから取り出し、保管場所に移動します。

メディアを消去する

メディアを消去できるのは、光磁気プラッタの場合だけです。バックアップセッションの開始前に光磁気プラッタを消去しておくと、バックアップの処理速度が向上します。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**をクリックします。
3. [結果エリア]で、メディアを消去する光磁気デバイスをダブルクリックします。
4. メディアを右クリックし、**[消去...]**をクリックしてウィザードを起動します。
5. 必要に応じて、**[操作後メディアを取り出し]**オプションを選択します。
6. **[完了]**をクリックして、ウィザードを終了します。これによって、メディアが消去されます。

[セッション情報]メッセージに消去処理の進行状況が表示されます。

書き込み保護メディアの検出

Data Protectorでは、書き込み保護スイッチをオンにすることによって物理的に保護されているメディアを検出して取り扱うことができます。

書き込み保護メディアの検出と取り扱いは、以下の操作の場合に可能です。

- リスト表示、スキャン、および検証などの読み取り専用操作。読み取り専用操作の場合は、書き込み保護メディアが検出され、警告なしで操作が続行されます。
- 初期化、消去、バックアップなどの書き込み操作。これらの操作では、書き込み保護メディアが検出された後、セッションが中止されるか、書き込み保護メディアがスキップされます。バックアップセッションでは、書き込み保護メディアを使用不可のメディアとして扱います。その後の動作はメディア割り当てポリシーに従います。割り当てポリシーが[厳格]の場合は、マウント要求が発行されます。割り当てポリシーが[緩和]の場合は、メディアがスキップされます。

書き込み保護メディアの検出とメディアの書き込み保護状態に対するすべての変更が`media.log`ファイルに書き込まれます。

> **注:**
> Data Protectorでは、書き込み保護メディアの使用を避けることをお勧めします。

マウント要求について

マウント要求時には、デバイスにメディアを挿入するように促す画面が表示されます。必要なメディアを挿入してマウント要求に応じると、セッションが継続します。

Data Protectorは、以下の場合にマウント要求を発行します。

- 指定したメディアが使用できない場合。事前割り当てリストがバックアップに使用されているか、または復元に必要なメディアが紛失している場合が該当します。
- 使用可能な適切なメディアがない場合。現在ライブラリ内にあるプールからのメディアが使用できないか、スタンドアロンデバイスのメディアが使用できないか、デバイスが空である場合が該当します。
- メールスロットが開いている場合。この場合、メールスロットを閉じる必要があります。

バックアップに最も適したメディアがData Protectorによって自動的に選択されます。バックアップ用のメディアがどのように選択されるかを知っている必要があります。

ライブラリ固有のメディア管理について

Data Protectorには、ライブラリなどの複合デバイスに特化したメディア管理機能がいくつか用意されています。これらの機能を使用して、大量のメディアを簡単に管理できます。

メディアの選択、コピー、リサイクル、移動、およびメディア位置の変更などの操作は標準的な処理手順で実行できますが、スロットの追加や削除、メディアの挿入、取り出し、検証、フォーマット、インポート、スキャン、消去などの操作は、使用するデバイスの種類に応じた処理手順で実行する必要があります。

バーコードがサポートされているライブラリの場合、初期化中にData Protectorによって、バーコードに基づいてメディアの説明を生成して、テープのヘッダーに書き込むことができます。

他のアプリケーションによるライブラリメディアの使用

ライブラリ(特に、ADIC/GRAUやStorageTekなどの大容量ライブラリ)内のメディアは、Data Protectorに限らず、さまざまなアプリケーションから使用される可能性があるため、上書きを避けるために、どのアプリケーションがどのメディアを使用するかを把握しておく必要があります。

Data Protector専用のライブラリを用意し、そのライブラリ全体をData Protectorで管理するのが理想的ですが、他のアプリケーションからも同じライブラリを使用する場合は、Data Protectorと他のアプリケーションの間で重複が生じないようにメディアのサブセットを割り当てる必要があります。Data Protectorは専用の独立したメディア割り当てポリシーを保持します。このため、特定のメディアをData Protectorに割り当てると、そのメディアはData Protectorのメディアプールに追加され、使用期限が切れるかまたはData Protectorメディアプールから削除されない限り、Data Protectorの制御下に維持されます。

> **重要:**
> Data Protectorでは、メディアの種類ごとに個別のライブラリを割り当てる必要があります。ADIC/GRAUシステムまたはStorageTekシステムでは、多数の物理的に異なる種類のメディアを扱うことができますが、Data Protectorでは1種類のメディアが格納されたライブラリしか認識できません。したがって、システムで使用するメディアの種類ごとに、Data Protectorライブラリを1つずつ作成する必要があります。

以下の操作を使用すると便利です。

- ADIC/GRAU DASライブラリおよびStorageTekライブラリの場合は、メディアの取り扱いにData Protectorのコマンドを使用します。ADIC/GRAU DASまたはStorageTek ACSのコマンドを使用してメディアを手動で扱うと、位置の変化やメディアに関する情報をData Protectorが追跡できなくなります。
- ライブラリ全体をData Protectorで管理します。これにより、ライブラリ内のData Protectorメディアと非Data Protectorメディアの両方をData Protectorで追跡する一元管理が可能になります。
- 各メディアの種類ごとにメディアプールを少なくとも1つ作成します(たとえば、4mmメディアタイプ用の1つ、3480メディアタイプ用に1つ)。使用環境に応じて、さらにメディアプールを作成することができます(各部門ごとに1つ、など)。
- Data Protectorでは、ほかのアプリケーションと重複しないメディアセットを使用してください。

ADIC/GRAU DASライブラリまたはSTK ACSライブラリを使用した場合のHPE Data Protectorの照会処理について

Data Protectorの照会処理が実行されると、DASまたはACS Library Serverで構成されているすべてのメディアが照会されます。これらのメディアがData Protectorで複数の論理ADIC/GRAU DASライブラリまたはSTK ACSライブラリ(同じ物理ライブラリ用)に属するメディアとして構成されている場合も同様です。さらに、Data Protectorの照会処理により、Data Protector以外のアプリケーションで使用するように構成されているDASまたはACS Library Server上で構成されているメディアも照会されます。結果として、Data Protectorから照会処理が実行された後、照会処理の実行対象以外の論理ADIC/GRAU DASライブラリまたはSTK ACSライブラリに属するメディアが照会処理の実行対象の論理ADIC/GRAU DASライブラリまたはSTK ACSライブラリに移動されます。

そのため、ADIC/GRAU DASライブラリまたはSTK ACSライブラリを使用する場合は、Data Protectorの照会処理はお勧めしません。Data Protector照会処理によってIDBを同期化するのではなく、Data Protector追加VOLSER操作によって手動でVOLSERを追加することをお推めします。

> **注:**
> 論理ライブラリがData ProtectorではなくADIC/GRAU DASユーティリティを使って構成されているADIC/GRAU DASライブラリの場合は、上記の説明には該当しません。ADIC/GRAU DASユーティリティを使って複数の論理ライブラリが構成されている場合は、問題なくADIC/GRAU DASライブラリを照会できます。Data Protector

スロットを追加する

Data Protectorスロットは、ライブラリで使用するメディアプール内のスロットおよびメディアの処理を完全にサポートします。記憶デバイス内におけるメディアの位置は、スロットを追加することによって構成できます。

一部のライブラリスロットは、ライブラリの構成時に自動的に検出、追加されます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**をクリックします。

3. [結果エリア]でライブラリの名前を右クリックし、**[プロパティ]**をクリックします。
4. **[レポジトリ]**タブをクリックし、Data Protectorで使用するスロットを指定します。**[追加]**をクリックして、そのスロットをリストに追加します。複数のスロットを同時に指定するには、図5-12のようにダッシュを使います。

   ライブラリがサポートしているフォーマットを使用してください。たとえば、SCSIライブラリにスロットを追加するときは、文字を使ったり先頭にゼロを付けたりすることはできません。
5. **[適用]**をクリックして設定内容を確定します。

スロットを削除する

Data Protectorスロットは、ライブラリで使用するメディアプール内のスロットおよびメディアの処理を完全にサポートします。スロットを削除すると、Data Protectorはレポジトリ内のそのスロットを使用したりアクセスしたりすることができなくなります。スロットに関する情報がIDBから削除されます。

メディアスロットの削除は任意のデバイス上の空のスロットに対してのみ有効です。

この操作は、GRAU DASライブラリ内のvolsersには影響しません。IDBから特定のメディアが削除されるのみです。そのため、Data Protectorでは、以降、これらのメディアの存在が認識されず、それらが使用されることはなくなります。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**をクリックします。
3. [結果エリア]でライブラリの名前を右クリックし、**[プロパティ]**をクリックします。
4. **[レポジトリ]**タブをクリックして削除するスロットを選択し、**[削除]**をクリックします。
5. **[適用]**をクリックして設定内容を確定します。

削除したスロットは、スロットリストに表示されなくなります。

メディアを挿入する

メディアの挿入操作では、メディアをライブラリレポジトリに物理的に挿入し、そのメディアをライブラリのメンバーとして自動登録します。

使用するスロットを選択できます。メディアを挿入しても、そのメディアの所属先のメディアプールは影響されません。

メディアを挿入するには、Data Protector GUIを使用することをお勧めします。デバイスの制御機構を使って手動でメディアを挿入した場合は、IDB内の情報の整合性がとれなくなります。この情報を更新するには、デバイスをスキャンする必要があります。

> **ヒント：**
> 1回の操作で複数のメディアをデバイスに挿入することができます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**をクリックします。[結果エリア]に、構成済みデバイスのリストが表示されます。
3. [結果エリア]で、ライブラリの名前をダブルクリックします。
4. **[スロット]**をダブルクリックします。スロットのリストが[結果エリア]に表示されます。
5. メディアを挿入するスロットを右クリックし、**[挿入]**をクリックしてウィザードを起動します。また、複数のスロットに同時に挿入することもできます。

他のメディアを引き続きデバイスに挿入する必要がある場合は、そのように促すプロンプトが表示されます。

メディアを取り出す

メディアの取り出し操作では、ライブラリデバイス内のメディアをレポジトリスロットから挿入/取り出し領域(メールスロット)に物理的に移動します。

メディアを取り出すには、Data Protector Managerを使用することをお勧めします。デバイスの制御機構を使って手動でメディアを取り出した場合は、IDB内の情報との間に食い違いが生じます。この情報を更新するには、デバイスをスキャンします。

メールスロットがいっぱいでメディアを取り出せない場合、Data Protectorでは、メールスロットに空きができるまで、または既定の時間が経過するまで、取り出し操作が繰り返されます。この繰り返し操作の間、ロボティクスは他のセッションにアクセスすることができます。

取り出し操作の実行中、指定されたメディアを他のセッションで使用することはできません。

メディアの一括取り出し

ライブラリ内の複数のメディアは、1回の操作で取り出すことができます。Data Protectorは、メールスロットがいっぱいになると、メディアを取り出して、取り出し用に選択されている他のメディアのためにスペースを開放するように指示を出します。

メディアの取り出しの事前定義

メディアの自動コピーなど、一部の操作では、セッション終了後にメディアを自動で取り出すかどうかを指定できます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**をクリックします。構成されているデバイスのリストが[結果エリア]に表示されます。
3. [結果エリア]で、ライブラリの名前をダブルクリックします。
4. **[スロット]**をダブルクリックします。スロットのリストが[結果エリア]に表示されます。

5. メディアを取り出すスロットを右クリックし、**[取り出し]**をクリックしてウィザードを起動します。また、複数のスロットから同時に取り出すこともできます。
6. 必要に応じて、メディアの新しい収納場所を指定します。
7. **[完了]**をクリックして、ウィザードを終了します。これによって、メディアが取り出されます。

[セッション情報]メッセージに取り出し処理の進行状況が表示されます。

ライブラリデバイス内のメディアを消去する

メディアを消去できるのは、光磁気プラッタの場合だけです。バックアップセッションの開始前に光磁気プラッタだけを消去しておくことができます。これにより、バックアップの処理速度が向上します。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**をクリックします。
3. [結果エリア]で、メディアを消去する光磁気デバイスをダブルクリックします。[スロット]項目と[ドライブ]項目が表示されます。
4. **[スロット]**項目をダブルクリックします。
5. 消去するメディアが格納されているスロットを右クリックし、**[消去...]**をクリックしてウィザードを起動します。
6. 消去するメディアがエクスチェンジャーによってロードされるライブラリドライブを選択します。
7. **[完了]**をクリックして、ウィザードを終了します。これによって、メディアが消去されます。

[セッション情報]メッセージに消去処理の進行状況が表示されます。

VOLSERを手動で追加する

ADIC/GRAU DASまたはSTK ACSライブラリの場合、ライブラリを照会しなくてもに構成されているライブラリにvolsersData Protectorを追加できます。同じ物理ライブラリ用に複数の論理ライブラリが構成されている状況でADIC/GRAU DASライブラリまたはSTK ACSライブラリを使用する場合は、この方法でData Protectorに構成されているライブラリにVOLSERを追加することをお勧めします。ただし、ADIC/GRAU DASライブラリを使用する場合に、論理ライブラリがData ProtectorではなくADIC/GRAU DASユーティリティを使用して構成されている場合は、VOLSERを手動で追加しなくても問題なくADIC/GRAU DASライブラリに対して照会処理を実行できData Protectorます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、VOLSERの追加先のライブラリを検索して展開します。
3. **[スロット]**を右クリックし、ポップアップメニューから**[VOLSERの追加]**を選択します。
4. [プレフィックス]テキストボックスに、VOLSERのプレフィックスを入力します。プレフィックスは、通常は3文字で入力します。

   [開始]テキストボックスに、ライブラリに追加する最初のVOLSERの番号を入力します。

[終了]テキストボックスに、ライブラリに追加する最後のVOLSERの番号を入力します。

5. [完了]をクリックして、IDBにVOLSERを追加します。

ADIC/GRAU DASホストおよびStorageTek ACSLMホストを照会する

ADIC/GRAUライブラリまたはStorageTekライブラリに関する情報をサーバーから取得する場合は、DASまたはACSLMホスト(サーバー)に対する照会を実行できます。照会を実行すると、サーバーのメディアデータベースの内容が返され、IDB内の情報がレポジトリ内に実際に格納されている情報と同期化されます。

GRAU DASまたはStorageTek ACSのコマンドでメディアを管理すると、ライブラリレポジトリ内のメディアの最新の状態をData Protectorが認識できないため、IDBとの不整合が生じますが、この場合に照会を使用すると特に効果的です。

制限事項

レポジトリでADIC/GRAUライブラリに3970を超えるVOLSERが構成されている場合、VOLSERスキャンが正常に完了しないことがあります。この問題を回避するには、スロットを大きなレポジトリから複数の小さなレポジトリに分割するために、複数の論理ADIC/GRAUライブラリを構成します。

> **重要:**
> 同じ物理ライブラリ用に複数の論理ライブラリが構成されている状況でADIC/GRAU DASライブラリおよびSTK ACSライブラリを使用する場合、DASまたはSTK ACSLM Serverを照会することはお勧めしません。手動でVOLSERを追加するようにしてください。ただし、ADIC/GRAU DASライブラリを使用する場合に、論理ライブラリがData ProtectorではなくADIC/GRAU DASユーティリティを使って構成されている場合は、Data Protectorで問題なくADIC/GRAU DASライブラリを照会できます。

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. 構成済みデバイスのリストで、照会対象のライブラリの名前を右クリックし、**[照会]**をクリックします。

これにより、DASホストまたはACSLMホストに対する照会が実行され、情報が取得されます。

第10章: バックアップ

バックアップについて

バックアップとは、システムデータのコピーをバックアップメディア上に作成するプロセスです。このコピーは、オリジナルのデータが破損した場合に備えて保管されます。

バックアップセッションは、バックアップ仕様に基づいており、対話的に開始できます。バックアップセッション中に、Data Protectorはバックアップオブジェクトを読み取り、そのデータをネットワーク経由で転送し、デバイスにセットされたメディアに書き込みます。

> **重要:**
> バックアップするデータが必ず整合性を持つよう注意します。たとえば、バックアップ中にデータが変更されないように、バックアップ前にアプリケーションをシャットダウンするか、「バックアップ」モードに設定します。整合性のないデータをバックアップすると、復元データの使用時に予期せぬ結果を招く場合があります。

Data Protectorバックアップの拡張機能を以下に示します。

- デバイスの使用率の自動調整(負荷調整)
- 共有ディスクのバックアップ
- 無人バックアップのスケジュール設定
- フルバックアップと増分バックアップを組み合わせることによる時間とメディアの節約
- バックアップのさまざまな方法での整理と編成
- オブジェクトミラー機能を使用した、複数の場所への同時バックアップ

Data Protectorヘルプの手順では、バックアップまたはテンプレートに対応するデータの種類に応じたデフォルトのバックアップビュー([種類別])を使用している場合を想定しています。

Oracle、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server、Informix Server、IBM DB2 UDB、Sybaseといったデータベースアプリケーションのバックアップ方法については、『HPE Data Protectorインテグレーションガイド』を参照してください。

バックアップビューを設定する

バックアップビューは、実際のニーズに応じて設定できます。デフォルトのバックアップビューは、**[種類別]**です。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. [表示]メニューで、ビューを設定するオプションのいずれかを選択します。

[バックアップ]コンテキストは、ここで選択したビューに応じて表示されます。

バックアップの種類

Data Protectorのファイルシステムバックアップには、フルバックアップと増分バックアップの2種類があります。これらのバックアップの種類は、バックアップ仕様全体と、ファイルシステムオブジェクトにのみ適用されます。

フルバックアップと増分バックアップを組み合わせるには、バックアップオブジェクトの以下の要素が完全に同じである必要があります。

- クライアント名
- ドライブ/マウントポイント
- 説明
- オーナー(プライベートオブジェクトの場合)

対話型バックアップを行う場合、バックアップの種類を選択するよう要求されます。バックアップをスケジュールする場合は、スケジュールウィザードでバックアップの種類を選択します。たとえば、土曜日にはフルバックアップと同じ、その他の営業日にはIncr1と同じバックアップ仕様を実行するスケジュールを作成できます。

フルバックアップ

フルバックアップでは、前回のバックアップ以降に変更がなくても、選択されたオブジェクトをすべてバックアップします。あるオブジェクトを初めてバックアップするときには、かならずフルバックアップが実行されます。2回目以降のバックアップでは、同じ所有権(プライベートオブジェクトの場合)の保護されていないフルバックアップがバックアップ時点で存在しない場合に、フルバックアップが実行されます。

増分バックアップ

増分バックアップの場合には、保護されているファイルのうち、前回の(フルまたは増分)バックアップより後に更新されたファイルのみがバックアップされます。オブジェクトの増分バックアップを実行できるのは、オブジェクトのフルバックアップ(同一のクライアント名、マウントポイント、記述、およびオーナーを持つ)が存在する場合のみです。

増分バックアップの種類

Data Protectorで実行できる増分バックアップには以下の種類があります。

- 増分

  単純な増分バックアップは、保護されているバックアップのうち最新のバックアップ(フルバックアップか増分バックアップ)をベースとします。

- 増分1～9

  レベル分けされた増分バックアップは、保護されている1つ下のレベルのバックアップのうち、最新のバックアップをベースとします。たとえば増分1バックアップを実行すると、前回のフルバックアップ時より後に更新された、すべてのデータが保存されます。また、増分5バックアップを実行すると、前回の増分4バックアップより後に更新されたすべてのデータが保存されます(増分4バックアップが存在する場合)。[増分1～9]バックアップでは、既存の増分バックアップは参照されません。

- 差分
  この用語は、一部のアプリケーション統合ソフトウェアにおいて増分1バックアップの意味で使用されます。差分バックアップでは、前回のフルバックアップより後の変更がすべて保存されます。

拡張バックアップソリューション

Data Protectorには、拡張増分バックアップおよび合成バックアップなどの拡張バックアップソリューションがあります。

フルバックアップと増分バックアップ

バックアップデータの量を減らすことは、バックアップのパフォーマンスを向上するための基本的なアプローチの1つです。フルバックアップや増分バックアップを計画する際には、時間とリソースをフル活用できるよう検討してください。通常、すべてのシステムのフルバックアップを同じ日に実行する必要はありません。

バックアップの種類については、以下の点を考慮してください。

	フルバックアップ	増分バックアップ
リソース	増分バックアップに比べて時間を要し、多くのメディア容量を必要とします。	前回のバックアップ以降の変更部分のみをバックアップするため、必要な時間とメディア容量が少なくて済みます。
デバイスの取り扱い	単一ドライブのスタンドアロンデバイスを使用する場合は、バックアップデータの量が1つのメディアのサイズを上回っていると、手動でメディアを交換する必要が生じます。	バックアップ中にメディアを追加する必要性は、あまりありません。
復元	シンプルで迅速な復元が可能です。	複数のメディアが必要になるため、復元に時間を要します。
IDBへの影響	IDB内に占めるスペースが大きい	IDBに書き込む情報の量がフルバックアップほど多くありません。

> **注:**
> 適切なデータ保護を設定して、必要なフルバックアップと増分バックアップのすべてを復元に利用できることを保証する必要があります。データ保護が正しく設定されていないとメディアが上書きされるおそれがあり、上書きされると復元チェーンが不完全になります。

従来の増分バックアップ

従来の増分バックアップの仕組み

Data Protectorでは、バックアップオブジェクトの増分バックアップが実行される前に、バックアップオブジェクト内のツリーと、そのオブジェクトの有効な復元チェーン内のツリーが比較されます。前回のバックアップより

後にバックアップオブジェクト内の追加のディレクトリがバックアップ対象として選択された場合や、同じバックアップオブジェクトに対してツリー指定が異なるバックアップ仕様が複数存在する場合など、ツリーが一致していない場合には、フルバックアップが自動的に実行されます。これにより、選択されたファイルがすべてバックアップに含まれるようになります。

変更の検出

従来の増分バックアップでは、前回のバックアップからファイルが変更されたかどうかを判断する主な条件として、ファイルの更新時刻が使用されます。ただし、この基準が役に立たない場合があります。たとえば、ファイルの名前が変更されたり、ファイルが新しい場所に移動されたり、ファイルの属性の一部が変更されたりした場合、そのファイルの更新時刻は変更されません。このため、ファイルは増分バックアップでバックアップされないことがあります。このようなファイルは、次回のフルバックアップでバックアップされます。

名前、場所、属性が変更されたファイルが増分バックアップでバックアップされるかどうかは、バックアップ仕様における以下のオプションによっても決まります。推奨設定を使用すると変更の検出が向上します。

Windowsシステムの場合: アーカイブ属性を使用しない

このオプションは、デフォルトでは選択されていません(アーカイブ属性は使用されます)。これは、推奨設定です。

UNIXシステムの場合: アクセス時刻属性を保存しない

このオプションは、デフォルトでは選択されていません(アクセス時刻属性は保存されます)。このオプションを選択することを推奨します。

従来の増分バックアップは、Windows NTFS Change Log Providerを使用して実行することができます。その場合、前回のフルバックアップ以降に変更されたファイルのリストの生成にはWindows変更ジャーナルが使用され、ファイルツリー巡回は実行されません。Change Log Providerを使用すると、拡張増分バックアップの場合と同様、増分バックアップの全体的なパフォーマンスが向上します。Change Log Providerが何らかの理由で使用できない場合は、通常どおり従来の増分バックアップが実行されます。

名前変更、移動、および属性変更されたファイルを確実に検出し、バックアップするためには、拡張増分バックアップを使用してください。

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からファイルが変更されたかどうかを判断する主な条件として、ファイルの更新時刻が使用されます。ただし、この基準が役に立たない場合があります。たとえば、ファイルの名前が変更されたり、ファイルが新しい場所に移動されたり、ファイルの属性の一部が変更されたりした場合、そのファイルの更新時刻は変更されません。このため、ファイルは増分バックアップでバックアップされないことがあります。このようなファイルは、次回のフルバックアップでバックアップされます。

拡張増分バックアップでは、名称変更や移動が行われたファイルや、特定の属性が変更されたファイルも、確実に検出されてバックアップされます。

一部の変更(パーミッションやACLの変更など)が検出されるかどうかは、バックアップ仕様で下記のオプションをどう設定するかによっても決まります。推奨設定を採用すると、拡張増分バックアップによって変更検出機能が最大限に活用されます。

- **Windowsシステムの場合:** アーカイブ属性を使用しない

  このオプションは、デフォルトでは選択されていません(アーカイブ属性は使用されます)。これは、推奨設定です。

- **UNIXシステムの場合:** アクセス時刻属性を保存しない

  このオプションは、デフォルトでは選択されていません(アクセス時刻属性は保存されます)。このオプションを選択することが推奨設定です。

また、拡張増分バックアップを採用した場合、バックアップ対象として選択されているツリーの一部が変更されたときに、バックアップオブジェクト全体のフルバックアップを行う必要がありません。たとえば、前回のバックアップ以降にバックアップ対象として新たに1つのディレクトリが選択された場合、このディレクトリ(ツリー)についてはフルバックアップが行われ、その他の部分のバックアップは増分型となります。

さらに、Windows NTFS Change Log Providerを使用する場合も、拡張増分バックアップを実行することができます。その場合、前回のフルバックアップ以降に変更されたファイルのリストの生成にはWindows変更ジャーナルが使用され、ファイルツリー巡回は実行されません。特に、多数あるファイルのごく一部のみ変更されるような環境で、Change Log Providerを使用することによって増分バックアップの全体的なパフォーマンスが向上します。

拡張増分バックアップの利点

拡張増分バックアップには、次のような利点があります。

- 名前、位置、または属性が変更されているファイルが増分バックアップされる
- 選択されているツリーの一部が変更されても必要以上のフルバックアップが不要
- 以降のオブジェクト集約(合成バックアップ)ができるようになる

ディスクスペース消費に対する影響

拡張増分バックアップでは、バックアップ対象の各クライアント上で、サイズの小さいデータベースが使用されます。ファイルシステムのマウントポイントごとに、データベースが作成されます。拡張増分バックアップレポジトリは、次のディレクトリに格納されます。

- Windowsシステムの場合: **Windows systems:** *Data_Protector_home*\enhincrdb*MountPointDir*

  マウントポイントディレクトリ(MountPointDir)は、マウントポイントのすべての「:」(コロン)および「\」(円記号)の文字を「_」(下線)で置き換え、末尾の「:」または「\」を省略すれば得られます。
- HP-UXシステムおよびLinuxシステムの場合: **HP-UX and Linux systems:** /var/opt/omni/enhincrdb

通常、クライアント上のディスクスペースへの影響は、バックアップ対象として選択されたファイルのサイズの1%未満です。拡張増分バックアップデータベースを定期的にパージするようにしてください。このパージを行うには、omnircオプション(OB2_ENHINC_DELETE_INTERVALおよびOB2_ENHINC_DELETE_THRESHOLD)を設定します。

Disk Agentの同時処理数

拡張増分バックアップデータベースは、複数のDisk Agentから同時にアクセスできます。バックアップ時に発生しうる問題を回避するには、次のomnircオプションを設定して、Disk Agentの動作を構成します。

- OB2_ENHINC_LOCK_TIMEOUT
- OB2_ENHINC_SQLITE_MAX_ROWS
- OB2_ENHINC_MAX_MEMORY_LIMIT

制限事項

- 拡張増分バックアップはディレクトリレベルでのみサポートされています。バックアップに個々のファイルを選択する場合、拡張増分バックアップモードは使用できなくなります。
- 拡張増分モードを使用する場合は、ハードリンク検出が無効になります。

Change Log Providerを使用した増分バックアップ

従来の増分バックアップおよび拡張増分バックアップでは、バックアップするファイルのリストを作成するために、ファイルツリー巡回が実行されます。ディレクトリ構造の規模が大きく、ファイルが多数含まれている場合など、この処理は非常に時間がかかります。Windows NTFS Change Log ProviderはWindows変更ジャーナルをベースとしており、この問題に対処するため、ファイルツリー巡回を行う代わりに、変更されたファイルのリストを変更ジャーナルに照会します。変更ジャーナルはNTFSボリューム上のファイルに対するすべての変更を高い信頼性で検出および記録することから、Data Protectorでは、前回のフルバックアップ以降に変更されたファイルのリストを生成する際、変更ジャーナルを追跡メカニズムとして使用できます。この方法は、バックアップ間のファイル変更の割合が小さい大規模なファイルシステムを持つ環境できわめて効果的です。この場合、変更があったファイルを判断する処理にかかる時間が大幅に短縮されます。

NTFSボリュームにはそれぞれ固有の変更ジャーナルデータベースがあります。ファイルやディレクトリに変更があると、変更ジャーナルの末尾にレコードが追加されます。レコードには、ファイル名、時刻、および変更の種類が記録されます。変更ジャーナルに実際の変更日が記録されない点に注意してください。ファイルが大きくなりすぎた場合は、変更ジャーナルの先頭にある最も古いレコードが削除されます。バックアップに必要なデータが変更ジャーナルから削除されている場合、Data Protectorはフルバックアップを実行し、変更ジャーナルが使用できなかったという警告を発します。

Change Log Providerを使用したファイルの増分バックアップが実行されるかどうかは、バックアップ仕様の[可能な場合は、標準で用意されているファイルシステムのChange Log Providerを使用]オプションの設定で決まります。このオプションが指定されていると、Data Protectorは変更ジャーナルを使おうとします。変更ジャーナルがアクティブでない場合、Data Protectorは警告を発します。この状況が拡張増分バックアップ中に発生した場合、代わりにフルバックアップが実行されます。この状況が従来の増分バックアップ中に発生した場合、代わりに通常の増分バックアップが実行されます。オプション[アクセス時刻属性を保存しない]および[アーカイブ属性を使用しない]は自動的に選択され、無効にはできません。

前提条件

- 必要なボリュームで変更ジャーナルが有効になっていることを`omnicjutil -query`コマンドを使用して確認します。変更ジャーナルが有効でなかった場合は、`omnicjutil - start`を実行して開始します。`omnicjutil`コマンドの詳細については、*`Mount_point`*`/DOCS/C/MAN`ディレクトリ内のインストールパッケージにある*HPE Data Protector Command Line Interface Reference*を参照してください。
- Change Log Providerを使用して、拡張増分バックアップを開始する前に、少なくとも1つのフルバックアップ(バックアップ仕様でオプション**[可能な場合は、標準で用意されているファイルシステムのChange Log Providerを使用]**が選択されている)が存在することを確認してください。

パフォーマンスとディスクスペース消費

Change Log Providerのパフォーマンスを最高にするには、バックアップを開始する際に増分バックアップを使用します(バックアップの種類は[増分])。増分1～9もサポートされていますが、パフォーマンスが若干低下する可能性があります。

変更ジャーナルは、有効の場合にCPU時間とディスクスペースをある程度消費します。ディスクスペース消費の上限は4 GBです。変更ジャーナルの最大サイズと、最大サイズに達したときに切り捨てられるサイズとを設定できます。詳細については、『*HPE Data Protector Command Line Interface Reference*』を参照してください。

Change Log Providerの最適なパフォーマンスを得るため、Change Log Providerがメモリに保持するエントリ数を`OB2_CLP_MAX_ENTRIES` omnircオプションを使用して指定できます。詳細は、『*HPE Data Protectorトラブルシューティングガイド*』を参照してください。

次の場合、Data Protectorはフルバックアップを実行し、バックアップ仕様のChange Log Providerオプションの設定を無視します。

- クライアントシステム側で変更ジャーナルが有効になっていない場合。
- 必要なデータが変更ジャーナルから削除されていた場合。
- 変更ジャーナルIDが以前と異なっている場合(これは、他のアプリケーションが変更ジャーナルを削除して作り直したことを意味します)。

デフォルトでは、Change Log Providerの初回実行時に拡張増分レポジトリを作成しません。つまり、Change Log Providerエラーが初めて発生したときにフルバックアップが実行され、その際に拡張増分レポジトリが作成されます。この動作は、`OB2_CLP_CREATE_EI_REPOSITORY` omnircオプションを使用して変更できます。詳細は、『*HPE Data Protectorトラブルシューティングガイド*』を参照してください。

考慮事項

- Data Protectorからは、変更ジャーナルに排他モードでアクセスできません。そのため、変更ジャーナルを有効または無効にした場合、Data Protectorに他のアプリケーションの影響が及ぶ可能性があります。指定したボリューム上で変更ジャーナルが無効になると、ファイルやディレクトリに対する変更が該当する変更ジャーナルに一切記録されなくなります。NTFSボリュームでは変更ジャーナルがデフォルトで無効になっているため、`cjutil`または`omnicjutil`コマンドを使用して明示的に有効にする必要があります。同時に、ボリュームの変更ジャーナルは他のアプリケーションがいつでも有効または無効にできます。変更ジャーナルの詳細は、Windowsのマニュアルを参照してください。

  Windows Vista、Windows 7、Windows 8、Windows Server 2008、およびWindows Server 2012では、変更ジャーナルはデフォルトで有効です。
- Change Log Providerの使用は、ファイルシステムの変更割合が少ない環境で有効です。多くの変更が発生するファイルシステムをバックアップする(例えば、多くの一時ファイルが作成された後、間もなく削除されるような環境)では、通常のツリー検索の方が高速です。
- Windows変更ジャーナルのAPIには、属性の詳細情報は含まれません。すべての属性変更がひとまとまりとして扱われます。変更ジャーナルにエントリが生成された場合に、その生成理由がアーカイブ属性の設定解除かそれとも前回のアクセス時刻の変更かを、APIを介して判別することはできません。

  Change Log Providerがアーカイブ属性の設定を解除することはありません。Data Protectorの通常の動作では、ファイルがバックアップされた後でアーカイブ属性が解除されます。このため、Change Log

Providerが使用されている場合は、オプション**[アーカイブ属性を使用しない]**が自動的に選択されます。

通常のData Protectorの動作では、ファイルがバックアップされた後で前回のアクセス時刻がリセットされます(これは、バックアッププロセスは常に前回のアクセス時刻を変更するためです)。Change Log Providerはこのリセットを行わないため、オプション**[アクセス時刻属性を保存しない]**が自動的に選択されます。

この2つのオプションを自動選択する理由は、同じファイルが何度もバックアップされないようにするためです。アーカイブ属性の設定が解除されたり、前回のアクセス時刻が設定し直されたりすると、変更ジャーナルにエントリが表示されて、変更がないのにファイルが次のセッションで再びバックアップされます。

- `NextUsn`の値を`cjutil - query`コマンドを使用してときどき監視し、`NextUsn`が`MaxUsn`の値に近づいたら変更ジャーナルを開始し直す必要があります。
- バックアップ仕様が変更された場合、新しいツリーは全体がバックアップされます。つまり、新しいツリーに対しては通常のツリー巡回が実行され、古いツリーに対してはChange Log Providerが使用されます。
- バックアップスペースの下のディレクトリの名前が変更された場合、そのディレクトリに対しては通常のツリー巡回が実行されます。

制限事項

- Windows NTFSのバックアップのみサポートされています。

合成バックアップ

合成バックアップは、通常のフルバックアップを実行する必要のない高度なバックアップソリューションです。最初のフルバックアップ後には、増分バックアップのみが実行され、続いてそれがフルバックアップとマージされると、新規合成フルバックアップとなります。この処理は何度でも制限なく繰り返すことができ、フルバックアップを再び実行する必要はありません。復元速度については、この形式のバックアップでも従来のフルバックアップでも同じです。

Data Protectorでは、合成バックアップの実行にオブジェクト集約と呼ばれる操作を使用します。

合成バックアップの実行方法

合成バックアップを行う手順は、次のとおりです。

1. フルバックアップと増分バックアップに使用されているバックアップ仕様で、**[拡張増分バックアップ]**オプションを有効にします。
2. フルバックアップを実行します。
3. 以降の増分バックアップが1つのファイルライブラリまたはB2Dデバイス(Smart Cacheを除く)に書き込まれるよう構成します。
4. 増分バックアップが少なくとも1つ存在する場合は、オブジェクト集約を実行します。オブジェクト集約の実行頻度は、バックアップ戦略によって異なります。

仮想フルバックアップ

仮想フルバックアップは、さらに効率の良い合成バックアップです。このソリューションでは、データをコピーするのではなく、ポインターを使ってデータを集約します。これにより、より短時間で集約でき、不必要なデータ複製を行わずに済みます。

この手順は、通常の合成バックアップと基本的に同じですが、次の要件を伴います。

- 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1つのファイルライブラリに書き込まれる必要があります。
- ファイルライブラリで配布ファイルメディア形式を使用する必要があります。

> **注:**
> 仮想フルバックアップではオブジェクトが同じデータブロックを共有するため、スペース消費を削減することができます。ただし、1つのデータブロックが破損した場合には、複数のオブジェクトに影響が生じる可能性があります。信頼性を向上させるため、ファイルライブラリはRAIDディスク上に置いてください。

標準バックアップ手順

標準バックアップ手順では、以下の段階を踏んでバックアップを実行します。

- バックアップ対象データの選択
- バックアップの保存先の選択
- バックアップコピー(ミラー)の作成数の指定
- バックアップセッションの開始またはスケジュール設定

これらの指定は、バックアップ仕様の作成時に行います。バックアップ方法の詳細は、各種オプションを設定することで定義します。デフォルト値をそのまま使用することも、実際のニーズに応じた設定に変更することもできます。

これらの定義済みの設定を変更するには、以下の項目を指定します。

- 目的のバックアップ仕様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。バックアップ仕様の実行前コマンドやデータ保護などが該当します。
- バックアップを実行する日時。

前提条件

- NFS(UNIXシステム上)を使用していない場合、またはシステムをバックアップするためにネットワーク共有バックアップ(Windowsシステム上)を実行していない場合は、Disk Agentを各システムにインストールしている必要があります。
- Data Protectorセル内に少なくとも1つのバックアップデバイスを構成する必要があります。
- バックアップに使用するメディアを準備しておく必要があります。
- バックアップの実行に必要なユーザー権限を持っている必要があります。

ファイルシステムのバックアップ

各ファイルシステムで、バックアップを特定のディレクトリツリーに制限することができます。個々のディレクトリツリーに対して以下のことができます。

- 一部のサブツリーやファイルを除外する
- 特定のワイルドカードのパターンに合致するファイルをバックアップする。
- 特定のワイルドカードのパターンに合致するファイルを除外する

一部のファイルはソフトウェアアプリケーションなどによって無期限に使用されています。これらのファイルは、ファイルシステムバックアップからは除外して、特別な方法でバックアップする必要があります。

バックアップ仕様を作成する

バックアップ仕様では、バックアップするクライアント、ディスク、ディレクトリ、およびファイル、使用するテープデバイスまたはドライブ、追加バックアップコピー(ミラー)の数、バックアップオプション、およびタイミング情報(バックアップをいつ実行するか)を定義します。スタンドアロンDDSドライブに単一のディスクをバックアップするという単純なものから、40台もの大規模なサーバーを8ドライブのテープライブラリにバックアップするという複雑なものまで、さまざまなニーズを満たすバックアップ仕様を柔軟に構成できます。

制限事項

- Data ProtectorのGUIに表示できるバックアップ仕様の数は制限されています。バックアップ仕様の数はパラメーター(名前、グループ、所有者の情報、バックアップ仕様が負荷調整されているかどうかという情報)のサイズによって異なります。このサイズは80kBを超えてはいけません。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで**[バックアップ仕様]**を展開します。
3. バックアップの対象となるデータの種類(**[ファイルシステム]**など)を右クリックし、**[バックアップの追加]**をクリックします。
4. **[バックアップの新規作成]**ダイアログボックスで、利用可能なテンプレートのいずれかを選択し、バックアップの種類とその他のオプションを適切に設定します。**[OK]**をクリックしてウィザードを起動します。
5. ゼロダウンタイムバックアップの場合、構成ページが表示されます。統合を構成して**[次へ]**をクリックします。
6. 統合ソフトウェアバックアップの場合は、クライアントとアプリケーションデータベースを選択します。**[次へ]**をクリックします。
7. [ソース]プロパティページで、バックアップ対象のオブジェクトが格納されているシステムを展開して目的のオブジェクトを選択します。

> **重要:**
> UNIXシステムでインスタントリカバリを実行する予定の場合は、バックアップ対象のすべてのファイルシステムをボリュームグループから選択します。選択しないと、Data Protector GUIを使用してインスタントリカバリを実行できなかったり(Data Protector CLIを使用してインスタント

> リカバリを実行する場合)、データが破損したりすることがあります。

[次へ]をクリックします。

8. [あて先]プロパティページで、バックアップに使用するデバイスを選択します。

   バックアップセッション中にバックアップの追加コピー(ミラー)を作成するかどうかを指定することもできます。**[ミラーの追加]**ボタンと**[ミラーの削除]**ボタンをクリックして、作成するミラー数を指定します。バックアップおよび各ミラーに別のデバイスを選択します。ディスクへのZDBまたはNDMPを使用してバックアップされたオブジェクトは、ミラーリング対象外です。

   > **ヒント:**
   > [負荷調整]オプションをオンにしている場合は、バックアップにデバイスを使用する順序を設定できます。選択したデバイスを右クリック**し、**[デバイスの並べ替え]Data Protectorをクリックしてください。

   [次へ]をクリックします。

9. [オプション]プロパティページでは、バックアップオプションを設定できます。設定可能なバックアップオプションは、バックアップ対象のデータの種類によって異なります。たとえば、ファイルシステムバックアップとディスクイメージバックアップとでは、利用できるオプションの組み合わせが異なります。**[次へ]**をクリックします。

10. [バックアップオブジェクトのサマリー]ページには、バックアップ仕様のサマリーが表示されます。まずバックアップ仕様を保存した上で、プレビューを開始することをお勧めします。Data Protector内部データベースバックアップ、特定のData Protectorアプリケーション統合のバックアップセッション、およびゼロダウンタイムバックアップ(ZDB)では、プレビューを使用できません。**[次へ]**をクリックします。

11. [バックアップ]ウィザードの最後の画面では、構成したバックアップ仕様を保存、保存とスケジュール、開始、またはプレビューできます。以下の処理が行われます。

    - 保存した構成済みバックアップ仕様は、Scopingペインの[バックアップ]コンテキストに新しいバックアップ仕様として表示されます。保存したバックアップ仕様は、そのままプレビューまたは開始することも、修正してからプレビューまたは開始することもできます。

    - 構成したバックアップを保存してスケジュールする場合、まずバックアップ仕様が保存され、次にスケジューラーページが開き、この保存したバックアップ仕様が起動する日時を指定できます。

    - 構成済みバックアップを開始またはプレビューすると、バックアップの進行状況を示すセッション情報メッセージが表示されます。

> **ヒント:**
> 既存のバックアップ仕様をコピーして修正を行う方法で、複数のバックアップ仕様を作成できます。

バックアップ仕様を修正する

既に構成され、保存されているバックアップ仕様を修正することができます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 変更するバックアップ仕様をクリックします。
4. [ソース]プロパティページやその他のプロパティページ([あて先]、[オプション]、および[スケジューリング])を使って、バックアップ仕様を修正し、**[適用]**をクリックします。

修正し終えたバックアップ仕様は、**[アクション]**メニューからプレビューしたり、起動することができます。

> **注:**
> Data Protector内部データベースバックアップ、特定のData Protectorアプリケーション統合のバックアップセッション、およびゼロダウンタイムバックアップ(ZDB)では、プレビューを使用できません。

> **ヒント:**
> バックアップ仕様を修正する場合、まずバックアップを実行してから復元対象のオブジェクトを選択します。復元対象に選択できるのは、最新のバージョンでバックアップされたファイルとディレクトリだけです。バックアップバージョンを変更するには、オブジェクトを右クリックして**[バージョンの選択]**をクリックします。

バックアップをプレビューして開始する

バックアップをプレビューすると、設定内容を確認できます。バックアップのプレビューは、バックアップ対象のディスクからデータを読み取らずに行われます。また、バックアップ用のデバイス内のメディアに対しても、データの書き込みは行われません。

バックアップに関するすべての情報をData Protectorに対して指定すると、既存の(構成され、保存された)バックアップを開始することができます。

制限事項

- Data Protector内部データベースおよび特定のData Protectorアプリケーション統合のバックアップセッションでは、プレビューを使用できません。
- プレビューはゼロダウンタイムバックアップ(ZDB)では使用できません。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 開始またはプレビューするバックアップ仕様を選択します。
4. **[アクション]**メニューを開きます。バックアップ仕様をプレビューするには**[バックアップのプレビュー]**をクリックし、バックアップ仕様を開始するには**[バックアップ開始]**をクリックします。
5. [バックアップのプレビュー]ダイアログボックスまたは[バックアップ開始]ダイアログボックスで、[バックアップの

種類]([フル]または[増分];他のバックアップの種類は個々の統合によって異なる)と[ネットワーク負荷]を選択します。

ディスク+テープへのZDBまたはディスクへのZDB (インスタントリカバリが有効)の場合は、[スプリットミラー/スナップショットのバックアップ]オプションを指定します。

6. **[OK]**をクリックしてバックアップをプレビューまたは開始します。

バックアップの状況がセッション情報メッセージとして表示されます。

> **ヒント:**
> 新しいバックアップを構成する場合、[バックアップ]ウィザードの終了時に対話型バックアップまたは対話型プレビューを開始できます。

バックアップを中止する

バックアップセッションを中止すると、バックアップセッションが強制終了されます。セッションを中止するまでにバックアップしたデータについてのみ、バックアップコピーが存在することになります。

手順

1. [アクション]メニューの**[中止]**をクリックして、バックアップセッションを中止します。

   バックアップ用に選択したディスクのサイズをチェックしているときにバックアップセッションを中止しようとした場合は、サイズのチェックが完了した時点でバックアップが中止されます。バックアップは、サイズチェックが完了すると中止されます。

> **ヒント:**
> Data Protectorの[モニター]コンテキストでは、現在実行されている1つ以上のセッションを中止できます。

失敗したバックアップを再開する

バックアップセッション中に、システムのシャットダウン実行、一時的なネットワーク接続の問題などの理由で、一部のシステムを使用できない場合があります。そのような状況では、一部のシステムに対してバックアップが行われないか、部分的にのみ行われる、つまりいくつかのオブジェクトが失敗することになります。障害を解決した後、問題のセッションを再開できます。この操作では、失敗したオブジェクトのみ再開されます。

前提条件

- Data Protector Admin ユーザーグループに追加されているか、Data Protectorモニターユーザー権限が付与されていることが必要です。

考慮事項

- 失敗したファイシステムやOracle Server統合のバックアップセッションでは、再開セッション機能を使用して、セッションが失敗した地点からバックアップを続行できます。

制限事項

- 対話式で実行されていたセッションが失敗した場合、未保存のバックアップ仕様に基づくことになり、セッションを再開することはできません。
- 一度に複数のセッションを再開することはできません。

> **重要:**
> 失敗したバックアップセッションを再開する前に、バックアップ仕様を変更しないでください。変更すると、すべてのオブジェクトを再開できなくなります。

手順

1. 通常のCell Managerを使用している場合、コンテキストリストで**[内部データベース]**をクリックします。

   Manager-of-Managersを使用している場合は、コンテキストリストで**[クライアント]**を選択し、**[エンタープライズクライアント]**を展開します。問題のセッションのCell Managerを選択します。[ツール]メニューの**[データベース管理]**を選択します。新しいData Protector GUIウィンドウに、[内部データベース]コンテキストが表示されます。
2. Scopingペインで**[内部データベース]**を展開し、**[セッション]**をクリックします。

   [結果エリア]に、セッションのリストが表示されます。各セッションのステータスが[ステータス]列に示されます。
3. 失敗したセッション、中止したセッション、または失敗やエラーで終了したセッションを右クリックし、**[失敗したオブジェクトの再開]**を選択し、失敗したオブジェクトをバックアップします。
4. **[はい]**をクリックして処理を実行します。

バックアップ仕様をコピーする

構成して保存したバックアップ仕様をコピーできます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. [結果エリア]で、コピーしたいバックアップ仕様を右クリックし、**[別名でコピー]**をクリックします。[バックアップを別名でコピー]ダイアログボックスが表示されます。
4. バックアップ仕様のコピーに付ける名前を[名前]テキストボックスに入力します。このバックアップ仕様を特定のバックアップ仕様グループに追加する場合は、[グループ]ドロップダウンリストから目的のグループを選択します。
5. **[OK]**をクリックします。

コピーしたバックアップ仕様は、Scopingペインの[バックアップ]コンテキストと[結果エリア]に新しい名前で表示されます。

バックアップ仕様を削除する

構成して保存したバックアップ仕様を削除できます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 削除するバックアップ仕様を右クリックし、**[削除]**をクリックします。選択を確定します。

選択したバックアップ仕様がScopingペインの[バックアップ]コンテキストから削除されます。

拡張バックアップタスク

バックアップは、さまざまな方法で制御できます。Data Protectorでは、WindowsシステムおよびUNIXシステムに対応した拡張バックアップタスクをサポートしています。

前提条件

- NFS(UNIXシステム上)を使用していない場合、またはシステムをバックアップするためにネットワーク共有バックアップ(Windowsシステム上)を実行していない場合は、Disk Agentを各システムにインストールしている必要があります。
- セル内に少なくとも1つのバックアップデバイスを構成する必要があります。
- バックアップに使用するメディアを準備しておく必要があります。
- バックアップの実行に必要なユーザー権限を持っている必要があります。
- 拡張バックアップタスクを続行する前に、標準バックアップ手順を考慮してください。

拡張バックアップタスクとは

拡張バックアップタスクでは、デフォルトで使用されない特定のオプションを指定したり、標準バックアップ手順とは異なる操作を実行することができます。

- バックアップ対象となるネットワーク共有ディスクを選択する
- 条件に一致するファイルだけをバックアップ対象として選択する
- バックアップ対象から除外するファイルを指定する
- バックアップを開始するためのショートカットの位置を選択する
- 複数のDisk Agentを使用してバックアップを実行する
- ディスクディスカバリによるクライアントバックアップ
- ディスクイメージバックアップ
- Webサーバーのバックアップ

バックアップ対象となるネットワーク共有ディスクを選択する

データのバックアップ先としてWindows共有ディスクを使用できます。共有ディスクを介して他のリモートシステムをバックアップするには、通常のData Protector Disk Agentクライアントを使用する必要があります。

直接にバックアップできないシステムがある場合は、共有ディスクを経由して間接的にバックアップすることができます。ただし、共有ディスクのバックアップを主なバックアップ方法として使用することはお勧めできません。

ネットワーク内で共有されているWindowsシステム上のファイルシステムをバックアップするのは、次の場合です。

- システムがData Protectorのセルの一部ではなく、Data Protector Disk Agentがインストールされていない場合。
- Data Protectorで直接サポートされていないプラットフォーム(Windows for Workgroups、Windows 3.1システム、Windows NTなど)をバックアップする場合。

> **ヒント：**
> ネットワーク負荷を軽減するためには、Disk AgentクライアントはMedia Agentクライアントでもある必要があります。そうでない場合、データはネットワーク上を2度転送されます。

前提条件

バックアップ対象の共有ディスクにアクセスするための適切なパーミッションが付与されるように、Disk Agentクライアント上のData Protector Inetアカウントを変更しておく必要があります。このアカウントには、ローカルクライアントシステムとリモート共有ディスクの両方に対するパーミッションが付与されていなければなりません。Windows VistaおよびWindows Server 2008システムより前のバージョンのWindowsの場合、アカウントはローカルシステムアカウントではなく特定のユーザーアカウントである必要があります。

Inetサービスのユーザーアカウントを設定すると、ローカルシステム上にあっても共有ディスクをバックアップできます。

Windows Vista、Windows 7、Windows 8、Windows Server 2008、およびWindows Server 2012の場合

バックアップ対象の共有ディスクにアクセスするために必要なパーミッションを持つユーザーアカウントを追加する必要があります。このアカウントはローカルシステムアカウントである必要があります。

Disk AgentクライアントでData Protector Inetアカウントを変更する前に、この前提条件を満たしている必要があります。Disk Agentが実行されるData Protectorクライアントで、次のコマンドを実行します。

```
omniinetpasswd -add User@Domain [Password]
```

要件

- 共有ドライブは、バックアップウィザードでマッピングする必要があります。
- Windows GUIを使用します。これは、WindowsシステムのブラウズがUNIX GUIでサポートされていない

ためです。

制限事項

- 共有ディスクのバックアップでは、一部のファイル属性がバックアップされません。共有ホスト上で表示されている属性だけがバックアップ可能です。データの復元には支障がありませんが、ファイルやディレクトリの属性が一部失われる可能性があります。
- VSS機能を使用してネットワーク共有ボリューム上にデータを格納するライターのバックアップはサポートされていません。また、Disk Agentと[シャドウコピーを使用]オプションを有効にしてネットワーク共有またはリモートネットワークフォルダーをバックアップすることは、Windows Server 2012でもサポートされていません。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで**[バックアップ仕様]**を展開します。
3. バックアップの対象となるデータの種類(**[ファイルシステム]**など)を右クリックし、**[バックアップの追加]**をクリックします。
4. **[バックアップの新規作成]**ダイアログボックスで、利用可能なテンプレートのいずれかを選択し、**[OK]**をクリックしてウィザードを起動します。
5. [ソース]プロパティページで、ドロップダウンリスト(Windowsシステム上で実行されているGUIで使用可能)から**[ネットワーク共有のバックアップ]**を選択します。
6. **[ネットワーク共有の割り当て]**をクリックして**[ネットワーク共有のブラウズ]**ウィンドウを開きます。
7. バックアップに使用するDisk Agentが動作しているクライアントシステムを[クライアントシステム]ドロップダウンリストから選択します。
8. [共有ディレクトリ]ボックスで、目的の共有ディレクトリを入力または選択し、**[OK]**をクリックします。他のディスクも選択したい場合は、**[適用]**をクリックします。
9. [ソース]プロパティページで、バックアップ対象の共有ファイルシステムを入力または選択します。**[次へ]**をクリックします。
10. [あて先]プロパティページで、バックアップに使用するデバイスを選択します。

    バックアップセッション中にバックアップの追加コピー(ミラー)を作成するかどうかを指定することもできます。**[ミラーの追加]**ボタンと**[ミラーの削除]**ボタンをクリックして、作成するミラー数を指定します。バックアップおよび各ミラーに別のデバイスを選択します。ディスクへのZDBまたはNDMPバックアップ機能を使用してバックアップされたオブジェクトは、ミラーリング対象外です。

    > **ヒント:**
    > [負荷調整]オプションをオンにしている場合は、バックアップにデバイスを使用する順序を設定できます。選択したデバイスを右クリックし、[デバイスの並べ替え]Data Protectorをクリックしてください。

    [次へ]をクリックします。
11. [オプション]プロパティページでは、バックアップオプションを設定できます。設定可能なバックアップオプションは、バックアップ対象のデータの種類によって異なります。たとえば、ファイルシステムバックアップとディスクイメージバックアップとでは、利用できるオプションの組み合わせが異なります。

Windows Vista、Windows 7、Windows Server 2008、およびWindows Server 2012では、次の追加手順を実行します。

a. [バックアップ仕様オプション]で、**[拡張]**ボタンをクリックします。

b. [バックアップオプション]ダイアログボックスの[所有権]に、バックアップ対象の共有ディスクにアクセスするために必要なパーミッションを持つユーザーアカウントの情報を入力します。

c. **[OK]**をクリックします。

12. **[次へ]**をクリックします。
13. [バックアップオブジェクトのサマリー]ページには、バックアップ仕様のサマリーが表示されます。まずバックアップ仕様を保存した上で、プレビューを開始することをお勧めします。**[次へ]**をクリックします。
14. [バックアップ]ウィザードの最後の画面では、構成したバックアップ仕様を保存、保存とスケジュール、開始、またはプレビューできます。以下の処理が行われます。
    - 保存した構成済みバックアップ仕様は、Scopingペインの[バックアップ]コンテキストに新しいバックアップ仕様として表示されます。保存したバックアップ仕様は、そのままプレビューまたは開始することも、修正してからプレビューまたは開始することもできます。
    - 構成したバックアップを保存してスケジュールする場合、まずバックアップ仕様が保存され、次にスケジューラーページが開き、この保存したバックアップ仕様が起動する日時を指定できます。
    - 構成済みバックアップを開始またはプレビューすると、バックアップの進行状況を示すセッション情報メッセージが表示されます。

バックアップする各ディスクについて、Disk Agentが1つずつ起動されます。このため、同時に多数のディスクをバックアップすると、バックアップの性能が低下することがあります。

条件に一致するファイルだけをバックアップ対象として選択する

ワイルドカード文字を使用することで、特定の条件に一致するファイルをバックアップできます。

> **注:**
> この機能は、Data ProtectorのNDMPサーバー用統合ソフトウェアではサポートされていません。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 目的のオブジェクトに対応するバックアップ仕様を選択します。
4. **[バックアップオブジェクトのサマリー]**タブをクリックします。
5. [バックアップオブジェクトのサマリー]ページで、バックアップオブジェクトを右クリックし、**[プロパティ]**をクリックします。
6. **[ツリー/フィルター]**タブをクリックし、**[フィルター]**ボタンをクリックします。
7. 特定のファイルだけをバックアップするための条件を[オンリー]テキストボックスに入力し、**[追加]**ボタン

をクリックします。

必要な条件をすべて入力し終えるまで、この手順を繰り返します。

8. **[OK]**をクリックします。

バックアップ対象から除外するファイルを指定する

ワイルドカード文字を使用することで、特定の条件に一致するファイルをバックアップ対象から除外できます。

> **注:**
> Data Protector NDMPサーバー統合ソフトウェアでは、バックアップ対象からのファイルの除外はサポートされていません。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 目的のオブジェクトに対応するバックアップ仕様を選択します。
4. **[バックアップオブジェクトのサマリー]**タブをクリックします。
5. [バックアップサマリー]ページで、バックアップオブジェクトを右クリックし、**[プロパティ]**をクリックします。
6. **[ツリー/フィルター]**タブをクリックし、**[フィルター]**ボタンをクリックします。
7. スキップするファイルを指定する条件(*.tmpなど)を[スキップ]テキストボックスに入力し、**[追加]**ボタンをクリックします。

   必要な条件をすべて入力し終えるまで、この手順を繰り返します。
8. **[OK]**をクリックします。

バックアップを開始するためのショートカットの位置を選択する

ディスク上に選択したバックアップ仕様のショートカットを作成し、後でこのショートカットを使用して、Data Protector GUIを使用せずにバックアップを実行できます。このショートカットをダブルクリックすると、コマンドプロンプトが開き、選択したバックアップ仕様に対して`omnib`コマンドが実行されます。

制限事項

- バックアップを開始するためのショートカットは、Windowsシステム上でのみサポートされています。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**な

ど)を展開します。

3. 選択したバックアップ仕様を右クリックし、**[ショートカットの位置を選択]**をクリックします。[別名で保存]ダイアログボックスが表示されます。
4. 名前を入力し、ショートカットの位置を選択して、**[保存]**をクリックします。

ディスク上の選択した位置に、選択したバックアップを開始するためのショートカットが表示されます。

複数のDisk Agentを使用してバックアップを実行する

大きなオブジェクトをバックアップする場合は、バックアップを高速化するために複数のDisk Agentを使用できます。

以下に追加情報を示します。

- バックアップ仕様内で、どのディレクトリ/ファイルを新しいDisk Agentでバックアップするかを手動で定義する必要があります。同じデータが重複しないように注意してください。
- 複数のDisk Agentが同時に同じディスクにアクセスすると、ディスクからのデータ読み込み速度が低下します。ディスクアレイを使用している場合は、この限りではありません。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで**[バックアップ仕様]**を展開します。
3. バックアップの対象となるデータの種類(**[ファイルシステム]**など)を右クリックし、**[バックアップの追加]**をクリックします。
4. [バックアップの新規作成]ダイアログボックスで、利用可能なテンプレートのいずれかを選択し、**[OK]**をクリックしてウィザードを起動します。
5. 複数のDisk Agentを使用してディレクトリ/ファイルをバックアップする場合、[ソース]プロパティページでは、同じ論理ディスクまたはマウントポイント上のディレクトリ/ファイルを選択しないでください。一方、1つのDisk Agentでバックアップするディレクトリ/ファイルは選択できます。**[次へ]**をクリックします。
6. [あて先]プロパティページで、バックアップに使用するデバイスを選択します。**[次へ]**をクリックします。

   バックアップセッション中にバックアップの追加コピー(ミラー)を作成するかどうかを指定することもできます。**[ミラーの追加]**と**[ミラーの削除]**をクリックして、作成するミラー数と、これに使用するデバイスを指定します。オブジェクトミラーの作成には、バックアップに使用するデバイスと同じデバイスを使用することはできません。ディスクへのZDB、およびNDMPバックアップでは、オブジェクトのミラー操作はサポートされていません。
7. [オプション]プロパティページで、その他のオプションを必要に応じて指定し、**[次へ]**をクリックします。
8. [バックアップサマリー]ページで**[手動で追加]**をクリックします。
9. [バックアップオブジェクトの選択]ダイアログボックスで、バックアップするオブジェクトの種類(**Windows ファイルシステム**など)を選択します。**[次へ]**をクリックします。
10. [一般的な選択項目]ダイアログボックスで、バックアップ対象のクライアントシステムとマウントポイントを選択します。説明も入力する必要があります。**[次へ]**をクリックします。
11. [ツリー/フィルターの選択]ダイアログボックスで、バックアップに含めるディレクトリ/ファイルまたはバックアップから除外するディレクトリ/ファイルを指定します。ここで選択したディレクトリ/ファイルは、単一のDisk Agentでバックアップされます。**[次へ]**をクリックします。

12. [一般オブジェクトオプション]、[拡張オブジェクトオプション]、[Windows固有オブジェクトオプション]の各ダイアログボックスで、その他のオプションを必要に応じて指定し、**[次へ]**をクリックします。最後のダイアログボックスでは**[完了]**をクリックします。
13. 他のDisk Agentでバックアップするマウントポイント上のディレクトリ/ファイルについても手順9～13を繰り返します。
14. [バックアップサマリー]ページで、バックアップ仕様のサマリーを確認し、**[次へ]**をクリックします。
15. [バックアップ]ウィザードの最後の画面では、構成したバックアップ仕様を保存、保存とスケジュール、開始、またはプレビューできます。

小サイズの繰り返しバックアップを処理する

数多くの小サイズのオブジェクトを繰り返しバックアップしなければならない場合、多数のバックアップセッションを実行する必要が生じます。各バックアップセッション中には、メディアがドライブにロードおよびアンロードされます。そのようなバックアップは速度が遅いだけでなく、メディアも劣化させます。より経済的にメディアを使用し、時間を節約するには、ファイルライブラリデバイスを作成し、テープではなくディスクで小サイズの繰り返しバックアップを実行することをお勧めします。データは、オブジェクトコピー機能を使用して、後でディスクからテープメディアに移動できます。

この方法を使用すると、メディアのロードとアンロードが1度で済むため、オブジェクトコピーセッションでバックアップが高速に実行され、メディアが経済的に使用されます。

小サイズの多数のオブジェクトのバックアップを頻繁に実行するには、以下のタスクを実行します。

1. ファイルライブラリデバイスを構成します。ライターのブロックサイズを第2段階で使用されるデバイスのブロックサイズに設定します。
2. 小サイズのオブジェクトすべてに対して1つのバックアップ仕様を作成します。最初の手順で作成したファイルデバイスをバックアップに使用します。
3. バックアップを実行またはスケジュール設定します。
4. オブジェクトコピー機能を使用して、バックアップデータをテープに移動します。

ディスクイメージバックアップ

ディスクイメージのバックアップはUNIXプラットフォームとWindowsプラットフォームのどちらでも実行できます。

ディスクのディスクイメージバックアップは、データソースに保存されたファイルやディレクトリ構造が追跡されることなく、ディData Protectorスク、ディスクパーティション、または論理ボリュームがバックアップされる、高速なバックアップです。Data Protectorディスクイメージ構造はキャラクター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。

> **注:**
> Windowsシステムの場合、VSSライターを使用してディスクイメージのバックアップを実行します。この方法では、バックアップ中のボリュームがロック解除されたままの状態で、他のアプリケーションからアクセスできます。これは、システムボリュームをバックアップする場合に特に重要です。ディスクイメージのVSSバックアップは、デフォルトで有効になっています。VSSディスクイメージバックアップのカスタマイズには、次のomnircオプションを使用します。`OB2_VSS_RAW_BACKUP`、`OB2_VSS_RAW_BACKUP_ALLOW_FALLBACK`、および`OB2_VSS_SNAPSHOT_TIMEOUT`。

どのような場合にディスクイメージバックアップを使用するか

- 小サイズのファイルが多数存在し、バックアップ速度の高さが要求される場合。
- ディザスタリカバリへの備えやソフトウェアの大幅な変更を控えていることなどを理由にフルディスクバックアップが必要な場合。Windowsシステムでは、EADRおよびOBDRの準備をする場合にディスクイメージバックアップを使用できます。
- ディスク間の直接接続が不可能な環境でファイルシステムを他のディスクに複製する必要がある場合。後者はオリジナルのディスクと同じでなければなりません。

ディスクイメージセクションの指定方法

UNIXシステムの場合

- ディスクイメージセクションを指定するには、`/dev/rdsk/Filename`という形式を使用します。例: `/dev/rdsk/c2t0do`
- raw論理ボリュームセクションを指定するには、`/dev/vgNumber/rlvolNumber`のように指定します。例: `/dev/vg01/rlvol1`

Windowsシステムの場合

ディスクイメージセクションは2つの方法で指定できます。1番目は特定のボリュームを選択する方法で、2番目はディスク全体を選択する方法です。ゼロダウンタイムバックアップの場合は、2番目の方法を使用します。

- `\\.\DriveLetter`例: `\\.\E:`

> **注:**
> ボリューム名にドライブ文字を指定すると、バックアップ中にボリュームがロックされません。マウントされていないボリュームやNTFSフォルダーとしてマウントされているボリュームをディスクイメージのバックアップに使用することはできません。

- `\\.\PHYSICALDRIVE#`ここで、#は、バックアップするディスクの現在の番号です。例: `\\.\PHYSICALDRIVE3`

ディスクイメージセクションの場所

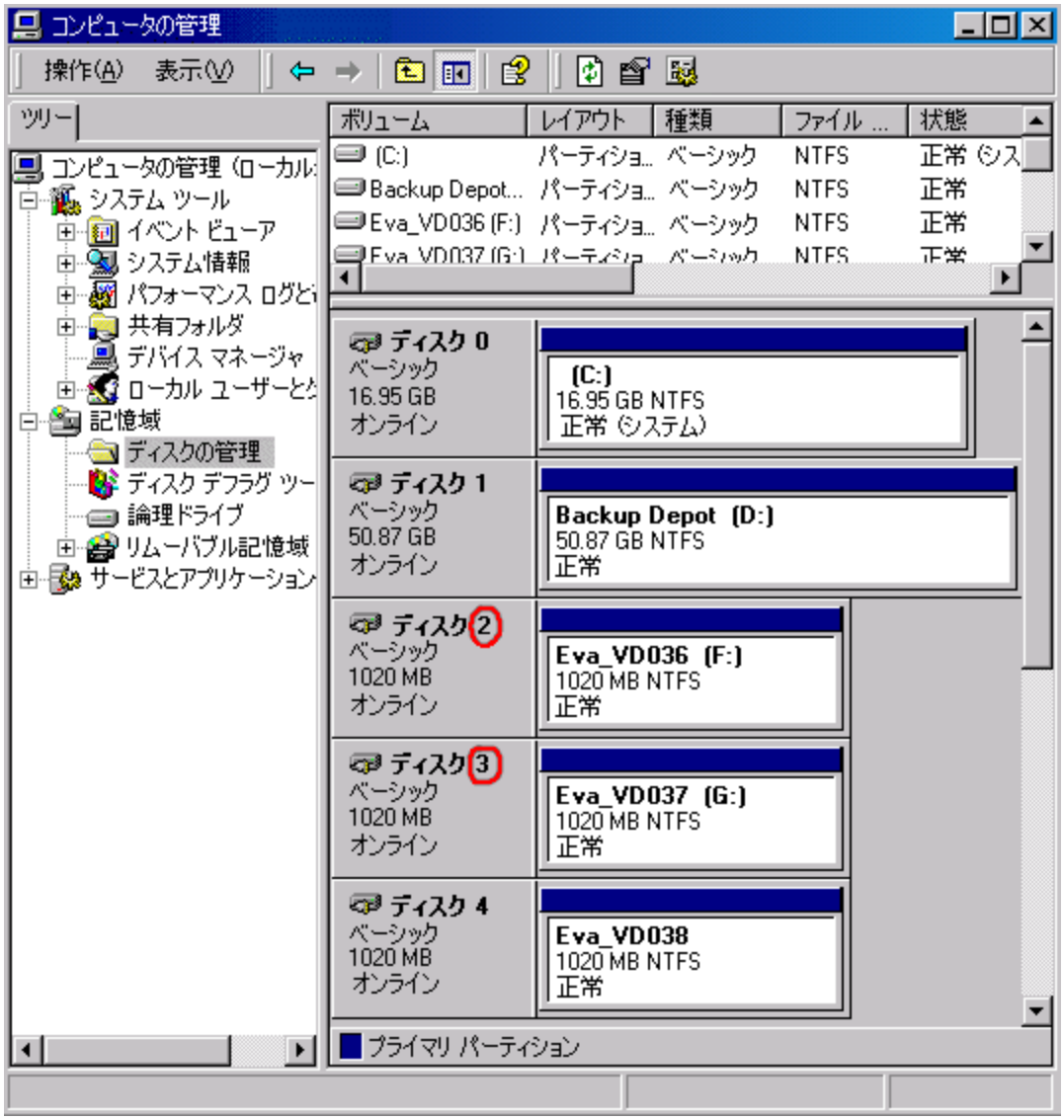
UNIXシステムの場合

通常、`/dev/rdsk`ディレクトリにディスクイメージセクションがあります。raw論理ボリュームは`/dev/vgNumber`にあります。HP-UXシステムの場合、raw論理ボリュームは`/dev/vgNumber`にあります。新しい論理ボリュームの先頭文字は`r`でなければなりません(例: `/dev/vg01/rlvol2`)。

Windowsシステムの場合

コントロールパネルの**[管理ツール]**をクリックし、**[コンピューターの管理]**、**[記憶域]**、**[ディスクの管理]**を順にクリックすると、ディスクの現在の番号(およびドライブ文字)を確認できます。

Windowsシステム上でディスクを表す番号(物理ドライブ番号)



> **注：**
> Windowsシステムでは、システムを再起動すると、ディスクを表す番号が変更されることがあります。

ディスクディスカバリによるクライアントバックアップ

ディスクディスカバリによるクライアントバックアップの場合、クライアントをデータソースとして指定します。別のディスクが後でマウントされた場合、そのディスクはバックアップに加えられます。ファイルシステムのバックアップでは、新たに追加されたディスクやマウントされたファイルシステムがバックアップ仕様で指定されていない場合は、ユーザーが指定する必要がありますが、ディスクディスカバリの場合は、ユーザーによる指定は不要です。

Data Protectorでは、バックアップ時にクライアントに問い合わせが行われ、そのシステムに付加されているディスク上の全ファイルシステムが検出されます。検出された各ファイルシステム(WindowsシステムのCONFIGURATIONも)は、通常のファイルシステムとしてバックアップされます。各ファイルシステムオブジェクトに関する記述が生成され、ファイルシステムマウントポイントがクライアントバックアップの記述に追加されます。

ディスクディスカバリによるバックアップ時には、実ディスクだけがバックアップのData Protector対象になります。したがって、UNIXシステムでは、NFS、CDマウントフData Protectorァイルシステム、および取り外し可能メディアのマウントポイントの検出は行われません。さらに、Windowsシステムでは、CDや取り外しData Protector可能メディアのドライブは検出されません。

どのような場合にディスクディスカバリを使用するか

このバックアップの種類は、構成が急速に変化するダイナミックな環境で特に便利です。以下のような条件の場合に推奨されます。

- マウントやマウント解除が頻繁に行われる比較的小さなディスクを持つワークステーションをバックアップする場合。
- マウントされているファイルシステムの数にかかわらず、マウントポイントを使用して1つのディレクトリにデータをバックアップする場合。例えば、`/home/data`の場合、`/home/data/disk1`および`/home/data/newdisk/disk2`は、互いに独立して頻繁にマウントまたはアンマウントできます。
- システム全体をバックアップしてディザスタリカバリの準備をする場合。

バックアップ仕様

ディスクディスカバリバックアップを定義するバックアップ仕様を作成する場合は、システムのディスク(ボリューム)の横にあるチェックボックスではなく、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クリックします。クライアントシステムを選択した後、構成済みのバックアップの種類を[バックアップオブジェクトのサマリー]プロパティページで確認できます。`Type`ラベルの下に`Client System`と表示されるはずです。

Webサーバーのバックアップ

Webサーバーをバックアップするには、標準バックアップ手順でファイル、ディレクトリ、およびクライアントをバックアップします。さらに、以下のことを考慮する必要があります。

- クライアントバックアップの実行時にはWebサーバー全体がバックアッData Protectorプされますが、デフォルトでは、他のクライアント/サーバー上のデータはバックアップされません。他のクライアント/サーバー上のデータをバックアップするには、それらもバックアップ対象として明示的に選択する必要があります。
- ファイルシステムバックアップの実行時には、Webサーバーとそのクライアントのファイルとディレクトリがどこに存在するかを指定する必要があります。Web構成ファイルとルートディレクトリは、常にバックアップ対象に含めてください。
- Data Protectorでは、すべてのファイルを静的な状態でバックアップします。バックアップ中にファイルが変更されても、変更内容はバックアップされません。

OracleやInformix Serverなどのデータベースが Webサーバー上に置かれている場合は、そのデータベースに固有のバックアップ手順を使用してください。

Wake ONLANサポートを有効にする

WindowsシステムがWake ONLANに対応している場合、Data Protector Wake ONLANサポートを使用できます。

バックアップセッションマネージャーは、Wake ONLANサポートの使用が設定されたクライアントと接続できなかったとき、Wake ONLANプロトコルに従ってwake-up要求を送信し、クライアントとの接続をリトライします。この結果、通常であればバックアッププロセスに支障が出るデスクトップシステムの節電機能を完全に活用することができます。

Wake ONLANサポートを利用できるのは、HPE NightDIRECTORシリーズなど、Wake ONLAN互換のLANインターフェイスを備えたコンピューターです。BIOSセットアップに、Wake ONLAN (WOL)オプションがあります。

WindowsクライアントにDisk Agentをインストールしてセルに追加すると、クライアントのMACアドレスが自動的に検出されます。MACアドレスは、手動で変更することもできます。

手順

1. コンテキストリストで**[クライアント]**をクリックします。
2. Scopingペインでクライアントを参照して右クリックし、**[プロパティ]**をクリックします。
3. **[詳細設定]**タブをクリックします。
4. [マジックパケットを使用可能にする]オプションを選択します。必要に応じて、MACアドレスを変更します。
5. **[適用]**をクリックします。

バックアップテンプレートについて

Data Protectorバックアップテンプレートを使用すると、(多数の)バックアップ仕様と関連オプションの処理が簡略化されます。テンプレートにはバックアップ仕様で明確に指定されたオプション群が含まれており、これらはバックアップ仕様を作成したり変更したりするときのベースとして使用できます。

テンプレートは、同じような使われ方をする(デバイスオプションやファイルシステムオプションなどの設定に共通性がある)さまざまなオブジェクトを持つバックアップ仕様を多数構成する場合に使用します。

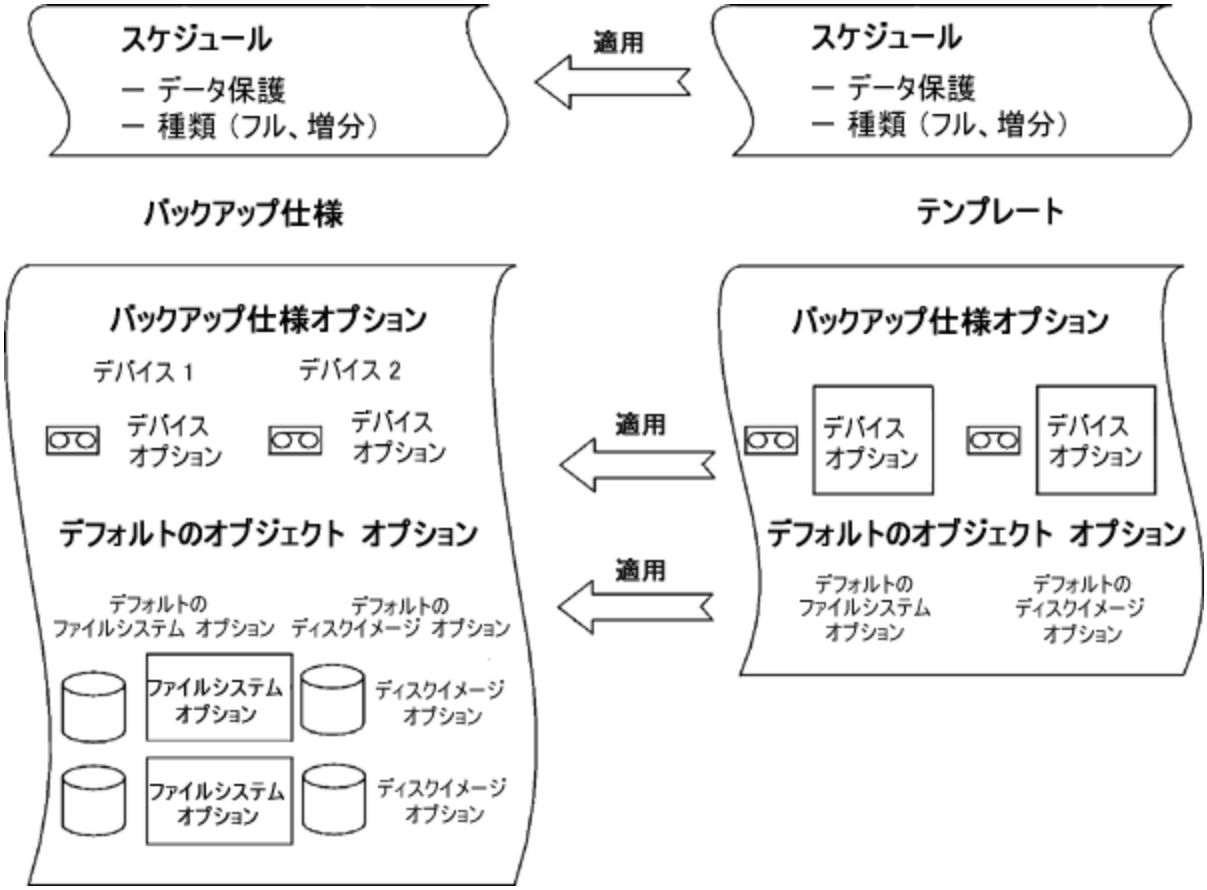
Data Protectorには、各種データ(ファイルシステム、Exchangeなど)用に、オブジェクト、デバイス、オプション、およびスケジュールの指定がないデフォルトのテンプレートが用意されています。空のファイルシステムバックアップや空のInformixバックアップのように空白のバックアップテンプレートの場合、選択するオブジェクトやデバイスはありません。バックアップ仕様のオプションやオブジェクトのオプションにはData Protectorのデフォルトの値があり、バックアップのスケジュールはありません。

テンプレートは、バックアップ仕様と同じように作成および変更できますが、オブジェクトなどの要素が指定されていない点が異なります。テンプレートは、既存のバックアップ仕様に適用することも、また、新しいバックアップの作成時に使用することもできます。後でテンプレートを変更する場合、その変更を有効にするためには再度そのテンプレートを適用しなければなりません。

> **ヒント:**
> カーソルをテンプレートの上に移動すると、テンプレートの説明を示すポップアップウィンドウが表示さ

れます。

バックアップオプションスキーム



バックアップテンプレートを新規作成する

実際の環境のニーズに応じた新しいバックアップテンプレートを作成することができます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで**[テンプレート]**を展開します。
3. 作成するテンプレートの種類(**[ファイルシステム]**など)をマウスの右ボタンでクリックし、**[テンプレートの追加]**をクリックしてウィザードを起動します。
4. ウィザードの指示に従って、使用するバックアップデバイスおよび適用するバックアップオプションを設定します。また、必要に応じてスケジュールも設定できます。

新しいテンプレートは、新しいバックアップ仕様を作成するとき、またはテンプレートを1つまたは複数のバックアップ仕様に適用するときに利用できます。

バックアップテンプレートを修正する

バックアップテンプレートは修正が可能です。バックアップ仕様をテンプレートに合わせて変更する場合、仕様は自動更新されないため、テンプレートを適用し直す必要があります。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[テンプレート]**を展開し、修正するテンプレートに関連付けられているデータの種類(**[ファイルシステム]**など)を展開します。その種類の保存済みテンプレートがすべて表示されます。
3. 修正するテンプレートを右クリックし、**[プロパティ]**をクリックします。
4. テンプレートのプロパティページで、テンプレートを修正し、**[適用]**をクリックします。

修正したテンプレートは、バックアップ仕様を新規作成するときに使用でき、また、バックアップ仕様に適用することもできます。

バックアップテンプレートをコピーする

バックアップテンプレートは、以下の手順でコピーできます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[テンプレート]**を展開し、目的の種類のバックアップテンプレート(**[ファイルシステム]**)を展開します。保存済みのバックアップテンプレートがすべて表示されます。
3. [結果エリア]で、コピーしたいテンプレートを右クリックし、**[別名でコピー]**をクリックします。[バックアップを別名でコピー]ダイアログボックスが表示されます。
4. テンプレートのコピーに付ける名前を[名前]テキストボックスに入力します。このテンプレートのコピーを特定のグループに追加する場合は[グループ]ドロップダウンリストから目的のグループを選択します。
5. **[OK]**をクリックします。

コピーしたバックアップテンプレートがScopingペインと[結果エリア]に表示されます。

バックアップテンプレートを削除する

バックアップテンプレートは、以下の手順で削除できます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[テンプレート]**を展開し、目的の種類のバックアップテンプレート(**[ファイルシステム]**)を展開します。保存済みのバックアップテンプレートがすべて表示されます。
3. 削除するテンプレートを右クリックし、**[削除]**をクリックします。選択を確定します。

バックアップテンプレートが削除されます。

バックアップテンプレートをバックアップ仕様に適用する

テンプレートを1つまたは複数のバックアップ仕様に適用するときに利用できます。この場合、適用するオプショングループを選択できます。

> **注:**
> バックアップテンプレートを既存のバックアップ仕様に適用し、[ファイルシステム]オプションおよび[スケジュール]オプション、またはいずれか一方を選択する場合、テンプレートからの保護設定がバックアップ仕様の該当部分に設定されていた保護設定より優先して適用されます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで**[バックアップ仕様]**を展開します。
3. 保存済みのバックアップ仕様を右クリックし、**[テンプレートの適用]**をクリックします。
4. **[テンプレートの適用]**ダイアログボックスで、バックアップ仕様に適用するテンプレートを選択します。

   > **ヒント:**
   > テンプレートのオプション(**[ツリー]**、**[バックアップオプション]**、**[デバイス]**など)のうち、特定のオプションの選択を解除できます。この場合、それらのオプションはバックアップ仕様に適用されません。

   > **注:**
   > 統合ソフトウェアのバックアップ仕様にテンプレートを適用する場合は、目的のバックアップ仕様を[結果エリア]で開けずに操作を行う必要があります。バックアップ仕様を最初にクリックして開いてしまうと、**[テンプレートの適用]**オプションが有効にならないので、そのバックアップ仕様にテンプレートを適用できません。

5. **[OK]**をクリックすると、テンプレートがバックアップ仕様に適用されます。

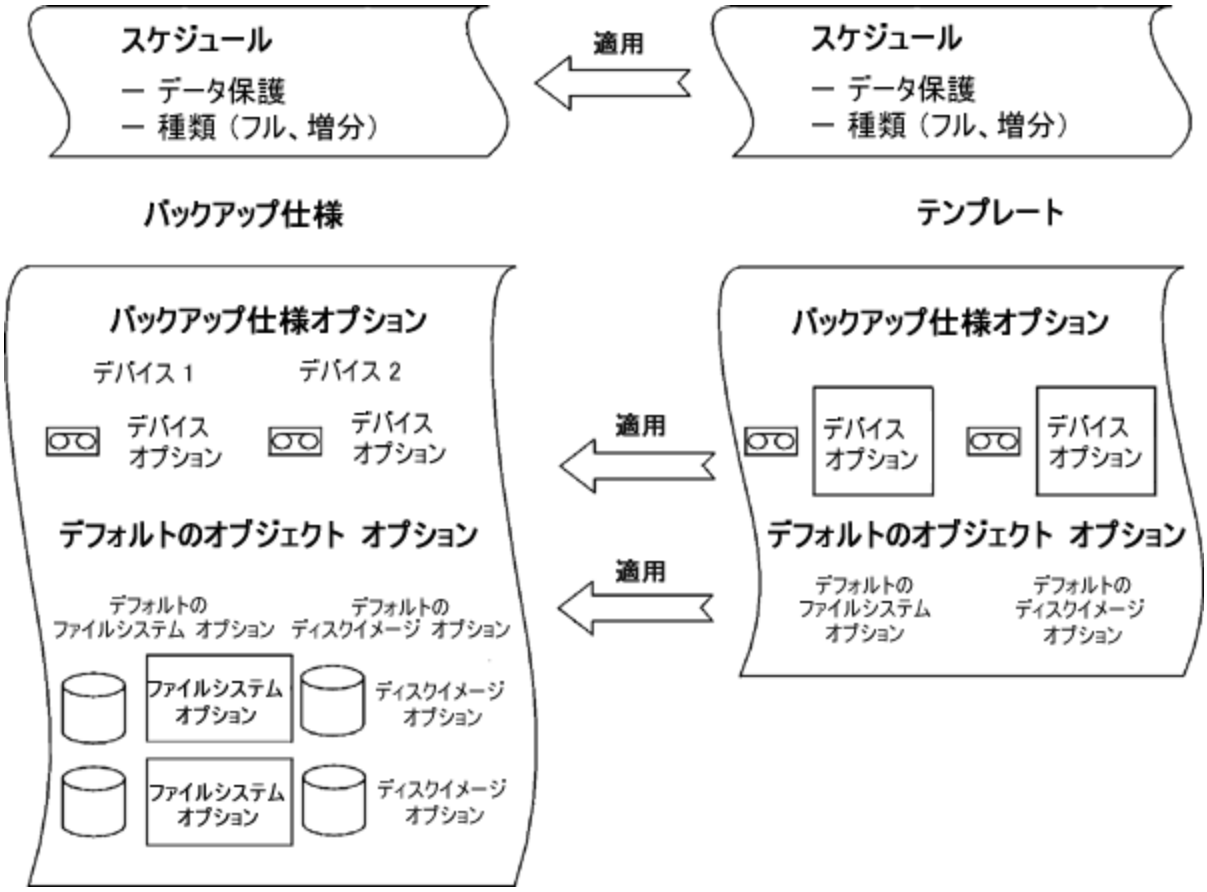
いったんテンプレートオプションを適用した後でも、バックアップ仕様を修正してどの設定も変更することができます。

バックアップオプションについて

Data Protectorには、さまざまなバックアップオプションが用意されており、バックアップを詳細に構成できます。これらのオプションは、いずれもデフォルト値(選択されている、または、選択されていない)が割り当てられています。多くの場合、デフォルト値のままバックアップを構成できます。

利用できるバックアップオプションは、バックアップの対象となるデータの種類によって異なります。たとえば、ファイルシステムバックアップとディスクイメージバックアップとでは、利用できるオプションの組み合わせが異なります。ExchangeやSQLなどの[オプション]プロパティページに用意されている共通オプションおよびアプリケーション固有オプションについては、状況依存型ヘルプで特定のバックアップの種類に関する説明を参照してください。

バックアップオプションスキーム



利用可能なバックアップオプション

データのバックアップ時に利用できるオプションには、以下の種類があります。

バックアップ仕様オプション

これらのオプションは、バックアップオブジェクトの種類に関係なく、バックアップ仕様全体に適用されます。

ファイルシステムオプション

ファイルシステムオプションは、ファイルシステムバックアップのどのオブジェクトにも適用されます。特定のオブジェクトのオプションを変更することもできます。特定のオブジェクトにオプションを設定すると、その設定がデフォルト設定の代わりに適用されます。

ディスクイメージオプション

ディスクイメージオプションは、ディスクイメージバックアップの各オブジェクトに適用されます。特定のオブジェクトのオプションを変更することもできます。特定のオブジェクトにオプションを設定すると、その設定がデフォルト設定の代わりに適用されます。

デバイスオプション

デバイスオプションは、バックアップデバイスの動作を定義します。デバイスオプションを設定しなかった場合、値はデバイス定義から読み込まれます。

スケジュール用オプション

個々のバックアップまたは定期的に実行するようスケジュールされたバックアップそれぞれについて、バックアップの種類(フルまたは増分。統合によっては他の種類も使用可能)、ネットワーク負荷、およびデータ保護を指定できます。ZDBを使用する場合は、ディスク+テープへのZDBまたはディスクへのZDBを選択できます(インスタントリカバリが有効の場合)。

スケジュールウィザードで指定したデータ保護は、バックアップ仕様の他の場所での保護設定より優先されます。

使用頻度の高いオプション

ここでは、実際のバックアップポリシーに応じて設定を変更することが特に多いオプションのリストを示します。

- データ保護
- カタログ保護
- ロギング
- 負荷調整
- 所有権

データ保護: データをメディア上に保持する期間を指定します。

データの安全性を確保し、環境を適切に管理するには、保護ポリシーの構成がきわめて重要です。会社のデータ保護ポリシーに基づいて、バックアップデータをメディア上に保持する期間を指定する必要があります。この期間(たとえば3週間)を経過したデータは、それ以降のバックアップで上書きされます。

データ保護は、数通りの方法で指定できます。対話式バックアップを実行しているか、保存済みバックアップ仕様を呼び出しているか、バックアップのスケジュールを設定しているかによって、使用できる組み合わせが異なります。デフォルト値は、[無期限]です。

対話式バックアップ

対話式バックアップの構成時は、バックアップ全体に対するデフォルトのデータ保護を変更できます。さらに、個々のバックアップオブジェクトに対して異なるデータ保護期間を指定できます。バックアップオブジェクトレベルで指定した保護は、デフォルトの保護設定よりも優先して適用されます。

保存済みのバックアップ仕様によるバックアップ

GUIを通じて保存済みバックアップを開始するときは、対話式バックアップの場合と同様にデータ保護が適用されます。

CLIを通じて保存済みバックアップを開始するときは、データ保護の指定も可能です。指定したデータ保護は、バックアップ仕様内のすべてのデータ保護設定に優先して適用されます。

スケジュールバックアップ

個々のバックアップまたは定期的に実行するようにスケジュールしたバックアップのそれぞれに対して、異なる保護期間を指定できます。スケジュールウィザードで設定したデータ保護は、バックアップ仕様内で他に定義されている保護設定よりも優先して適用されます。デフォルトの保護のままにした場合は、対話式バックアップの場合と同様にデータ保護が適用されます。

カタログ保護: データをIDBに維持する期間を指定します。

カタログ保護とデータ保護は別々に設定できます。データ保護の期間が終了しメディアが上書きされると、カタログ保護の設定に関係なくオブジェクトのカタログが削除されます。

カタログ保護は、ロギングレベルと共に、IDBの拡張性、復元対象データのブラウズの容易さ、およびバックアップパフォーマンスに大きな影響を与えます。実際の環境に適したカタログ保護ポリシーを定義することが重要です。ロギングレベルが[記録しない]に設定されている場合、カタログ保護は無視されます。

カタログ保護が無期限に設定されている場合、メディアがエクスポートまたは削除された時点でIDB内の情報が削除されます。この場合、セル内のファイル数が変わらなくても、IDBのサイズはデータ保護期限が切れるまで直線的に増加します。

デフォルト値は、**[データ保護と同じ]**です。つまり、メディアが復元に使用できる限り、ファイルやディレクトリをブラウズして選択できます。

オペレーティングシステム側の制約により、保護期限の設定は、2038年1月18日までに制限されます。

カタログ保護の期限切れ

カタログ保護期限が過ぎても、情報はすぐにIDBからは削除されません。Data Protectorは一日に一度自動的に削除作業を実行します。IDB内の情報はメディア別に編成されているので、各メディアに関する情報はメディア上のすべてのオブジェクトのカタログ保護期限が切れない限り削除されません。

カタログ保護の期限が切れた場合でも復元は可能ですが、ファイル名は手作業で指定しなければなりません。

カタログ保護とバックアップ

カタログ保護の設定は、バックアップパフォーマンスに影響を与えません。

カタログ保護と復元

カタログ保護期限が過ぎたデータは、[記録しない]オプションを使用してバックアップしたデータと同様に復元されます。

ロギング: IDBに格納するデータの詳細を変更します。

Data Protectorロギングレベルでは、バックアップ時にファイルやディレクトリについてIDBに書き込む詳細情報の量を決定します。次の4つのロギングレベルが使用できます。

- すべてログに記録
- ログファイル
- ディレクトリレベルまでログに記録
- 記録しない

HPEは同一セル内で複数のロギングレベルを使用することをお勧めします。セルは通常、毎日大量のファイルを生成するメールサーバー(または同様のサーバー)、少数のファイルにすべての情報を格納するデータベースサーバー、および数台のワークステーションで構成されています。これらのシステムはそれぞれの変動の仕方がかなり異なるため、すべてに適合する1つの設定を決定することは困難です。HPE以下に示すロギングレベル設定で複数のバックアップ仕様を作成することをお勧めします。

- 電子メールサーバーには、[ディレクトリレベルまでログに記録]オプションを使用します。
- データベースサーバーの場合は、[記録しない]オプションを使用します。この場合、個々のファイルをブラウズする意味がないためです。
- ワークステーションの場合は、[ファイルレベルまでログに記録]オプションを使用し、さまざまなバージョンのファイルを検索および復元できるようにします。
- [すべてログに記録]オプションを使用すると、変更時刻やACLなどのファイル属性を確認できます。

ロギングレベルとバックアップ速度

バックアップ速度は、どのロギングレベルを選択してもほとんど変わりません。

ロギングレベルと復元時のブラウズ

保存される情報のレベルを変更すると、復元時にData Protector GUIを使用したファイルのブラウズ機能も影響を受けます。**[記録しない]**オプションが設定されている場合は、参照できません。**[ディレクトリレベルまでログに記録]**オプションが設定されている場合は、ディレクトリの参照は可能です。**[ファイルレベルまでログに記録]**オプションが設定されている場合、全体の参照は可能ですが、ファイル属性(サイズ、作成日付、変更日付など)は表示されません。

復元するファイル名がわかっている場合は、ロギングレベルに関係なくファイル名をブラウズせずに常に手動で指定できます。

ロギングレベルと復元速度

復元速度は、対応するバックアップセッションのログレベルが、**[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]**のいずれであってもほとんど変わりません。

[記録しない]ロギングレベルを使用してバックアップセッションを実行した場合、単一ファイルを復元する場合に復元速度が減速する可能性があります。この場合は、Data Protectorがオブジェクトの先頭からすべてのデータを読み取って復元対象のファイルを見つけることが必要になるためです。

システム全体を復元する場合は、バックアップオブジェクト全体が読み取られるので、ロギングレベルは影響しません。

負荷調整: バックアップデバイスの使用率を調整します。

[負荷調整]オプションは、多数のオブジェクトを使用可能な多数のデバイスにバックアップして、常にすべてのデバイスを使用中にしておきたい場合に使用します。Data Protector使用不可能なデバイスによるバックアップへの影響を最小限に抑えるには、このオプションを使用してください。

少数のオブジェクトをバックアップする場合、オブジェクトを単純なデバイス(DDSなど)にバックアップする場合、オブジェクトのバックアップ先のデバイスを手動で選択する場合、またはどのメディアにオブジェクトがバックアップされるかを知りたい場合は、[負荷調整]オプションをオフにします。オブジェクトは、負荷調整バックアップ仕様で指定されたデバイスのリストから利用可能なデバイスに割り当てられます。

リストの先頭にあるデバイスが最初に起動されます。各デバイスに割り当てられるオブジェクトの数は、そのデバイスの同時処理数によって決まります。リスト内のオブジェクトがなくなるか、または稼動可能なデバイスの最大数に達するまで、2番目以降のデバイスが起動され、オブジェクトが割り当てられます。

デバイスが利用不能になった場合は、その時点でデバイスに割り当てられていたオブジェクトについてのみ、バックアップが中止されます。失敗時以前にデバイスにバックアップされたすべてのオブジェクトは、実際にバックアップされています。バックアップ仕様に他のデバイスが指定されていれば、デバイスの最大数に達していない限り、新しいデバイスが起動されます。デバイスは以下の理由で使用不可になります。

- バックアップ中に失敗する。
- バックアップ中に停止する。
- 別のセッションが使用中である。
- 開始できない。

バックアップ対象のオブジェクトは、以下の条件に基づいて選択されます。

- バックアップデバイスに接続されているクライアント上に存在するオブジェクトは、他のオブジェクトよりも優先して選択されます。
- オブジェクトは、クライアントあたりのDisk Agent数ができるだけ少なくなるように選択されます。
- オブジェクトをデバイスに割り当てるときに、オブジェクトのサイズは考慮されません。

テンプレートからデバイスオプションを適用する場合は、次の点に注意してください。

- テンプレート内で[負荷調整]オプションを選択していない場合、デバイスにバックアップ仕様が適用されません。
- テンプレートとバックアップ仕様の両方で[負荷調整]オプションが選択されていれば、デバイスオプションが適用されます。
- テンプレートでのみ[負荷調整]オプションが選択されている場合は、バックアップ仕様にデバイスがないときにのみデバイスオプションが適用されます。

所有権:どのアカウントが復元を実行できるかを指定します。

バックアップセッションオーナーとは

各[バックアップセッション]およびその内部にバックアップされたすべてのデータには、オーナーが割り当てられます。このオーナーは、対話型のバックアップを開始するユーザー、CRSプロセスを実行しているアカウント、またはバックアップ仕様オプションでオーナーとして指定されるユーザーです。

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。

- ユーザーが[セッションの所有権を切り替え]のユーザー権限を持っています。
- 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。

UNIX Cell Manager上でスケジュール設定したバックアップの場合は、上記の条件に当てはまらない限り、root:sysがセッション オーナーになります。

Windows Cell Manager上でスケジュール設定したバックアップの場合は、上記の条件に当てはまらない限り、インストール中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。

なぜバックアップオーナーを変更するか

管理者がバックアップ仕様を構成およびスケジュール設定している場合、オペレーターにバックアップ仕様の実行を許可しても、オペレーターがバックアップ仕様を修正したり保存したりすることはできません。[プライベート]バックアップオプションをすべてのオブジェクトに対して設定すると、オペレーターはどのデータも復元できませんが、バックアップを管理したり、失敗したセッションを再開したりすることはできます。

バックアップ構成を変更した後、保存しなければ、対話式バックアップとみなされるのでオーナーは変更されません。フルバックアップのオーナーではないユーザーが増分バックアップを対話型で起動すると、増分バックアップではなく別のフルバックアップが作成されることになります。

誰がプライベートオブジェクトを復元できるか

オブジェクトが[パブリック]とマークされている場合を除き、次のユーザーのみがオブジェクトを復元できます。

- Adminユーザーグループおよび Operatorユーザーグループのメンバー。
- [復元の開始]ユーザー権限を持っているバックアップセッションオーナー。その他の[ユーザー権限]([別のクライアントへ復元]など)も必要になる場合があります。
- [プライベートオブジェクトを表示]ユーザー権限を持つユーザー。

プライベートオブジェクトを表示および復元する権限は、adminまたはoperator以外のグループにも付与できます。

バックアップ仕様オプション

これらのオプションは、バックアップオブジェクトの種類に関係なく、バックアップ仕様全体に適用されます。

基本となるオプションは**[負荷調整]**です。デフォルトで、このオプションは[バックアップの新規作成]ダイアログボックスで有効になっています。このページでオプションを無効にしても、後でバックアップ仕様の[あて先]プロパティページの[バックアップ]タブで選択できます。

バックアップ仕様オプションの詳細については、『HPE Data Protectorヘルプ』を参照してください。

一般的なバックアップ仕様オプション

- 説明
- 実行対象クライアント
- 実行後
- 実行前
- 切断された接続の再接続
- 所有権

クラスター化に関するバックアップ仕様オプション

セッションの自動再起動

クラスター対応Data Protectorのフェイルオーバーがバックアップ中に発生した場合、実行中および保留中のバックアップセッションがすべて失敗します。フェイルオーバー発生後のData Protectorの動作は、以下のオプションで定義できます。

- フェイルオーバー時にバックアップを再開しない
- すべてのオブジェクトのバックアップを再開
- 失敗したオブジェクトのバックアップを再開

セッションパラメーターの破棄とIDパラメーターの破棄

Data Protector以外のクラスター対応アプリケーションがData Protectorとは異なるノード上で稼働しており、それがData Protectorが稼働しているノードにフェイルオーバーした場合、このシステムへの負荷を制御できます。このようなフェイルオーバーが発生した後のData Protectorの動作を定義するには、以下のオプションを`omniclus`コマンドと組み合わせて使用します。

- セッションの経過時間をチェックしない
- ～未満の場合は中止
- ～以上の場合は中止
- 破棄IDをチェックしない
- 破棄IDをチェックする

EMC Symmetrixに関するバックアップ仕様オプション

クライアントシステム

- アプリケーションシステム
- バックアップシステム

ミラーの種類

- TimeFinder
- Symmetrix Remote Data Facility
- 組み合わせ([SRDF] + [TimeFinder])

EMC Symmetrixでの実行前と実行後の分割

- 分割実行前コマンド
- 分割実行後コマンド

EMC Symmetrixオプション

- Symmetrix環境の検出を実行
- バックアップ前にリンクを再確立
- バックアップ後にリンクを再確立

HPE P9000 XPディスクアレイファミリバックアップ仕様オプション

クライアントシステム

このオプションのセットは、バックアップ仕様が保存された後でなければ修正できません。

- アプリケーションシステム
- バックアップシステム

ミラーの種類

- HPE Business Copy P9000 XP
- HPE Continuous Access P9000 XP
- 組み合わせ(HPE Continuous Access P9000 XP + HPE Business Copy P9000 XP)
- MU番号

複製管理オプション

- バックアップ後に複製を保持
- 複製をインスタントリカバリに使用する

セッションの開始時

- ディスクが同期されていない場合はディスクを同期する
- ミラーディスクが同期されていない場合はセッションを中止する

セッションの終了時

- バックアップに備えて次のミラーディスクを準備(再同期)する

アプリケーションシステムオプション

- アプリケーションシステム上のファイルシステムをアンマウントする
- アプリケーションコマンドラインの停止/休止
- アプリケーションコマンドラインの再開

バックアップシステムオプション

- アプリケーションシステムと同じマウントポイントを使用
- バックアップシステムのマウントパスのルート
- ディレクトリをマウントパスに追加
- ファイルシステムを目的のマウントポイントで自動的にアンマウントする
- バックアップシステムを使用可能にしておく
- バックアップシステムを読み書き可能モードにしておく

HPE P6000 EVAディスクアレイファミリバックアップ仕様オプション

クライアントシステム

- アプリケーションシステム
- バックアップシステム

複製モード

- HPE Business Copy P6000 EVA
- HPE Continuous Access P6000 EVA + HPE Business Copy P6000 EVA

フェイルオーバーシナリオにおける複製処理

- 複製の方向に従う
- 複製場所を維持

スナップショット管理オプション

- スナップショットソース
- スナップショットの種類
- 冗長レベル
- スナップクローンが完全に作成されない場合、テープバックアップを最大n分間遅らせる

ミラークローンの準備/同期

- セッションの開始時
- セッションの終了時

複製管理オプション

- バックアップ後に複製を保持
- ローテーションされる複製数
- 複製をインスタントリカバリに使用する

アプリケーションシステムオプション

- 複製生成前にアプリケーションシステム上のファイルシステムをアンマウント
- アプリケーションコマンドラインの停止/休止
- アプリケーションコマンドラインの再開

バックアップシステムオプション

- アプリケーションシステムと同じマウントポイントを使用
- バックアップシステムのマウントパスのルート
- ディレクトリをマウントパスに追加
- ファイルシステムを目的のマウントポイントで自動的にアンマウントする
- バックアップシステムを使用可能にしておく
- バックアップシステムを読み書き可能モードにしておく

ファイルシステムオプション

ファイルシステムオプションは、ファイルシステムバックアップのどのオブジェクトにも適用されます。

基本となるオプションは[保護]です。

いくつかのカテゴリの**拡張**ファイルシステムオプションが用意されています。

- ファイルシステムオプション
- その他のファイルシステムオプション
- WinFSファイルシステムオプション

ファイルシステムオプションの詳細については、『HPE Data Protectorヘルプ』を参照してください。

ファイルシステムオプション

- カタログ保護
- 実行後
- 実行前
- パブリック
- レポートレベル

その他のファイルシステムオプション

- バックアップファイルのサイズ
- POSIXハードリンクをファイルとしてバックアップ
- POSIXハードリンクをファイルとしてバックアップ
- ディザスタリカバリイメージ全体をディスクにコピー
- **データセキュリティ**
  - なし
  - AES 256ビット
  - 暗号化
- 統計情報の表示
- アクセス時刻属性を保存しない
- 拡張増分バックアップ
- 可能な場合は、標準で用意されているファイルシステムのChange Log Providerを使用
- バックアップ時にファイルをロック
- ロギング

  Data Protectorロギングレベルでは、バックアップ時にファイルやディレクトリについて内部データベースに書き込む詳細情報の量を決定します。次の4つのロギングレベルが使用できます。
  - すべてログに記録
  - ログファイル
  - ディレクトリレベルまでログに記録
  - 記録しない
- ソフトウェア圧縮

WinFSファイルシステムオプション

- 非同期の読み込み
- ディレクトリ共有情報のバックアップ
- NTFSハードリンクを検出
- アーカイブ属性を使用しない
- **開いているファイル**
  - 再試行回数
  - タイムアウト
- ロックされたファイルを別名で開いたことを通知

- **MSボリュームシャドウコピーのオプション**
  - シャドウコピーを使用
  - フォールバックを許可

ディスクイメージオプション

これらのオプションは、バックアップ対象として選択したすべてのディスクイメージオブジェクトに適用されます。

基本となるオプションは[保護]です。

ディスクイメージオプションの詳細については、『HPE Data Protectorヘルプ』を参照してください。

以下の**拡張**ディスクイメージオプションを設定できます。

- カタログ保護
- **データセキュリティ**
  - なし
  - AES 256ビット
  - 暗号化
- 統計情報の表示
- 実行後
- 実行前
- パブリック
- レポートレベル
- ソフトウェア圧縮

デバイスオプション

これらのオプションは、特定のバックアップ仕様に現在選択されているバックアップデバイスに対して設定できます。これらのオプションは、バックアップデバイスの構成時やバックアップデバイスプロパティの変更時に設定するオプションのサブセットで、特定のバックアップ仕様に対してのみ適用されます。これらのオプションは、[デバイス/メディア]コンテキストのオプションより優先して適用されます。[デバイス/メディア]コンテキストのオプションは、各デバイスに汎用的に適用されるオプションです。

デバイスオプションの詳細については、『HPE Data Protectorヘルプ』を参照してください。

デバイスのプロパティ - 一般

- CRCチェック
- 同時処理数
- ドライブベースの暗号化
- メディアプール

- 事前割り当てリスト
- 再スキャン

スケジュール用オプション

バックアップのスケジュール設定時には、付加的なオプションを設定できます。スケジュールされたバックアップそれぞれについて、バックアップの種類(フルまたは増分、統合によってはその他のバックアップの種類が使用できます)、データ保護、優先順位、ネットワーク負荷、再帰パターン、および推定時間を指定できます。ZDBを使用する場合は、ディスク+テープへのZDBまたはディスクへのZDBを選択できます(インスタントリカバリが有効の場合)。

スケジューラーで指定したデータ保護は、バックアップ仕様の他の場所での保護設定より優先されます。

スケジュールウィザードを使用して、Data Protectorでスケジュールを作成および編集する方法の詳細については、「*スケジューラー、ページ 103*」を参照してください。

セッションオプション

- **バックアップの種類**
  - フル
  - 増分
- バックアップ保護
- 優先順位
- ネットワーク負荷
- 繰り返しパターン
- 推定時間

スプリットミラー/スナップショットのバックアップ

(ZDBで使用できます。ただし、ディスク+テープへのZDBまたはディスクへのZDB(インスタントリカバリが有効化されている)の場合のみ)

バックアップオプションの設定

バックアップオプションは、新しいバックアップ仕様の作成中に設定できます。その場合は、ウィザードに表示される[オプション]プロパティページを使います。

構成を完了した保存済みバックアップ仕様に対してバックアップオプションを設定することもできます。

> **注:**
> オブジェクトオプション(ファイルシステムオプションとディスクイメージオプション)は2つのレベルで設定できます。まず、*デフォルトのオブジェクトオプション*を、すべてのファイルシステムやすべてのディスクイメージオブジェクトに対して、バックアップ仕様の中で個別に設定できます。次に、*個々のオブジェクト*に対して個別に設定できます。個別の設定は、デフォルトの設定よりも優先して適用されま

> す。たとえば、低速のCPUのクライアントを除く全クライアントのデータを圧縮するには、ファイルシステムオプションの設定中に**[圧縮]**オプションを有効にします。次に、低速のクライアントを選択し、このクライアントの**[圧縮]**オプションをオフにします。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. バックアップオプションを設定するバックアップ仕様をダブルクリックして、**[オプション]**タブをクリックします。
4. [オプション]ページでオプションを適切に設定します。設定したいオプションのタイプに応じて、**[拡張]**のボタンのいずれかをクリックして、拡張オプションを設定します。

   バックアップ仕様オプションに加えて、たとえばファイルシステムオプションやディスクイメージオプションなどを、構成するバックアップ仕様のデータの種類に応じて設定できます。
5. 必要なオプションを探し、オン/オフを切り替えるか、または適切な情報を入力します。
6. **[OK]**をクリックし、**[適用]**をクリックして、変更内容を保存します。

データ保護を指定する

データ保護は、対話式バックアップの実行時、保存済みのバックアップ仕様の開始時、またはバックアップのスケジュール時に指定できます。デフォルト値は、[無期限]です。

> **注:**
> オペレーティングシステム側の制約により、保護期限の設定は、2038年1月18日までに制限されます。

バックアップ仕様レベルでデータ保護を指定する

データ保護を、新しいバックアップ仕様の作成時、または既存のバックアップ仕様の修正時に指定できます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. バックアップオプションを設定するバックアップ仕様をダブルクリックして、**[オプション]**タブをクリックします。
4. ファイルシステムをバックアップする場合、[ファイルシステムオプション]の下の[保護]オプションを指定します。統合ソフトウェアの場合、[共通アプリケーションオプション]の下の**[拡張]**をクリックし、[オプション]タブの**[保護]**オプションを指定します。
5. **[OK]**をクリックし、**[適用]**をクリックして、変更内容を保存します。

個々のバックアップオブジェクトに対してデータ保護を指定する

ファイルシステムオブジェクトおよびディスクイメージオブジェクトのそれぞれに対して異なる保護期間を指定できます。

個々のオブジェクトに対するデータ保護は、新しいバックアップ仕様の作成時、または既存のバックアップ仕様の変更時に指定できます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. バックアップオプションを設定するバックアップ仕様をダブルクリックして、**[バックアップオブジェクトのサマリー]**タブをクリックします。
4. オブジェクトを右クリックし、**[プロパティ]**をクリックします。
5. **[オプション]**タブをクリックし、[保護]オプションを指定します。
6. **[OK]**をクリックし、**[適用]**をクリックして、変更内容を保存します。

スケジュールバックアップに対してデータ保護を指定する

個々のバックアップまたは定期的に実行するようにスケジュールしたバックアップのそれぞれに対して、異なる保護期間を指定できます。スケジュールウィザードで設定したデータ保護は、バックアップ仕様内で他に定義されている保護設定よりも優先して適用されます。

スケジュールバックアップのデータ保護は、バックアップのスケジュール設定中に指定できます。

CLIを通じてデータ保護を指定する

CLIを通じてバックアップを実行するときは、データ保護の指定も可能です。指定したデータ保護は、バックアップ仕様内のすべてのデータ保護設定に優先して適用されます。

手順

1. 次のコマンドを実行します。

   ```
   omnib -datalist Name -protect ProtectionPeriod
   ```

   ここで、*Name*はバックアップ仕様の名前です。

   たとえば、2週間の保護期間を設定してバックアップを実行するには、次のように入力します。

   ```
   omnib -datalist MyBackup -protect weeks 2
   ```

   詳細については、omnibのmanページまたは『*HPE Data Protector Command Line Interface Reference*』を参照してください。

特定のオブジェクトのオプションを変更する

オプションは、特定のオブジェクトだけに適用することもできます。また、デフォルトのオプションを変更することもできます。

新しいバックアップ仕様を作成するときにこれらのオプションを適用できます。これらのオプションの適用には、ウィザードに表示される[バックアップオブジェクトのサマリー]ページを使います。

これらのオプションは、構成を完了した保存済みバックアップ仕様に対して適用することもできます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. オプションを特定のオブジェクトに適用するバックアップ仕様をダブルクリックして、**[バックアップオブジェクトのサマリー]**タブをクリックします。
4. [バックアップオブジェクトのサマリー]ページでは、オブジェクトのプロパティ、オブジェクトの順序、またはミラーオプションを変更できます。

   オブジェクトプロパティを変更するには:

   a. オブジェクトを右クリックし、**[プロパティ]**をクリックします。
   b. 特定のオブジェクトのオプションを変更するには、[オブジェクトのプロパティ]ダイアログボックスを使用します。このダイアログボックスには、**[一般]**、**[オプション]**、**[その他]**、**[ツリー/フィルター]**、**[WinFSオプション]**、**[オプション]**、**[データベース]**の各タブのうち、選択したオブジェクトに応じたタブが表示されます。適切なタブをクリックしてオプションを変更できます。
   c. **[OK]**をクリックして変更内容を適用します。

   オブジェクトの順序を変更するには:

   a. オブジェクトを右クリックし、**[上へ移動]**または**[下へ移動]**をクリックします。目的の順序になるまでこの手順を繰り返します。
   b. **[適用]**をクリックします。

   ミラーオプションを変更するには:

   a. オブジェクトを選択し、**[ミラーの変更]**をクリックします。
   b. ミラーのデバイスを変更するには、ミラーが選択されていることを確認し、ミラーを強調表示し、デバイスを**[デバイス]**ドロップダウンリストから選択します。選択したバックアップオブジェクトのミラーの選択を解除することもできます。

バックアップデバイスオプションを変更する

新しいバックアップ仕様の作成時に、バックアップデバイスオプションおよびデバイスの順番を設定できます。これらの設定には、ウィザードに表示される[あて先]プロパティページを使います。

構成を完了した保存済みバックアップ仕様に対してバックアップデバイスオプションを設定することもできます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. デバイスオプションを変更するバックアップ仕様をダブルクリックして、**[あて先]**タブをクリックします。
4. [あて先]プロパティページでは、デバイスオプションを変更できます。
   - 負荷調整が行われているバックアップのデバイスを変更するには、デバイスの選択を解除し、別のデバイスを選択します。
   - 負荷調整されていないバックアップ用のデバイスを変更するには、使用するすべてのデバイスを選択します。**[バックアップオブジェクトのサマリー]**タブをクリックし、目的のオブジェクトをクリックし、**[デバイスの変更]**をクリックします。
   - ミラーリングされているオブジェクト用のデバイスを変更するには、特定のミラーに使用するすべてのデバイスを選択します。**[バックアップオブジェクトのサマリー]**タブをクリックし、目的のオブジェクトをクリックし、**[ミラーの変更]**をクリックします。
   - デバイスの順序を変更するには([負荷調整]オプションを指定していないバックアップの場合)、任意のデバイスを選択して右クリックし、**[デバイスの並べ替え]**をクリックします。
   - その他のデバイスプロパティを設定するには、任意のデバイスを選択して右クリックし、**[プロパティ]**をクリックします。
5. 適切なオプションを指定し、**[OK]**をクリックします。
6. **[適用]**をクリックします。

スケジュールバックアップオプションを設定する

バックアップのスケジュール設定時には、付加的なオプションを設定できます。これらのオプションはスケジュールバックアップについてのみ有効で、対話的に開始されたバックアップに対しては無効です。スケジュールウィザードで指定したデータ保護は、バックアップ仕様の他の場所での保護設定より優先されます。

スケジュールバックアップオプションは、スケジュールバックアップに使用する新しいバックアップ仕様の作成中に設定できます。バックアップウィザードで**[保存とスケジュール]**オプションを選択して、バックアップのスケジュールを設定します。

構成を完了した保存済みバックアップ仕様でバックアップのスケジュールを設定するときにも、スケジュールバックアップオプションを設定できます。Data Protectorでスケジュールを作成および編集する方法の詳細については、「*スケジューラー、ページ 103*」を参照してください。

実行前/実行後コマンドについて

実行前/実行後コマンドとは

実行前/実行後コマンドは、バックアップまたは復元の前後に付加的な処理を実行するために使用される実行可能ファイルまたはスクリプトです。こうした処理には、バックアップ対象のファイル数のチェック、実行中の一部のトランザクションの停止、バックアップ前のアプリケーションのシャットダウンとそれに続く再起動などが含まれます。実行前/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。目的の処理を実行するスクリプトをユーザーが独自に作成する必要があります。これらのコマンドには、Windowsシステム上で動作する実行可能ファイルやバッチファイル、またはUNIXシステム上で動作するシェルスクリプトを使用できます。バッチファイル内から実行されるコマンドは、常に、成功を示す終了コード`0`か、または失敗を示す1以上を返す必要があります。`0`

バックアップオブジェクトの種類が`Client System`の場合(ホストバックアップ)、特別な動作があります。実行前コマンドおよび実行後コマンドを1回しか指定していなくても、ファイルシステム(または論理ドライブ)ごとにコマンドが起動されます。

バックアップ用の実行前/実行後コマンドの構成

実行前/実行後コマンドは、以下の2つのレベルで構成できます。

バックアップ仕様

実行前コマンドはバックアップセッションが開始される前に実行されます。実行後コマンドはバックアップセッションが停止してから実行されます。これらのコマンドは、バックアップ仕様全体に対するバックアップオプションとして指定します。デフォルトでは、バックアップセッションの実行前および実行後コマンドはCell Managerで実行されますが、別のシステムも選択できます。

バックアップオブジェクト

バックアップオブジェクトに対する実行前コマンドは、オブジェクトのバックアップ前に開始されます。同様に、特定のバックアップオブジェクトを対象とする実行後コマンドは、そのオブジェクトをバックアップした後に実行されます。これらのコマンドは、オブジェクトに適用するバックアップオプションとして指定します。オブジェクトに対する実行前および実行後コマンドは、オブジェクトをバックアップするDisk Agentが実行されているシステム上で実行されます。

実行前/実行後コマンドの実行方法

1. バックアップ仕様全体の実行前コマンドが開始し、終了します。
2. バックアップ仕様の各オブジェクトについて、次の処理が実行されます。
   a. 実行前コマンドが開始し、終了します。
   b. オブジェクトがバックアップされます。
   c. (バックアップ仕様に含まれている各オブジェクトについて)実行後コマンドが開始し、終了します。
3. バックアップ仕様全体の実行後コマンドが開始し、終了します。

バックアップ仕様を対象とする実行前/実行後コマンド

実行前/実行後コマンドは、Windowsシステム上では実行可能ファイルやバッチファイル、UNIXシステム上ではシェルスクリプトとして記述できます。バッチファイル内から実行されるコマンドは、常に、成功を示す終了コード(0)か、または失敗を示す終了コード(0を超える値)を返す必要があります。

実行前/実行後コマンドの特徴

- セキュリティを確保するためのコマンドの起動と場所
- 環境変数
- SMEXIT値
- 実行前/実行後コマンドに関する留意事項

セキュリティを確保するためのコマンドの起動と場所

バックアップセッション用の実行前および実行後コマンドは、それぞれバックアップセッションの前および後に起動します。これらはデフォルトではCell Manager上で実行されますが、別のシステムも選択できます。

Windowsシステム

実行前および実行後スクリプトは、Cell Manager上で実行された場合はData Protector CRSによって起動されます。リモート実行された場合は、Data Protector Inet Serviceアカウント(デフォルトではローカルシステムアカウント)で実行されます。

Cell Managerおよび他のシステム上のスクリプトは、`Data_Protector_ home\bin`ディレクトリに置かれている必要があり、ユーザーはファイル名のみまたは相対パス名を指定する必要があります。

実行前コマンドおよび実行後コマンドでサポートしている拡張子は、`.bat`、`.exe`、および`.cmd`のみです。サポートされていない拡張子(`.vbs`など)を使用したスクリプトを実行するには、そのスクリプトを起動するバッチファイルを作成します。そして、そのバッチファイルを実行前コマンドまたは実行後コマンドとして実行するようにData Protectorを構成します。これにより、サポートされていない拡張子のスクリプトが起動されます。

パス名を指定するのに引用符("")を使用する場合、円記号と引用符(\")を組み合わせて使用しないでください。パス名の末尾に円記号を入力するには、二重の円記号として入力してください(\\)。

> **注:**
> perl.exeを直接使用することはできません。

UNIXシステム

実行前スクリプトと実行後スクリプトは、バックアップセッションオーナーのアカウントで実行されます。ただし、例外として、バックアップセッションオーナーに`Backup as root`パーミッションが付与されている場合は、`root`で実行されます。

Cell ManagerまたはリモートUNIXクライアント上では、バックアップ仕様の実行コマンドを以下のディレクトリに置く必要があります。

HP-UXシステム、Solarisシステム、Linuxシステムの場合: **HP-UX, Solaris, and Linux systems:** `/opt/omni/lbin`

その他のUNIXシステムの場合: **Other UNIX systems:** `/usr/omni/bin`

コマンドを`/opt/omni/lbin`または`/usr/omni/bin`ディレクトリに置いた場合は、ファイル名だけを指定します。他のディレクトリに置いた場合は、フルパス名を指定する必要があります。

環境変数

以下の環境変数は、Data Protectorによって設定され、Cell Manager上のバックアップ仕様用の実行前および実行後スクリプトでのみ使用できます。ただし、Cell Manager以外のシステムでコマンドが実行される場合は使用できません。

環境変数の詳細については、『HPE Data Protectorヘルプ』を参照してください。

- DATALIST
- MODE
- OWNER
- PREVIEW
- RESTARTED
- SESSIONID
- SESSIONKEY
- SMEXIT

SMEXIT値

値	説明
0	すべてのファイルが正常にバックアップされました。
10	すべてのエージェントが正常に終了されましたが、一部のファイルがバックアップされませんでした。
11	障害の発生したエージェントがあるか、データベースエラーがあります。
12	操作を完了したエージェントがありません。セッションはData Protectorによって中止されました。
13	セッションはユーザーによって中止されました。

実行前/実行後コマンドに関する留意事項

- Windowsシステムの場合は、拡張子(`.exe`、`.bat`など)を含めた完全なファイル名を指定する必要があります。
- スクリプト名を指定する際、パスにスペース文字が含まれているために単一引用符(UNIXシステムの場合)または二重引用符(Windowsシステムの場合)を使用する必要が生じた場合は、両方を混在させないようにしてください。単一引用符と二重引用符のどちらかのみを使用してください。たとえば、

"S'ilvousplat.bat"は使用できません。S'ilvousplat.batは使用できます。

- 正常に終了した場合、実行前または実行後コマンドの終了値はゼロになります。
- 実行前コマンドが失敗した(0未満の値が返された)場合は、バックアップセッションステータスがFailedに設定され、セッションが中止されます。実行後コマンドは実行されません。
- 実行後コマンドが失敗した(0未満の値が返された)場合は、バックアップセッションステータスがCompleted with errorsに設定されます。
- 実行後コマンドが0未満の値を返し、omnibコマンドが11を返した場合は、バックアップステータスがCompleted with failuresに設定されます。
- セッションが中止された場合や、実行前コマンドが実行されていないか、または設定されていない場合を除いて、実行後コマンドは常に実行されます。omnircのOB2FORCEPOSTEXECオプションが設定されている場合、実行後コマンドは常に実行されます。
- デフォルトでは、実行前/実行後コマンドはバックアップのプレビュー中には実行されません。この動作は、グローバルオプションファイルのExecScriptOnPreviewオプションによって定義されます。
- 実行前/実行後コマンドは、コマンドプロンプトで入力したコマンドと同様に処理されます。ただし、?、*、"、|、<、および>といった特殊文字は使用できません。
- 実行前/実行後コマンドはパイプメカニズムを使って実行します。実行前または実行後に関数内で起動されたすべてのプロセスは、次のプロセスに移行する前に終了する必要があります。
- 実行前または実行後コマンド実行中にバックアップセッションを中止することはできません。
- 実行前/実行後コマンドはバックグラウンドモードで実行します。このため、ユーザーインターフェイスを必要とするコマンドは使用しません。
- タイムアウトが設定されており、実行前および実行後スクリプトは、デフォルトで少なくとも15分に1度出力を送信する必要があります。そうでない場合は、スクリプトが中止されます。この時間間隔はScriptOutputTimeoutグローバルオプションを編集することで変更できます。
- 実行前/実行後コマンドの結果はすべてIDBに書き込まれ、Data Protector GUIに表示されます。
- UNIXシステムでは、新しいプロセスを開始する前に、実行前または実行後スクリプトがすべてのファイル記述子を閉じなかったことにより、スクリプトが応答を停止することがあります。新しいプロセスがバックグラウンドで実行され、終了されないと(たとえばデータベースサーバープロセス(dbstart))、スクリプトが応答を停止します。

  detachコマンドを使用できます。detachコマンドのソースはdetach.cファイルに記述されていますが、サポートはされていません。例: /opt/omni/bin/utilns/detach pre_script [arguments...]
- Cell Managerでのセッションの実行前/実行後コマンドの実行を無効にする場合は、SmDisableScriptグローバルオプションを1に設定します。
- リモートセッションの任意のクライアントの実行前/実行後コマンドを無効にする場合は、OB2REXECOFF=1という行をomnircのファイルに追加します。
- クライアントを保護するには、そのクライアントにアクセスが許可されているCell Managerを指定します。許可されたCell Managerのみが、そのクライアントの実行前/実行後コマンドを実行することができます。
- UNIXシステムでは、コマンドによってstdoutに書き込まれたテキストは、セッションマネージャーに送られてデータベースに書き込まれます。stderrは/dev/nullにリダイレクトされます。それをstdoutにリダイレクトすることで、エラーメッセージをデータベースに記録できます。

バックアップ仕様を対象とする実行前/実行後コマンドを指定する

保存済みバックアップ仕様を対象とする実行前コマンドおよび実行後コマンドを指定するには、以下の手順に従ってください。

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 実行前コマンドおよび実行後コマンドを指定するバックアップ仕様をダブルクリックし、**[オプション]**タブをクリックします。
4. [バックアップ仕様オプション]で、**[拡張]**をクリックします。
5. [バックアップオプション]ダイアログボックスの[一般]タブで、**[実行前]**テキストボックスと**[実行後]**テキストボックスの一方または両方にファイル名またはパス名を入力します。
6. **[OK]**をクリックし、**[適用]**をクリックして、変更内容を保存します。

特定のバックアップオブジェクトを対象とする実行前/実行後コマンド

実行前/実行後コマンドは、Windowsシステム上では実行可能ファイルやバッチファイル、UNIXシステム上ではシェルスクリプトとして記述できます。バッチファイル内から実行されるコマンドは、常に、成功を示す終了コード`0`か、または失敗を示す1以上を返す必要があります。

コマンドの起動と場所

オブジェクト用の実行前および実行後コマンドは、それぞれオブジェクトのバックアップの前および後に実行されます。これらのコマンドは、バックアップ仕様に含まれるすべてのオブジェクトを対象として指定することも、個々のオブジェクトに対して個別に指定することもできます。Oracleなどの統合ソフトウェアをバックアップするときは、データベースが1つのオブジェクトとして扱われるので、データベースバックアップの前後にコマンドが実行されます。これらのコマンドは、Disk Agentが実行されているシステム上で実行されます。

Windowsシステムの場合:	バックアップオブジェクトの実行前スクリプトおよび実行後スクリプトは、Data Protector Inet Serviceアカウント(デフォルトではローカルシステムアカウント)で実行されます。 バックアップオブジェクトの実行スクリプトは、Disk Agentが稼動しているシステムの任意のディレクトリに置くことができます。ただし、クライアントバックアップの場合は、*`Data_Protector_home`*`\bin`に存在している必要があります。*`Data_Protector_home`*`\bin`ディレクトリ内にスクリプトを置いた場合は、ファイル名だけを指定します。他のディレクトリに置いた場合は、フルパス名を指定する必要があります。 実行前コマンドおよび実行後コマンドでサポートしている拡張子は、`.bat`、`.exe`、および`.cmd`のみです。サポートされていない拡張子(`.vbs`など)を使用したスクリプトを実行するには、そのスクリプトを起動するバッチファイルを作成します。そして、

	そのバッチファイルを実行前コマンドまたは実行後コマンドとして実行するようにData Protectorを構成します。これにより、サポートされていない拡張子のスクリプトが起動されます。 パス名を指定するのに引用符("")を使用する場合、円記号と引用符(\")を組み合わせて使用しないでください。パス名の末尾に円記号を入力するには、二重の円記号として入力してください(\\)。
UNIXシステムの場合:	実行前スクリプトと実行後スクリプトは、バックアップセッションオーナーのアカウントで実行されます。ただし、例外として、バックアップセッションオーナーに`Backup as root`パーミッションが付与されている場合は、rootで実行されます。 バックアップオブジェクトの実行コマンドは、Disk Agentが稼動しているシステムの任意のディレクトリに置くことができます。ただし、クライアントバックアップの場合、コマンドはデフォルトのData Protector管理コマンドディレクトリに存在する必要があります。デフォルトの管理コマンドディレクトリ内にコマンドを置いた場合は、ファイル名だけを指定します。他のディレクトリに置いた場合は、フルパス名を指定する必要があります。

環境変数

実行後コマンドに対して、Data ProtectorはBDACC環境変数を設定します。

実行前/実行後コマンドに関する留意事項

- クライアントシステム(ホスト)バックアップを実行する場合、実行後スクリプトはバックアップ終了後に開始されますが、実行前スクリプトは特定のシステムの最初のファイルシステムをバックアップする前に開始されます。この場合、BDACC`BDACC`変数はクライアントシステム(ホスト)全体ではなく、1つのファイルシステムオブジェクトに関連付けられているため、エクスポートできません。
- Windowsシステムの場合は、拡張子(`.exe`、`.bat`など)を含めた完全なファイル名を指定する必要があります。
- スクリプト名を指定する際、パスにスペース文字が含まれているために単一引用符(UNIXシステムの場合)または二重引用符(Windowsシステムの場合)を使用する必要が生じた場合は、両方を混在させないようにしてください。単一引用符と二重引用符のどちらかのみを使用してください。たとえば、"S'ilvousplat.bat"は使用できません。S'ilvousplat.batは使用できます。
- 正常に終了した場合、実行前または実行後コマンドの終了値はゼロになります。
- 実行前コマンドが失敗した(ゼロでない値が返された)場合は、このオブジェクトのバックアップが中止されます。オブジェクトステータスが`Aborted`に設定され、Disk Agentが処理を停止します。ただし、実行後コマンドが`BDACC`環境変数に依存していない限り、実行後コマンドは実行されます。この場合、すべてのオブジェクトがバックアップされません。
- 実行後コマンドが失敗した(ゼロでない値が返された)場合は、オブジェクトステータスが中止`Aborted`に設定されます。この場合、オブジェクトはバックアップされており、データを復元できます。
- クライアントに実行スクリプトが存在しないか、スクリプトのパスが間違っている場合、スクリプトが失敗したためセッションを中止するというメッセージが表示されます。Data Protector
- デフォルトでは、実行前/実行後コマンドはバックアップのプレビュー中には実行されません。この動作は、`ExecScriptOnPreview`グローバルオプションによって定義されます。

- 実行前/実行後コマンドは、コマンドプロンプトで入力したコマンドと同様に処理されます。ただし、?、*、"、|、<、および>といった特殊文字は使用できません。
- 実行前または実行後コマンド実行中にバックアップセッションを中止することはできません。
- 実行前および実行後プロセスはバックグラウンドモードで稼働します。このため、実行前/実行後コマンドではユーザーインターフェイスを必要とするコマンドは使用しません。
- タイムアウトが設定されており、実行前および実行後スクリプトは、デフォルトで少なくとも15分に1度出力を送信する必要があります。そうでない場合は、スクリプトが中止されます。この時間間隔は`ScriptOutputTimeout`グローバルオプションを編集することで変更できます。
- 実行前/実行後コマンドの結果はすべてIDBに書き込まれ、Data Protectorグラフィカルユーザーインターフェイスに表示されます。
- UNIXシステムでは、新しいプロセスを開始する前に、実行前または実行後スクリプトがすべてのファイル記述子を閉じなかったことにより、スクリプトが応答を停止することがあります。新しいプロセスがバックグラウンドで実行され、終了されないと(たとえばデータベースサーバープロセス(`dbstart`))、スクリプトが応答を停止します。

  `detach`コマンドを使用できます。`detach`コマンドのソースは`detach.c`ファイルに記述されていますが、サポートはされていません。例: `/opt/omni/bin/utilns/detach pre_script [arguments...]`
- 実行前/実行後コマンドは、デフォルトでは少なくとも120分に1度Disk Agentに出力を送信します。そうでない場合は、オブジェクトのバックアップが中止されます。この時間間隔は`SmDaIdleTimeout`グローバルオプションを編集することで変更できます。
- UNIXシステムでは、コマンドによって`stdout`に書き込まれたテキストは、セッションマネージャーに送られてデータベースに書き込まれます。`stderr`は`/dev/null`にリダイレクトされます。それを`stdout`にリダイレクトすることで、エラーメッセージをデータベースに記録できます。

セキュリティの留意事項

実行前コマンドおよび実行後コマンドは、無許可のユーザーが使用した場合に悪用される可能性があるため、危険性を含んでいます。実行前コマンドおよび実行後コマンドを使用しない場合は、無効にすることをお勧めします。また、実行前コマンドおよび実行後コマンドを使用する場合は、それらを安全な場所に置き、無許可のユーザーが変更できないようにします。

`StrictSecurityFlag`グローバルオプションを`0x0100`に設定すると、**[ルートユーザーとしてバックアップ]**または**[ルートユーザーとして復元]**パーミッションが付与されているユーザーのみ、実行前/実行後コマンドの実行が許可されます。

どのバックアップオブジェクトに対しても、実行前および実行後スクリプトを無効にする場合は、特定のクライアント上の`omnirc`ファイルに`OB2OEXECOFF=1`行を追加することで実現できます。どのクライアントに対しても、リモートセッションの実行前/実行後コマンドの実行を無効にする場合は、特定のクライアント上の`omnirc`ファイルに`OB2REXECOFF=1`を追加します。

クライアントを保護するには、そのクライアントにアクセスが許可されているCell Managerを指定します。許可されたCell Managerのみが、そのクライアントの実行前/実行後コマンドを実行することができます。

バックアップオブジェクトを対象とする実行前/実行後コマンドを指定する

すべてのバックアップオブジェクトを対象とする実行前/実行後コマンドを指定する

保存済みバックアップ仕様に含まれているすべてのオブジェクトを対象とする実行前コマンドおよび実行後コマンドを指定するには、以下の手順に従ってください。

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 実行前コマンドおよび実行後コマンドを指定するバックアップ仕様をダブルクリックし、**[オプション]**タブをクリックします。
4. [ファイルシステムオプション] (ディスクイメージバックアップの場合は保存済みバックアップ仕様内の[ディスクイメージオプション])で、**[拡張]**をクリックします。
5. [ファイルシステムオプション]ダイアログボックス(ディスクイメージバックアップの場合は[ディスクイメージオプション]ダイアログボックス)の[オプション]タブで、**[実行前]**テキストボックスと**[実行後]**テキストボックスの一方または両方にファイル名またはパス名を入力します。
6. **[OK]**をクリックし、**[適用]**をクリックして、変更内容を保存します。

個々のバックアップオブジェクトを対象とする実行前/実行後コマンドを指定する

保存済みバックアップ仕様に含まれている各オブジェクトに対して個別に実行前コマンドおよび実行後コマンドを指定するには、以下の手順に従ってください。

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[ファイルシステム]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 実行前コマンドおよび実行後コマンドを指定するバックアップ仕様をダブルクリックし、**[バックアップオブジェクトのサマリー]**タブをクリックします。
4. オブジェクトを右クリックし、**[プロパティ]**をクリックします。
5. [オブジェクトのプロパティ]ダイアログボックスで、**[オプション]**タブをクリックします。
6. **[実行前]**テキストボックスと**[実行後]**テキストボックスの一方または両方にファイル名またはパス名を入力します。
7. **[OK]**をクリックし、**[適用]**をクリックして、変更内容を保存します。

統合ソフトウェアを対象とする実行前/実行後コマンドを指定する

Oracleなどの統合ソフトウェアをバックアップするときは、データベースが1つのオブジェクトとして扱われるので、データベースバックアップの前後にコマンドが実行されます。これらのコマンドは、アプリケーションクライアント上で実行されます。

保存済みバックアップ仕様に含まれている統合ソフトウェアを対象とする実行前コマンドおよび実行後コマンドを指定するには、以下の手順に従ってください。

1. コンテキストリストで**[バックアップ]**をクリックします。
2. Scopingペインで、**[バックアップ仕様]**を展開し、目的の種類のバックアップ仕様(**[Oracle Server]**など)を展開します。保存されているすべてのバックアップ仕様が一覧表示されます。
3. 実行前コマンドおよび実行後コマンドを指定するバックアップ仕様をダブルクリックし、**[オプション]**タブをクリックします。
4. [アプリケーション固有オプション]で、**[拡張]**をクリックします。
5. [アプリケーション固有オプション]ダイアログボックスで、**[実行前]**テキストボックスと**[実行後]**テキストボックスの一方または両方にファイル名またはパス名を入力します。
6. **[OK]**をクリックし、**[適用]**をクリックして、変更内容を保存します。

バックアップスケジュールについて

> **重要:**
> Data Protector10.00では、基本スケジューラーとアドバンストスケジューラーが廃止され、代わりに新しいWebベーススケジューラが導入されました。Data Protectorのアップグレード中に、すべての既存のData Protectorスケジュールが新しいスケジューラーに自動的に移行されます。

特定の日時に実行するようバックアップセッションをスケジュールすることで、無人バックアップを構成できます。スケジュールは、日数単位、週単位、または月単位の間隔で設定できます。さらに、優先順位、ネットワーク負荷、およびデータ保護などのスケジュールのオプションを指定することもできます。

Data Protectorでスケジュールを作成および編集する方法の詳細については、「*スケジューラー、ページ 103*」を参照してください。

複数のバックアップを連続して実行する

特定のバックアップの終了後に他の特定のバックアップを開始できます。たとえば、ファイルシステムバックアップの終了後にOracleデータベースのバックアップを開始できます。

連続バックアップを開始するには、実行後コマンドを最初のバックアップ仕様で使用します。

手順

1. 先に実行するバックアップのスケジュールを設定します。
2. **[オプション]**タブをクリックし、**[バックアップ仕様オプション]**の**[拡張]**をクリックします。

3. [実行後]テキストボックスにomnibコマンドを入力し、このバックアップの終了後に実行するバックアップの名前をパラメーターとして指定します。たとえば、omnib -datalist *name_of_the_backup_specification*のような形式で指定します。コマンドを入力し終えたら、**[OK]**をクリックします。

> **ヒント:**
> また、先に実行するバックアップのステータスをチェックするためのスクリプトを指定することもできます。

バックアップ仕様グループについて

Data Protectorでは、バックアップ仕様をさまざまなグループに分けることができます。この機能は、多数のバックアップ仕様を管理したり、バックアップ仕様を共通する特性に応じてグループ分けする場合などに役立ちます。

バックアップ仕様を意味のあるグループに分けることによって、1つのバックアップ仕様の検索や保守が容易になります。また、グループ全体にテンプレートから共通のオプションを設定することも可能になります。たとえば、グループ内のバックアップ仕様すべてについてデバイスのリストを変更する場合に、テンプレートのデバイス設定を選択しながら適用することができます。

> **ヒント:**
> 共通したオプション設定値(デバイスのオプションなど)は、テンプレートからバックアップ仕様のグループに適用できます。これを行うには、まずグループ名をクリックして[CTRL+A]キーを押し、グループ内のすべてのバックアップ仕様を選択します。次に、ターゲットグループを右クリックして、**[テンプレートの適用]**をクリックします。

> **注:**
> Data ProtectorのGUIに表示できるバックアップ仕様の数には制限があります。バックアップ仕様の数はパラメーター(名前、グループ、所有者の情報、バックアップ仕様が不可調整されているかどうかという情報)のサイズによって異なります。このサイズは80kBを超えてはいけません。

バックアップ仕様グループの例

ここでは、大規模な企業のバックアップ仕様をグループ分けした例を示します。

User_files	このグループには、10の部署のそれぞれに所属する全ユーザーを対象に毎週のフルバックアップを実行するバックアップ仕様が含まれます。
SERVERS_DR	このグループには、会社のサーバーをディザスタリカバリに備えるためのバックアップ仕様が含まれます。新しいサーバーがインストールされるたびに、新しいバックアップ仕様が作成され、このグループに追加されます。
END_USER_ARCHIVE	このグループには、エンドユーザー要求ごとに作成されたバックアップ仕様が含まれます。たとえば、エンドユーザーがディスクスペースを解放しようとするときは、最初にハードディスクをアーカイブしておく必要があります。

バックアップ仕様グループを表示する

Data Protectorヘルプの手順では、デフォルトのバックアップビュー([種類別])を使用している場合を想定しています。ビューは、バックアップ仕様をグループ別に並べるよう変更することができます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. [表示]メニューの**[グループ別]**を選択します。

バックアップ仕様グループを作成する

さまざまな条件に応じた複数のバックアップ仕様グループを作成できます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. [表示]メニューの**[グループ別]**をクリックします。利用可能なバックアップグループのリストがScopingペインの[バックアップ仕様]の下に表示されます。
3. **[バックアップ仕様]**項目を右クリックし、**[グループの追加]**をクリックします。[新しいグループの追加]ダイアログボックスが表示されます。
4. 新しいグループの名前を[名前]テキストボックスに入力し、**[OK]**をクリックします。

[バックアップ仕様]項目の下に新しいバックアップグループが表示されます。適切なグループにバックアップ仕様を追加できます。

バックアップ仕様をグループに保存する

新しいバックアップ仕様を特定のグループに保存することができます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. [表示]メニューの**[グループ別]**をクリックします。利用可能なバックアップグループのリストがScopingペインの[バックアップ仕様]の下に表示されます。
3. **[バックアップ仕様]**を展開します。バックアップ仕様の追加先となるグループを右クリックし、**[バックアップの追加]**をクリックして、[バックアップ]ウィザードを起動します。
4. ウィザードの指示に従って、新しいバックアップ仕様を作成します。[バックアップ]ウィザードの最後のページ([別名で保存]、[バックアップ開始]、[プレビュー開始]を選択できるページ)で、**[別名で保存]**をクリックします。[バックアップを別名で保存]ダイアログボックスが表示されます。
5. バックアップ仕様の名前を[名前]テキストボックスに入力します。
6. バックアップ仕様の保存先のグループを[グループ]ドロップダウンリストから選択して**[OK]**をクリックする

と、バックアップ仕様が保存され、ウィザードが終了します。デフォルトで表示されるバックアップ仕様は、ウィザードの起動時に右クリックしたバックアップ仕様です。

指定したグループの下に保存済みバックアップ仕様が表示されます。

バックアップ仕様またはテンプレートをグループ間で移動する

バックアップ仕様またはテンプレートは、バックアップグループ間で移動できます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. [表示]メニューの**[グループ別]**をクリックします。利用可能なバックアップグループのリストがScopingペインの[バックアップ仕様]および[テンプレート]の下に表示されます。
3. **[バックアップ仕様]**項目または**[テンプレート]**項目を展開し、移動するバックアップ仕様が含まれているグループを展開します。
4. 移動するバックアップ仕様またはテンプレートを右クリックし、**[グループの変更]**をクリックします。[グループの変更]ダイアログボックスが表示されます。

   バックアップ仕様のプロパティを表示しているときは、**[グループの変更]**オプションが無効になります。
5. バックアップ仕様またはテンプレートの移動先のグループを[名前]ドロップダウンリストから選択し、**[OK]**をクリックします。

指定したグループにバックアップ仕様またはテンプレートが移動します。

バックアップ仕様グループを削除する

不要になったバックアップ仕様グループは削除できます。

手順

1. コンテキストリストで**[バックアップ]**をクリックします。
2. [表示]メニューの**[グループ別]**をクリックします。
3. **[バックアップ仕様]**項目を展開し、**[テンプレート]**項目を展開します。利用可能なバックアップ仕様グループのリストが表示されます。
4. 削除するグループを展開します。

   > **重要:**
   > バックアップ仕様やテンプレートが含まれているグループは削除できません。まず、グループから既存のバックアップ仕様とテンプレートを削除または移動する必要があります。

5. 削除対象のグループを右クリックし、**[グループの削除]**をクリックします。

選択したバックアップ仕様グループが削除されます。

Windowsシステムのバックアップについて

Windowsシステムのバックアップ手順は基本的に標準バックアップ手順と同じですが、Windows固有の要素がいくつかあります。

制限事項

VSSファイルシステムのバックアップを実行するには、システムに少なくとも1つのNTFSファイルシステムが存在していなければなりません。

バックアップの対象となるデータ

ファイルシステムをディスクドライブからバックアップする場合、ディレクトリ構造の読み込み、選択されたディスクドライブ上のファイルの中身の読み込み、およびファイルやディレクトリに関するWindows固有の情報の読み込みが発生します。

Windows Server 2012

- 圧縮ファイルはバックアップされ、圧縮状態で復元されます。
- 暗号化ファイルはバックアップされ、暗号化された状態で復元されます。

Windows固有の情報

- 完全なUNICODEファイル名
- FAT16、FAT32、VFATおよびNTFSの属性

  ファイルのバックアップが完了すると、そのファイルのアーカイブ属性がクリアされます。この動作は、バックアップ仕様の拡張ファイルシステムバックアップオプションの[アーカイブ属性を使用しない]オプションを設定することによって変更できます。
- NTFS代替データストリーム
- NTFSセキュリティデータ
- ディレクトリ共有情報

  ディレクトリがネットワークで共有されている場合、共有情報はデフォルトでバックアップされます。復元時には、共有情報はデフォルトで回復され、ディレクトリは回復後にネットワークで共有されます。この動作は、**[ディレクトリ共有情報のバックアップ]**オプションの選択を解除することにより変更できます。

バックアップの対象外のデータ

バックアップ仕様では、バックアップから除外またはスキップされるファイルのリスト(プライベート除外リスト)を指定できます。プライベート除外リストに指定したファイルの他に、Data Protectorのデフォルトの設定では、以下のディレクトリが除外されます。

Windows Vista、Windows 7、Windows 8、Windows Server 2008、およびWindows Server 2012の場合:

- WindowsクライアントまたはCell Manager(Windows Server 2008のみ)のバックアップから、Windowsクライアントバックアップのデフォルトのの Data Protectorログファイルディレクトリ。
- WindowsクライアントまたはCell Manager(Windows Server 2008のみ)のバックアップから、Windowsクライアントバックアップのデフォルトのの Data Protector一時ファイルディレクトリ。
- Windows Cell Manager(Windows Server 2008のみ)のバックアップの内部データベースディレクトリ。
- レジストリキー`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup`で指定されたファイル。

Windows Server 2012

- Resilient File System (ReFS)でフォーマットされたボリューム

その他のWindowsシステム

- Windowsクライアントバックアップのデフォルトの Data Protectorログファイルディレクトリ。
- Windowsクライアントバックアップのデフォルトの Data Protector一時ファイルディレクトリ。
- レジストリキー`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup`で指定されたファイル。

たとえば、内部データベースディレクトリは、バックアップ仕様で選択されていてもCell Managerのバックアップから除外されます。これは、IDBデータの整合性を保証するために特別な方法でバックアップする必要があるためです。

すべてのData Protectorホストは、証明書およびプライベートキーファイルを以下の場所で保守します。

- `<programdata>/Omniback/Config/sscertificates` (Windows)
- `/etc/opt/omni/config/sscertificates/` (Linux)

ファイルシステムのバックアップ中に、上記の場所からファイルがインクルードされると、プライベートキー以外のすべてのファイルがバックアップされます。

NTFS 3.1ファイルシステムの機能

- NTFS 3.1ファイルシステムは、再解析ポイントをサポートしています。

  ボリュームマウントポイント、単一インスタンス記憶域(SIS)、およびディレクトリの接続は、再解析ポイントのコンセプトに基づいています。これらの再解析ポイントは、他のファイルシステムオブジェクトと同様に選択できます。
- NTFS 3.1ファイルシステムでは、Windows VistaおよびWindows Server 2008オペレーティングシステムで導入されたシンボリックリンクがサポートされます。

  Data Protectorは、NTFS再解析ポイントと同じ方法でシンボリックリンクを処理します。
- NTFS 3.1ファイルシステムは、ディスクスペースの割り当て量を効率的に低減する手段としてスパース

ファイルをサポートしています。

これらのファイルは、ディスクスペース節約のためスパースファイルとしてバックアップされます。スパースファイルのバックアップと復元は、NTFS 3.1ファイルシステムに対してのみ可能です。

- NTFS 3.1ファイルシステム固有の機能の一部は、独自のデータレコードを維持するシステムサービスによって制御されています。これらのデータ構造は、CONFIGURATIONの一部としてバックアップされます。
- NTFS 3.1ファイルシステムは、オブジェクトIDをサポートしています。このオブジェクトIDは、Data Protectorによって他の代替データストリームと共にバックアップされます。
- 暗号化ファイル

  Microsoft方式で暗号化されたNTFS 3.1ファイルは暗号化された状態でバックアップと復元が行われ、そのファイルの中身は復号化されて初めてその内容が正しく表示されます。

再解析ポイント

再解析ポイントは、再解析ポイントIDと呼ばれる固有のタグが付加されたプレーンファイルシステムオブジェクトです。NTFS 3.1ディレクトリまたはファイルには、再解析ポイントが含まれている場合があり、一般に、別の場所にあるデータにダイレクトすることによって内容を再現します。

Data Protectorが再解析ポイントを検出したとき、デフォルトでは、再解析ポイントIDは無視されます。この動作は、raw再解析ポイントのバックアップとも呼ばれます。以下のように、バックアップの構成方法に影響します。

- ディスクデリバリーでバックアップを構成した場合は、すべてのデータが一度にバックアップされます。
- 再解析ポイントが格納されているファイルシステムまたはドライブをバックアップする場合は、再解析ポイントのリンク先のデータも必ずバックアップしてください。たとえば、Windowsでディレクトリ接続に使用されている再解析ポイントは無視されるので、接続点を個別にバックアップする必要があります。SIS再解析ポイントの場合は例外です。

  ディスク上のファイルは、単一インスタンス記憶域(SIS)サービスによって定期的にチェックされます。重複しているファイルが検出されると、それらのファイルが再解析ポイントに置換され、データが共通レポジトリに格納されます。これにより、ディスクスペースが節約されます。

再解析ポイントを使用して、論理ボリュームをディスクドライブとしてマウントできます。Data Protectorでは、マウントされたボリュームを通常のドライブと同様に扱うので、それらのボリュームはバックアップ用の選択可能なオブジェクトとして表示されます。

スパースファイル

スパースファイルとは、圧縮ファイルに比べて非常に多くのゼロデータセットが格納されているファイルです。Data Protectorでは、非ゼロデータの部分に対してのみバックアップデバイス上のメディアスペースが割り当てられるように、ゼロデータ部分を自動的にスキップしてバックアップを行います。

UNIXのスパースファイルとWindowsのスパースファイルは互換性がありません。

システムディスクをバックアップする際の注意事項

システムディスク上にある一部のファイルは常に使用中であり、Disk Agentを含むいずれのアプリケーションでも開くことができません。これらのファイルの内容はCONFIGURATIONの一部としてのみバックアップすることができます。

たとえばシステムディスク全体のバックアップを行った場合などに、ファイルシステムバックアップがこれらのファイルにアクセスすると、Data Protectorはこれらのファイルを開くのに失敗し、警告またはエラーを報告します。

これは、ファイルシステムバックアップの観点では正しい動作ですが、管理上の問題につながることがあります。常に多数の警告が報告され続けるため、別のファイルのエラーを見落としてしまう可能性があります。

警告が発生しないようにするには、CONFIGURATIONバックアップでバックアップされるファイルを、ファイルシステムバックアップから除外します。

> **注:**
> (たとえばデュアルブート環境などで)アクティブでないシステムディスクをバックアップする場合、以前にリストしたファイルは、現在アクティブなCONFIGURATIONファイルの一部にはなりません。これらのファイルはファイルシステムバックアップでバックアップできるため、除外しないでください。

構成データのバックアップ(Windows)

Windowsオペレーティングシステムによって維持される特殊なデータ構造は、ファイルシステムバックアップの対象になりません。Data Protectorでは、CONFIGURATIONと呼ばれる特殊なデータ構造をバックアップできます。

構成バックアップを実行するには、ファイルシステムバックアップ仕様作成時に、CONFIGURATIONオブジェクトを選択するか、CONFIGURATIONの一部を選択します。イベントログ、プロファイル、ユーザーディスククォータは、バックアップウィザードでCONFIGURATIONを選択した場合に常にバックアップされます。

Windows Vista、Windows 7、Windows Server 2008、およびWindows Server 2012では、Microsoftボリュームシャドウコピーサービスを使用してCONFIGURATIONバックアップが実行されます。

制限事項

- 同じシステム上で一度に実行できるCONFIGURATIONバックアップセッションは1つだけです。
- Active DirectoryサービスとSysVolはペアでバックアップしなければなりません。

Windowsの構成オブジェクト

- Active Directoryサービス
- 証明書サーバー
- COM+クラス登録データベース(`ComPlusDatabase`)
- DFS
- DHCP
- DNSサーバー
- EISA Utility Partition
- イベントログ
- ファイル複製サービス
- Internet Information Server (IIS)

- ユーザープロファイル(Documents and Settings)
- Windowsレジストリ
- リムーバブル記憶域の管理データベース
- SystemRecoveryData
- SysVol
- ターミナルサービスデータベース
- ユーザーディスククォータ(QuotaInformation)
- WINSサーバー

CONFIGURATIONは、Windowsシステムによって違いがあります。

オブジェクトによっては、特に留意すべき留意事項があります。それらを以下に示します。

Active Directory

Active Directoryサービスをバックアップすると、FRS(ファイル複製サービス)およびDFS(分散ファイルシステム)もバックアップされます。複製ファイルおよび分散ファイルに関する構成情報はすべてActive Directoryに保存されます。

DFS

Data Protectorでは、WindowsのDFS (分散ファイルシステム)を以下のいずれかの項目の一部としてバックアップします。

- Windowsレジストリ － DFSがスタンドアロンモードで構成されている場合
- Windows Active Directory － DFSがドメインモードで構成されている場合

DHCPおよびWINS

Data ProtectorがDHCPおよびWINSデータベースをバックアップする際、各サービスは終了され、データベースのバックアップ後再起動されます。DHCPおよびWINSサービスを実行しているサーバーのCONFIGURATIONバックアップを営業時間外に行うようスケジュール設定することをお勧めします。

DHCPおよびWINSサービスでは、それぞれのデータベースの内部バックアップコピーが作成されます。これらのサービスを一時的にシャットダウンできない環境では、これらのサービスをData Protector CONFIGURATIONバックアップの対象から除外して、ファイルシステムバックアップを通じて内部バックアップコピーをバックアップします。内部バックアップコピーの場所や、コピーの作成頻度が適切かを確認する方法については、Microsoft社のMSDNドキュメントを参照してください。

プロファイル

システム全体をバックアップ対象として指定すると、プロファイルは2回バックアップされます(ファイルシステムバックアップの一部としてバックアップされ、CONFIGURATIONの一部としてもバックアップされます)。これを回避するには、ファイルシステムバックアップからプロファイルデータを除外します。ユーザープロファイルデータは、c:\Documents and Settingsディレクトリに格納されます。

ディレクトリには、システム上で構成されたすべてのユーザープロファイルが含まれており、Data Protectorによってバックアップされます。複数のユーザーをサポートするようにシステムを構成すると、ユーザーごとに個

別のユーザープロファイルが作成されます。たとえば、すべての定義済みユーザーに共通のプロファイル要素はAll Usersプロファイルに格納され、ユーザーを新規作成するときに適用するプロファイル要素はDefault Userプロファイルに格納されます。

Data Protectorでは、以下のレジストリキーを読み込んで、プロファイルの保存場所を特定します。

HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\\

CurrentVersion\Explorer\Shell Folders

(共通プロファイル要素に関する情報は、ここに格納されます)

HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\\

CurrentVersion\Explorer\User Shell Folders

リムーバブル記憶域の管理データベース

Windows VistaおよびWindows Server 2008オペレーティングシステムで、リムーバブル記憶域の管理データベースの構成オブジェクトのバックアップを有効にするには、バックアップを実行するシステムにリムーバブル記憶域マネージャーがインストールされていることを確認してください。

ターミナルサービスデータベース

Windows VistaおよびWindows Server 2008オペレーティングシステムで、ターミナルサービスデータベースの構成オブジェクトのバックアップを有効にするには、バックアップを実行するシステムにTerminal Server Licensingサービスがインストールされていることを確認してください。

Windowsサービス

Windowsサービスのバックアップでは、各種サービスに使用されるデータ構造をバックアップします。対応するデータベースがファイルにエクスポート(ダンプ)され、そのファイルがバックアップされます。Windowsサービスは、バックアップウィザードでCONFIGURATIONを選択した場合に必ずバックアップされます。

Data Protectorによって検出され、バックアップウィザードに選択可能項目として表示されるWindowsサービスは、現在稼動中のサービスだけです。サービスがバックアップ時に稼動していない場合、対応するバックアップオブジェクトはバックアップされません。

サービスのいずれかをバックアップするには、CONFIGURATIONの下の対応するフォルダーを選択します。たとえば、Active Directoryを通じて証明書失効リスト(CRL)を公開している場合は、Certificate ServerとともにActive Directoryサービスをバックアップする必要があります。

システム状態データのバックアップ

Windowsのシステム状態は、Windowsシステムのさまざまな側面に関連しているいくつかの要素で構成されています。Windowsバックアップオブジェクトごとにシステム状態があります。

Windowsのシステム状態は、選択可能なバックアップ項目ではありません。Data Protectorでは、個々のオブジェクト(レジストリまたはCOM+クラス登録データベースなど)をバックアップできます。CONFIGURATIONツリー全体をバックアップすることをお勧めします。Windows Vista、Windows 7、Windows 8、Windows Server 2008、Windows Server 2012システムの場合は、**[シャドウコピーを使用]**オ

プションを選択した状態でファイルシステムのバックアップ機能を使用して、特定のボリュームまたはクライアントシステム全体をバックアップする必要があります。

システム状態には次のようなものがあります。

- ブートファイル: Ntldr.exe、Ntdetect.com、および boot.ini
- Registry および COM+ Class Registration Database (ComPlusDatabase)
- System File Protection System Volume Informationディレクトリに保持されているサービス

以下のサービスがインストールおよび構成されている場合は、これらの状態データもWindows Serverシステムのシステム状態データに含まれます。

- ActiveDirectoryService
- CertificateServer
- Cluster Service information
- IIS Metadirectory
- RemoteStorageService
- RemovableStorageManagementDatabase
- SystemFileProtection
- SYSVOL directory
- TerminalServiceDatabase

Windows Vista、Windows 7、Windows 8、Windows Server 2008、およびWindows Server 2012システムの場合は、システム状態データに、インストールされる追加のサーバーの役割またはサービスに属しているデータも含まれます。

リモートストレージサービス

リモート記憶域サービスは、アクセス頻度の低いファイルをローカルからリモート記憶域へ自動的に移動するために使用されます。リモートファイルはファイルを開くと自動的に再呼び出しされます。RSSデータベースはシステム状態データの一部ですが、バックアップは手動で行います。

リモートストレージサービス:

- リモート記憶域エンジン: *%SystemRoot%*\system32\RsEng.exe
  使用頻度の低いデータの保存に使用されるサービスおよび管理ツールを調整します。
- リモート記憶域ファイル: *%SystemRoot%*\system32\RsFsa.exe
  リモート保存されたファイル上の操作を管理します。
- Remote Storage Notification: *%SystemRoot%*\system32\RsNotify.exe
  呼び出されたデータについてクライアントに通知します。

リモート記憶域データベース:

リモート記憶域データベースは、次のディレクトリにあります。*%SystemRoot%*\system32\RemoteStorage

- RSSエンジンデータベース: *%SystemRoot%*\system32\RemoteStorage\EngDb
- RSSエンジンバックアップデータベース: *%SystemRoot%*\system32\RemoteSorage\EngDb.bak

- RSSファイルデータベース: *%SystemRoot%*\system32\RemoteStorage\FsaDb
- RSSトレースデータベース: *%SystemRoot%*\system32\RemoteStorage\Trace

リムーバブル記憶域の管理データベース

リムーバブル記憶域データベースはバックアップ可能ですが、このサービスはData Protectorメディア管理では使用されません。ロボティクスメディアで使用されるネイティブロボティクスドライバーは、Data Protectorがデバイスを構成する前にあらかじめ無効にしておく必要があります。

ファイルシステム保護

システムファイル保護サービスでは、コンピューターの再起動後に、保護されたすべてのシステムファイルのバージョンをスキャンおよび検証します。システムファイル保護サービスでは、保護ファイルが上書きされていることを見つけたら、正しいバージョンのファイルを検索して不正なファイルを置き換えます。Data Protectorでは、保護ファイルを上書きすることなく、バックアップして復元することができます。保護ファイルは、ファイルシステムの標準バックアップ手順にある[使用中のファイルを移動]オプションを使用してバックアップすることができます。

UNIXシステムのバックアップについて

UNIXシステム上でバックアップを行う場合には、標準のバックアップ手順を使用してください。NFSを使ってディスクをバックアップする場合、VxFSスナップショットバックアップの場合、またはUNIXディスクイメージバックアップの場合は、いくつかの追加手順を実行する必要があります。

制限事項

- NFSマウントファイルシステムをバックアップする場合は、すべての属性が保持されるわけではありません。
- バックアップ可能なファイルの最大サイズは、オペレーティングシステムおよびファイルシステム側の制限に依存します。

サポートされているプラットフォームと既知の制限事項の詳しいリストについては、『HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照してください。

バックアップの対象となるデータ

- Data Protectorでは、ディレクトリ構造、通常のファイル、および特殊なファイルをバックアップします。特殊なファイルには、キャラクターデバイスファイル、ブロックデバイスファイル、UNIXドメインソケット、FIFOファイル、HP-UXのネットワークファイル、XENIXの名前付きファイルがあります。
- シンボリックリンクのリンク先はたどられず、シンボリックリンクとしてバックアップされます。
- マウントポイントがある場合は、マウント対象のデータではなく、マウントポイント自体が通常の空のディレクトリとしてバックアップされます。
- 同じファイルを参照する複数のハードリンクがある場合は、参照先ファイルが1回だけバックアップされます。これは、**[POSIXハードリンクをファイルとしてバックアップ]**オプションを設定することにより変更できます。

- 基本ACL(ファイルパーミッション属性)と時刻属性は、サポートされているすべてのUNIXプラットフォーム上のファイルと共にバックアップされます。ただし、拡張ACLのサポートは一部のプラットフォームに限定されます。詳細は、https://softwaresupport.hpe.com/にある『HPE Data Protectorのプラットフォームと統合ソフトウェアのサポート一覧』を参照してください。各ファイルへの最終アクセス時刻は、ファイルの内容を読み取る前に保存され、ファイルのバックアップ後に元の値に戻されます。この動作は、**[アクセス時刻属性を保存しない]**オプションを設定することにより変更できます。

UNIXファイルシステムのバックアップから除外するべきデータ

- 内部データベースディレクトリ。内部データベースディレクトリは特別な方法でバックアップ(オンライン)する必要があります。
- 一時ディレクトリ

NFSのバックアップ

NFS (Network Filesystem)とは、ネットワークを介したファイルのアクセスをローカルディスクの場合と同じようにできるようにする、分散ファイルシステムプロトコルです。NFSを使うと、アクセス可能なリモートUNIXシステムからファイルシステムをバックアップできます。

どのような場合にNFSバックアップを使用するか

- システムがData Protectorセルの一部ではない場合、またはシステムにDisk Agentがインストールされていない場合。
- Data Protectorによってサポートされていないシステムプラットフォームをバックアップする場合。

定期的に実行するファイルシステムバックアップを構成する場合は、NFSマウントファイルシステムをバックアップ対象から除外することをお勧めします。NFSマウントファイルシステムを除外しておくと、ディスクを実際に格納しているシステムが同時にバックアップされている場合に、警告メッセージが表示されたり、同じディスクが重複してバックアップされたりすることがなくなります。

制限事項

- HP-UX、Solaris、およびLinuxクライアント上でNFSを使用してバックアップできるのは、NFSでマウントされたボリュームです。ソフトリンク、キャラクター、およびデバイスファイルはバックアップできません。サポートされているプラットフォームの詳細については、最新のサポート一覧(https://softwaresupport.hpe.com/)を参照してください。
- ACL(アクセス制御リスト)属性は維持されません。NFSではリモートファイルに対するACLをサポートしていません。各種システムコール、ライブラリコール、およびコマンドは、個々の手動エントリとして指定します。省略可能なエントリを指定したファイルをネットワーク経由で転送したり、リモートファイルを操作すると、確認メッセージなしで省略可能なエントリが削除されることがあります。

HP OpenVMSファイルシステムのバックアップ手順は基本的に標準バックアップ手順と同じですが、OpenVMSに固有の要素がいくつかあります。

前提条件

- OpenVMSシステム上のデータをバックアップするには、OpenVMSシステム上にOpenVMS Disk Agentをインストールする必要があります。
- OpenVMSシステムに接続されているバックアップデバイスをData Protectorで使用するには、OpenVMSシステム上にGeneral Media Agentをインストールします。

制限事項

- GUIで入力されるかCLIに渡されるファイル仕様は、UNIXスタイルの構文である必要があります。

  `/disk/directory1/directory2/filename.ext.n`

  先頭にスラッシュを入力し、ディスク、ディレクトリ、ファイル名をそれぞれスラッシュで区切って入力します。

  ディスク名の後ろにコロンを付けないでください。

  バージョン番号の前には、セミコロンではなくピリオドを使用します。

  OpenVMSファイルのファイル指定では、ODS-5ディスク上にあるファイルを除き、大文字と小文字が区別されます。以下に例を示します。

  `$1$DGA100:[bUSERS.DOE]LOGIN.COM';1`

  上記は以下の形式で指定する必要があります。

  `/$1$DGA100/USERS/DOE/LOGIN.COM.1`
- 暗黙的なバージョン番号はありません。バージョン番号は常に明示的に指定する必要があります。バックアップされるのは、バックアップ対象として選択されたファイルバージョンのみです。ファイルの全バージョンを復元対象に含めるには、それらをすべてGUIウィンドウ内で選択するか、またはCLIで**[オンリー]** (`-only`)オプションにファイル指定を含めるときに、次の例のように、すべてのバージョン番号にマッチするワイルドカード文字を入力します。

  `/DKA1/dir1/filename.txt.*`
- 書き込み禁止ディスクおよびシャドウディスクを正しくバックアップするためには、バックアップ仕様で**[アクセス時刻属性を保存しない]**オプションを有効にします。
- **[アクセス時刻属性を保存しない]**オプションを有効にしてバックアップを実行すると、ODS-5ディスク上では、最終アクセス日時が現在の日時に更新されます。ただし、ODS-2ディスク上では、このオプションは無視され、すべての日付が元のまま残されます。
- OpenVMS上ではディスクイメージのバックアップを実行できません。"BACKUP/PHYSICAL"に相当する要素がないためです。
- **[POSIXハードリンクをファイルとしてバックアップ]** (`-hlink`)、**[ソフトウェア圧縮]** (`-compress`)、および**[暗号化]** (`-encode`)の各オプションは、OpenVMS上では使用できません。

  複数のディレクトリエントリがあるファイルは、プライマリパス名を使用して1回だけバックアップされます。セカンダリパスエントリは、ソフトリンクとして保存されます。復元時には、これらのセカンダリパスエントリも復元されます。

  BACKUP/IMAGEに相当する要素はサポートされていません。復元したOpenVMSシステムディスクを起動可能にするには、復元したディスクにOpenVMS WRITEBOOTユーティリティを使用してブートブロックを書き込む必要があります。

- **[バックアップ時にファイルをロック]** (`-lock`)オプションの有効/無効に関係なく、バックアップ中のファイルは常にロックされます。`-lock`オプションが有効になっている場合、書き込み用に開かれているファイルはいずれもバックアップされません。`-lock`オプションが無効になっている場合には、開かれているファイルもバックアップされます。
- 実行前コマンドプロシージャと実行後コマンドプロシージャのデバイスおよびディレクトリは、デフォルトでは`/omni$root/bin`になります。コマンドプロシージャを他の場所に配置するには、デバイスとディレクトリのパスをUNIXスタイルの形式でファイル指定に含める必要があります。例:

  ```
  /SYS$MANAGER/DP_SAVE1.COM
  ```
- ワイルドカード文字を**[スキップ]** (`-skip`)または**[オンリー]** (`-only`)フィルターで指定するとき、複数の文字については'*'を使用し、単一の文字については'?'を使用します。
- Data Protectorファイルライブラリは、OpenVMS ODS-2ディスク上ではサポートされていません。
- OpenVMSシステムでは、ボリュームおData Protectorよびボリュームセット上のディスククォータはサポートされません。

  ディスククォータを有効にしてボリューム上のデータのバックアップを実行するには、実行前スクリプトを構成してバックアップの開始前に関係するボリュームでディスククォータを無効にし、実行後スクリプトを構成してバックアップの完了後にディスククォータを有効にします。

バックアップの対象となるデータ

ディレクトリ構造およびファイルが、以下のファイルシステム情報と共にバックアップされます。

- ファイルおよびディレクトリの属性
- ACL(アクセス制御リスト)

ファイルは、マウントされているFILES-11 ODS-2またはODS-5ボリュームからのみバックアップできます。

Novell Open Enterprise Server (OES)のバックアップについて

Novell OESのバックアップ手順は基本的に標準バックアップ手順と同じですが、Novell OESに固有の要素がいくつかあります。

前提条件

- Data Protector Disk AgentがNovell OESシステムにインストールされている必要があります。
- ファイルシステム用Target Service Agent(TSAFS)がデュアルモードでロードされている必要があります。
- NDS/eDirectoryバックアップの場合は、Novellディレクトリサービス用Target Service Agent(TSANDS)がロードされている必要があります。
- GroupWiseバックアップの場合は、ファイルシステム用GroupWise Target Service Agent(TSAFSGW)がロードされている必要があります。
- Novell OESバックアップサービスにログインする際に使用するユーザーアカウントを選択して、`HPLOGIN.NLM`ファイルに保存する必要があります。任意のユーザーアカウントを使用できますが、バックアップ対象のファイルやディレクトリがそのユーザーアカウントのものに限定されます。
- Storage Management Services (SMS)をNovell OESシステムにインストールする必要があります。

制限事項

- ソフトウェアデータ圧縮はサポートされていません。バックアップオプションの[ソフトウェア圧縮]を選択しても、バックアップされるデータには適用されません。

圧縮ファイルのバックアップおよび復元

Novell OESにはファイル圧縮機能があります。Data Protectorはデフォルトで、圧縮されているファイルを圧縮形式でバックアップし、したがって圧縮形式で復元します。このため、これらのファイルはボリュームが圧縮されたNovell OESでしか復元できません。

バックアップの対象となるデータ

- ネイティブLinuxボリューム
- Novell GroupWiseデータ

ファイルのバックアップが完了するたびに、ファイルのアーカイブフラグがクリアされ、アーカイブ日時が設定されます。

Novell OESを構成する

HPLOGINユーティリティを使用してユーザー名とパスワードを保存する

HPLOGINユーティリティは`/opt/omni/lbin`ディレクトリにあります。このユーティリティを実行して、適切なユーザー資格情報(ユーザー名とパスワード)をファイル`/root/OMNI$CFG.DAT`に保存します。

手順

1. 現在の作業ディレクトリを`/opt/omni/lbin`に変更します。
2. HPLOGINユーティリティを実行します。

   ```
   ./hplogin
   ```

ファイルシステム用Target Service Agent(TSAFS)をデュアルモードでロードする

手順

1. ターゲットシステムでTSAを構成します。TSAはデフォルトでLinuxモードでロードされています。これをデュアルモードに変更します。
   a. 現在の作業ディレクトリを`/opt/novell/sms/bin`に変更します。
   b. TSAFSがロード済みかどうかを確認します。

```
./smsconfig -t
```

c. ロードされていた場合は、アンロードします。

```
./smsconfig -u tsafs
```

d. TSAをデュアルモードでロードします。

```
./smsconfig -l tsafs --tsaMode=Dual
```

2. Open Enterprise Server Linux上のTSAFS構成ファイルのフルパス名は、`/etc/opt/novell/sms/tsafs.conf`です。ロードされたTSAは、デフォルト構成用にこの構成ファイルを読み込みます。TSAがロードされるたびにTSAFSを自動的にデュアルモードでロードするように、このファイルを構成します。
3. ファイル`/etc/opt/novell/sms/tsafs.conf`,を編集してtsamodeをLinuxからデュアルモードに変更し、ファイルを保存します。

```
tsamode=Dual
```

Novellディレクトリサービス用Target Service Agent (TSANDS)をロードする

TSANDSエージェントを手動でロードするか、またはNovell OES起動時のエージェントの自動ロードを構成することができます。

手順

- エージェントを手動でロードするには、以下の手順を実行します。
  1. ターミナルウィンドウを開きます。
  2. 現在のディレクトリを`/opt/novell/sms/bin`に変更します。
  3. 次のコマンドを実行して、エージェントが既にロードされているかどうかを確認します。

     ```
     ./smsconfig -t
     ```

  4. エージェントがロードされていない場合は、次のコマンドでエージェントをロードします。

     ```
     ./smsconfig -l tsands
     ```

- エージェントの自動ロードを構成するには、以下の手順を実行します。
  1. 構成ファイル`/etc/opt/novell/sms/smdrd.conf`に以下の行を追加します。

     ```
     autoload: tsands
     ```

ファイルシステム用GroupWise Target Service Agent (TSAFSGW)をロードする

TSAFSGWエージェントを手動でロードするか、またはNovell OES起動時のエージェントの自動ロードを構成することができます。

手順

- エージェントを手動でロードするには、以下の手順を実行します。
  1. ターミナルウィンドウを開きます。
  2. 現在のディレクトリを/opt/novell/sms/binに変更します。
  3. 次のコマンドを実行して、エージェントが既にロードされているかどうかを確認します。

     ```
     ./smsconfig -t
     ```
  4. エージェントがロードされていない場合は、次のように適切なパラメーターを指定してエージェントをロードします。

     ```
     ./smsconfig -l tsafsgw --home DomainDirectory --home PostOfficeDirectory
     ```
- エージェントの自動ロードを構成するには、以下の手順を実行します。
  1. 構成ファイル/etc/opt/novell/sms/smdrd.confに、次の行を追加します(引数のプレースホルダーを実際の値に置き換えます)。

     ```
     autoload: tsafsgw --home DomainDirectory --home PostOfficeDirectory
     ```

バックアップのパフォーマンスについて

バックアップの構成時には、バックアップのパフォーマンス要因を考慮する必要があります。多数の変数をさまざまな組み合わせで指定できるので、あらゆるユーザーニーズを満たしつつ、投資レベルでも申し分のない推奨設定を明確に示すことはできません。ですが、バックアップまたは復元のパフォーマンスを向上するにあたっては、次の点に注意してください。

インフラストラクチャー

インフラストラクチャーは、バックアップおよび復元のパフォーマンスに大きく影響します。特に重要な要因として、データパスの並列化状況および高速装置の使用があります。

- バックアップおよび復元をネットワーク経由で行うか、ローカルに行うか

  ネットワーク経由でデータを送信する場合は、新たなオーバーヘッドが生じるため、ネットワーク自体がパフォーマンスに影響を及ぼす要素となります。Data Protectorは、次の場合にデータストリームを別に処理します。
  - ネットワークデータストリーム: ディスク→メモリ→ネットワーク→メモリ→デバイス
  - ローカルデータストリーム: ディスク→メモリ→デバイス

  パフォーマンスを最大化するには、高ボリュームデータストリームに対してローカルバックアップ構成を使用することをお勧めします。
- 使用するデバイス、コンピューターシステム自体、およびハードウェアの並列使用も、パフォーマンスに著しい影響を与える要因になることがあります。

  バックアップや復元のパフォーマンスを最大化するには、次のようなことができます。
  - 適切な同時処理数を設定して、デバイスストリーミングを実現する
  - セグメントサイズとブロックサイズを最適化する

- Disk Agentバッファーの数を調整する
- ソフトウェア圧縮またはハードウェア圧縮を使用する
- ディスクベースのバックアップデバイス(ファイルライブラリ)を使用する
- フルバックアップや増分バックアップを計画する
- 合成バックアップやディスクステージングなどの高度なバックアップ戦略を用いる
- メディアに対するバックアップオブジェクトの分配を最適化する
- ファイルシステムスキャンを無効にする

オブジェクトのミラーリングとバックアップパフォーマンス

オブジェクトのミラーリングは、バックアップの性能に影響します。Cell ManagerクライアントやMedia Agentクライアント上では、ミラーの作成に伴い、別のオブジェクトを追加してバックアップする場合と同等の影響が生じます。これらのシステムでは、ミラーの数に応じてバックアップパフォーマンスが低下します。一方、Disk Agentクライアント上ではバックアップオブジェクトの読み取りが1回しか行われないため、ミラーリングに伴う影響はありません。

バックアップパフォーマンスは、デバイスのブロックサイズやデバイスの接続などの要因によっても左右されます。バックアップとオブジェクトのミラーリングに使用するデバイスのブロックサイズが異なる場合、ミラーリングされたデータはセッション中に再パッケージされるため、より多くの時間とリソースが必要になります。また、ネットワークを介してデータを転送すると、新たなネットワーク負荷が発生し、処理時間もそれだけ長くなります。

デバイス以外の高パフォーマンスハードウェア

コンピューターシステム自体のディスクの読み取り速度とデバイスへの書き込み速度も、パフォーマンスを直接左右する要因になります。バックアップ中のディスク読み取りやソフトウェア圧縮(圧縮解除)などはシステムへの負荷となります。

I/Oパフォーマンスやネットワークの種類の他に、ディスクの読み取り速度とCPUの可用性もシステム自体のパフォーマンス上重要な要因になります。

ハードウェアの並列処理

複数のデータパスを並列に使用すると、パフォーマンスが向上します。パスにはネットワークインフラストラクチャーが含まれます。並列処理は、以下のような場合に効果的です。

- ローカルにバックアップされるシステム、つまり、ディスクとバックアップ用のデバイスが直接接続されているシステムが複数存在する場合。
- ネットワーク経由でバックアップするシステムが複数存在する場合。ただし、ネットワークトラフィックがオーバーラップしない経路で転送されることが前提となります。オーバーラップしていると、パフォーマンスが低下します。
- 1つまたは複数の(テープ)デバイスにバックアップするオブジェクト(ディスク)が複数存在する場合。

- 特定の複数のシステムの間で、複数の専用ネットワークリンクを使用できる場合。たとえば、システムAにバックアップするオブジェクト(ディスク)が6つあり、システムBに高速テープデバイスが3つあるとします。この場合は、システムAとシステムBとの間にバックアップ専用のネットワークリンクを3つ用意します。
- 使用デバイスが複数あり、**[負荷調整]**オプションが有効の場合。

同時処理数

各Media Agentから起動されるDisk Agentの数は、Disk Agent (バックアップ)同時処理数と呼ばれます。この数は、デバイス用の拡張オプションを使用して変更できるほか、バックアップの構成時にも変更可能です。バックアップ仕様に設定されている同時処理数は、デバイス定義に設定されている同時処理数より優先されます。

Data Protectorでは、Disk Agent数がデフォルト値に設定されており、ほとんどの場合はこの数で十分です。たとえば標準的なDDSデバイスの場合であれば、2つのDisk Agentにより、ストリーミングの維持に十分なデータをデバイスに送信できます。また、ライブラリデバイス内に複数のドライブがあり、各ドライブが個別のMedia Agentで制御される場合には、それぞれのドライブごとに個別に同時処理数を設定できます。

パフォーマンスへの影響

バックアップの同時処理数を適切に設定すると、バックアップのパフォーマンスが向上します。たとえば4つのドライブを持つライブラリデバイスがあり、各ドライブは個別のMedia Agentで制御されているとします。このとき、個々のMedia Agentがそれぞれ2つのDisk Agentから同時にデータを受け取ると、8つのディスク上のデータを同時にバックアップできます。

多重データストリーム

同じディスクを複数の部分に分け、それらを同時に複数のデバイスにバックアップすることができます。これにより、バックアップ速度が向上します。この方法は、非常に大型で高速なディスクを比較的低速なデバイスにバックアップする場合に効果的です。複数のDisk Agentが同じディスクから並列にデータを読み取り、複数のMedia Agentに送信します。

多数のDisk Agentを通じて単一のマウントポイントをバックアップした場合、データは複数のオブジェクトに格納されています。このマウントポイントの全体を復元するには、単一のバックアップ仕様でマウントポイントの分割部分をすべて定義した上で、セッション全体を復元する必要があります。

デバイスストリーミング

デバイスのパフォーマンスを最大限に引き出すには、デバイスをストリーミング状態に維持する必要があります。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。ストリーミングが保たれていないと、テープの送りを停止する必要が生じ、その間、デバイスはデータを待機します。データが到着すると、テープを若干逆送りしてテープへの書き込みを再開します。つまり、コンピューターがデバイスにデータを転送する速度と同じか、それ以下の速度でテープにデータが書き込まれていれば、デバイスはストリーミング状態になります。デバイスストリーミングはその他の要因、たとえばネットワーク負荷や、1度の操作でバックアップデバイスに書き込めるデータのブロックサイズにも左右されます。バックアップインフラストラクチャーでネットワークを多用する場合は、そのことにも注意が必要です。

ディスクとデバイスが同じシステムに接続されているローカルバックアップの場合は、ディスクが高速であれば、同時処理数を1に設定するだけで十分です。

デバイスストリーミングの構成方法

デバイスでストリーミングを行えるようにするには、デバイスに十分な量のデータを送信する必要があります。このため、Data Protectorでは、データをデバイスに書き込む各Media Agentに対して複数のDisk Agentを起動します。

ブロックサイズ

セグメントはユニットとして書き込まれるのではなく、ブロックと呼ばれるユニットより小さなサブユニットとして書き込まれます。デバイスハードウェアは、受信データの処理に、デバイスの種類固有のブロックサイズを使用します。

Data Protectorでは、さまざまな種類のデバイスにデフォルトのデバイスブロックサイズを使用します。このブロックサイズは、Data Protectorによって作成されたすべてのデバイスと、各種プラットフォーム上で実行されるMedia Agentに適用されます。

ブロックサイズを大きくすると、パフォーマンスが向上することがあります。デバイスに送信されるブロックは、新しいデバイスを構成しているときや、デバイスの拡張オプションでデバイスプロパティを変更するときに調整できます。復元はブロックサイズに合わせて実行されます。

> **注意:**
> Data Protector Media Agentで制御しているデバイスのブロックサイズを拡張する場合には、オペレーティングシステムでサポートされるデフォルトの最大ブロックサイズを超えないように注意してください。ブロックサイズが最大サイズを超えると、Data Protectorでデバイスのデータを復元できなくなります。ブロックサイズが調整可能かどうか、調整方法については、オペレーティングシステムのドキュメントを参照してください。

ブロックサイズの変更は、テープのフォーマットの前に行う必要があります。デバイスブロックサイズはメディアヘッダーに書き込まれ、Data Protectorはこの情報に基づいて使用するサイズを決定します。デバイスブロックサイズがメディアブロックサイズと異なっていると、エラーが発生します。

デバイスのブロックサイズを変更する前には、使用しているホストアダプターでサポートされているブロックサイズをチェックしておく必要があります。Adaptec 2940などの古いSCSIカードの最小ブロックサイズは56 kBでした。新しいSCSIカードで主に使用されている最小ブロックサイズは64 kBです。

Windows Media Agentクライアント上では、レジストリを編集すると最大ブロックサイズを大きくできます。手順はホストバスアダプターのタイプ(SCSI、ファイバーチャネル、またはiSCSI)によって異なります。詳細は、例のリンク先のトピックを参照してください。

特定のホストバスアダプターのブロックサイズを変更する場合は、前もってベンダーのマニュアルを参照するか、またはベンダーのサポート窓口に問い合わせてください。

セグメントサイズ

メディアは、データセグメント、カタログセグメント、ヘッダーセグメントに分かれています。ヘッダー情報は、ブロックサイズと同じ長さのヘッダーセグメントに格納されます。データは、データセグメント内のデータブロックに格納されます。各データセグメントに関する情報は、対応するカタログセグメントに格納されます。この

情報は、Media Agentのメモリにまず記録され、その後にメディアのカタログセグメントとIDBに書き込まれます。

セグメントサイズ(MB単位)は、データセグメントの最大サイズです。小サイズのファイルを多数バックアップする場合、実際のセグメントサイズはカタログセグメントの最大サイズに制限されることがあります。セグメントサイズはデバイスごとにユーザーが構成でき、復元とメディアのインポートの際のパフォーマンスに影響します。セグメントサイズは、新しいデバイスを構成しているときや、デバイスの拡張オプションでデバイスプロパティを変更しているときに調整できます。

最適なセグメントサイズは、デバイスで使用するメディアの種類およびバックアップするデータの種類によって異なります。テープごとの平均セグメント数は50です。デフォルトのセグメントサイズは、テープのネイティブ容量を50で除算して計算できます。最大カタログサイズは、すべてのメディアの種類で定数(12 MB)に制限されています。

Data Protector最初の制限値に達したときにセグメントは終了します。小サイズのファイルを多数バックアップする場合、メディアカタログの制限値に達する方が早いため、セグメントサイズが小さくなります。

Disk Agentのバッファー数

Data ProtectorのMedia AgentとDisk Agentは、転送待ちのデータを一時的に保持するためにメモリバッファーを使用します。このメモリは、複数のバッファー領域に分割されています。総数はデバイスの同時処理数に依存しますが、Disk Agentごとにバッファー領域が1つずつあります。各バッファー領域は8つのDisk Agentバッファー(デバイスに対して構成したブロックサイズと同じサイズ)で構成されます。

バッファー数は、新しいデバイスを構成しているときや、デバイスの拡張オプションでデバイスプロパティを変更するときに変更できます。この設定を変更する理由としては、主に以下の2つの理由が考えられます。

- メモリ不足:Media Agentに必要な共有メモリは次のように計算できます。

  ```
  DAConcurrency*NumberOfBuffers*BlockSize
  ```

  たとえば、バッファー数を8から4に減らすと、パフォーマンスに影響が生じる一方で、メモリ消費が50%減少します。
- ストリーミング

  バックアップ中に利用可能なネットワーク帯域幅が大幅に変動する場合は、デバイスをストリーミングモードに維持できるように十分な量の書き込みデータをMedia Agentが転送するように設定することが重要です。この場合は、バッファー数を増やす必要があります。

ソフトウェア圧縮

ソフトウェア圧縮は、ディスクからデータを読み取るときにクライアント側のCPUによって行われます。これにより、ネットワーク経由で転送するデータのサイズが小さくなりますが、クライアント側のCPUリソースを大きく消費します。

デフォルトでは、ソフトウェア圧縮は無効になっています。一般に、パフォーマンスを向上させる目的にはハードウェア圧縮のみを使用してください。低速なネットワークを経由して多数のシステムをバックアップする場合は、ソフトウェア圧縮を使用することでデータを圧縮してからネットワーク経由で転送できますが、それ以外の場合はお勧めできません。

ソフトウェア圧縮を使用する場合は、ハードウェア圧縮を無効化してください。両方の方法でデータを圧縮しようとすると、データのサイズが大きくなってしまいます。

ハードウェア圧縮

最近のバックアップデバイスは、ハードウェア圧縮機能が組み込まれているものが大半です。ハードウェア圧縮は、デバイス構成手順でデバイスファイルまたはSCSIアドレスを作成するときに有効化できます。

ハードウェア圧縮は、元データをMedia Agentクライアントから受信して、圧縮モードでテープに書き込むデバイスによって実行されます。ハードウェア圧縮を使うと、テープに書き込まれるデータのサイズが小さくなり、テープドライブがデータを受信する速度が向上します。

ハードウェア圧縮に関しては、次の点に注意してください。

- 圧縮モードで書き込んだデータを非圧縮モードのデバイスで読み込んだり、非圧縮モードで書き込んだデータを圧縮モードのデバイスで読み込んだりすることはできないため、ハードウェア圧縮を使用する際は注意が必要です。
- ソフトウェア圧縮とハードウェア圧縮を同時に使用しないでください。ハードウェア圧縮とソフトウェア圧縮を併用しても、圧縮率は向上せず、性能が低下するだけです。
- HPE Ultrium LTOドライブは自動ハードウェア圧縮機構を備えていますが、これを無効にすることはできません。HPE Ultrium LTOドライブをData Protectorで構成する場合は、[ソフトウェア圧縮]オプションを無効にすることをお勧めします。
- ハードウェア圧縮をサポートしていないデバイスでハードウェア圧縮を使用して書き込まれたメディアからの読み込みを行う場合、Data Protectorはそのメディアを認識したり、データを読み込んだりできません。このようなメディアは不明または新規として処理されます。

デバイスを構成するときに、ドロップダウンリストからSCSIアドレスを選択すると、デバイスがハードウェア圧縮を使用できるかどうかが自動的に判別されます。Data Protector

UNIXシステムでハードウェア圧縮を有効化するには、ハードウェア圧縮デバイスファイルを選択します。

Windowsシステムでは、検出に失敗し、SCSIアドレスを手動で入力する場合、デバイス/ドライブのSCSIアドレスの末尾に`C`を追加します。例えば、次のように設定します。例: `scsi:0:3:0C` (テープドライバーがロードされている場合は、`tape2:0:1:0C`)。デバイスがハードウェア圧縮をサポートしていれば、ハードウェア圧縮が使用されます。サポートしていなければ、`C`オプションは無視されます。

ハードウェア圧縮をWindowsシステム上で無効化するには、デバイスやドライブのSCSIアドレスの末尾に`N`を追加してください(例: `scsi:0:3:0N`)。

マルチパスデバイスの場合は、パスごとにこのオプションを設定します。

ディスクイメージバックアップとファイルシステムバックアップ

ディスクイメージバックアップとファイルシステムバックアップから選択する場合は、それぞれの長所と短所を考慮してください。ほとんどの場合については、ファイルシステムバックアップをお勧めします。

	ファイルシステムのバックアップ	ディスクイメージバックアップ
バックアップの整合性	バックアップ中にファイルをロックできるため、整合性のある状態でファイルがバックアップされます。ファイルとディレクトリの構造が維持されます。	バックアップ中にファイルをロックできないため、特定の時刻ポイントの状態でファイルがバックアップされます。ファイルとディレクトリの構造はブラウズできません。

バックアップサイズ	バックアップしたデータが占有する容量は、バックアップ時のファイルとフォルダーデータの累積サイズと同じになります。	バックアップメディアでバックアップしたデータが占有する容量は、バックアップ元のボリュームのサイズと同じになります。
バックアップおよび復元の速度	バックアップおよび復元の速度は、バックアップしたディスクに空き容量があり、ファイル数が少ない場合に高速になります。	バックアップおよび復元の速度は、バックアップしたディスクがいっぱいで、ファイル数が多い場合に高速になります。
復元の再使用性	ファイルとディレクトリの構造が維持されるため、復元したファイルを容易にナビゲートできます。	ディスク全体またはディスクセクションが復元され、ファイルとディレクトリの構造はブラウズできません。

> **注:**
> Windowsシステムの場合、VSSライターを使用してディスクイメージバックアップとファイルシステムバックアップを実行することができます。この方法では、バックアップ中のボリュームがロック解除されたままの状態で、他のアプリケーションからアクセスできます。これは、システムボリュームをバックアップする場合に重要です。

メディアに対するオブジェクトの分配

バックアップの構成時には、バックアップデータが最終的に記録されるメディアを指定できます。たとえば、1つのオブジェクトを特定の1つのメディアにバックアップしたり、オブジェクトごとに異なるメディアにバックアップしたりすることが可能です。

バックアップのパフォーマンスに関しては最適な分配方法であっても、復元パフォーマンスには不利に働く場合があります。バックアップのセットアップは頻繁に行う作業なので、適切なバックアップポリシーを定義することで、バックアップのセットアップを最適化する必要があります。同時に、メディア構成が復元パフォーマンスに及ぼす影響に関しては、許容できる範囲内にとどめる必要があります。

ファイルシステムスキャン

Data Protectorバックアップでは、ファイルをバックアップする前に、バックアップ対象として選択されたツリーをスキャンします。これがパフォーマンスに影響することがありますが、Windowsシステム上の高速なファイルシステムスキャンやUNIXシステム上のファイルシステムスキャン機能を使用する限り、無視できるほどの影響しか生じません。

したがって、デフォルト設定をパフォーマンス向上の目的だけで変更することはお勧めできません。

システム	ファイルシステムスキャン機能	無効化の方法
Windows	[高速ファイルシステムスキャン] (常に選択されています)	ファイルシステムスキャンは、`OB2NOTREEWALK omnirc`オプションを1に設定して無効にできます。
	[NTFSハードリンクを検出] (デフォルトでは選択されていません)	[NTFSハードリンクを検出]をオンにすると、パフォーマンスが大幅に低下します。NTFSハードリンクが実際に存在する場

		合以外は、このオプションをオンにしないでください。
UNIX	[Detect hardlinks and calculate size] (デフォルトでは選択されています)	**[POSIXハードリンクをファイルとしてバックアップ]**オプションをオンにすると、ファイルシステムスキャンが非アクティブになります。

パフォーマンスに関するさまざまなヒント

下表に示したヒントを利用することにより、バックアップまたは復元のパフォーマンスの向上を図れる場合があります。

パフォーマンスを向上させる要素	パフォーマンスの向上方法
パッチ	ネットワークのパフォーマンスに関係するすべてのパッチをインストールしておく必要があります。
デバイスがローカルであること	可能な限りローカルデバイスを使用します。
LANカード	FDDIカードには、バス上で高い優先順位を与えることができます。Media AgentシステムとDisk Agentシステムの間でFTPを使って大容量のファイルを転送し、Data Protectorのパフォーマンスと比較してください。 なお、半二重で構成したネットワークカードがあると、パフォーマンスが低下します。
高速デバイス	テープへのデータフローが低いと思われる場合や、デバイスがデータフローを適切に処理していないと思われる場合は、Media Agentクライアント上で高速デバイスをシミュレートできます。
デバイスの構成	デバイスに送信されるブロックを調整すると、パフォーマンスを向上できます。
[CRCチェック]オプション	[CRCチェック]オプションを無効にするとパフォーマンスが向上することがあります。このオプションが有効になっていると、Media AgentクライアントがCRC演算を実行するため、パフォーマンスに影響します。
ロギングとレポートレベル	IDBの更新に時間がかかりすぎる場合は、[記録しない]を設定してロギングを無効にできます。 また、[レポートレベル]を[危険域]に設定すると、メッセージにフィルターをかけることができます。
Data Protectorアプリケーションクライアント	アプリケーションクライアント(Oracle、SAP R/3)の復元セッションに時間がかかりすぎる場合は、`SmWaitforNewClient`の値を減らすことができます。デフォルト値(5分)より小さい値に設定してください。

第11章: オブジェクト集約

オブジェクト集約について

Data Protectorのオブジェクト集約機能を使用すると、1つのバックアップオブジェクトの復元チェーンを新たな集約されたバージョンのオブジェクトとしてマージできます。この機能によって、フルバックアップを実行する必要がなくなります。代わりに無制限に増分バックアップを実行し、必要に応じて復元チェーンを集約することができます。

オブジェクト集約セッション時に、Data Protectorは、ソースメディアからバックアップデータを読み取り、そのデータを集約し、結果のバージョンをターゲットメディアに書き込みます。オブジェクト集約セッションの結果、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。

オブジェクト集約の種類

オブジェクト集約セッションを対話式に開始するか、またはセッションを自動的に開始するかを指定できます。Data Protectorには、ポストバックアップのオブジェクト集約とスケジュール済みのオブジェクト集約という2種類の自動オブジェクト集約機能があります。

ポストバックアップのオブジェクト集約

ポストバックアップのオブジェクト集約は、自動オブジェクト集約仕様で指定されたバックアップセッションの完了後に実行されます。ある特定のバックアップセッションでバックアップされた自動オブジェクト集約仕様に従って、選択されたオブジェクトが集約されます。

スケジュール済みのオブジェクト集約

スケジュール済みのオブジェクト集約は、ユーザー定義のタイミングで実行されます。別のバックアップセッションでバックアップされたオブジェクトを、単独のスケジュール済みのオブジェクト集約セッションで集約できます。

オブジェクトの集約方法

最初に、オブジェクト集約仕様を作成します。この仕様では、集約するオブジェクトバージョン、使用するメディアとデバイス、およびセッションのオプションを選択します。

デバイスの選択

フルバックアップの読み取り、増分バックアップの読み取り、および合成フルバックアップの書き込み用にデバイスを分ける必要があります。あて先デバイスのブロックサイズは、ソースデバイスのブロックサイズより大きくすることができます。ただし、パフォーマンスへの影響を避けるためには、ブロックサイズが同じデバイスを用意し、それらを同じシステムに接続することをお勧めします。

セッションの開始時に使用できないデバイスは、そのセッションでは使用できません。メディアエラーが発生すると、そのセッション内では、エラーの発生したデバイスが回避されます。

オブジェクト集約のオプション

ソースオブジェクトのフィルター処理を有効にし、オブジェクト集約仕様のデータ保護、カタログ保護、およびロギングレベルを指定できます。これらのオプションのほとんどがバックアップにも使用されます。

メディアセットの選択

集約対象のオブジェクトのバージョンのコピーがさまざまなメディアセットに存在する場合は、任意のメディアセットをソースとして使用できます。デフォルトでは、Data Protectorは自動的に最も適切なメディアセットを選択します。メディアの位置の優先順位を指定すると、メディアセットの選択を制御できます。

メディアを選択するプロセス全体は、復元と同じです。オブジェクトを対話形式で集約する場合、使用するメディアセットを手動で選択することができます。オブジェクトのバックアップは後で実行されることが多いため、自動オブジェクト集約の構成時にメディアを選択することはできません。

集約されたオブジェクトの所有権

集約されたバックアップオブジェクトのオーナーは、元のバックアップオブジェクトのオーナーであり、オブジェクト集約セッションを起動したData Protectorユーザーではありません。

標準オブジェクト集約タスク

オブジェクト集約機能には、以下の前提条件と制限事項があります。

前提条件

- 集約されるすべてのバックアップが、拡張増分バックアップオプションを有効にして実行されていること。
- 集約されるすべての増分バックアップが、1つのファイルライブラリまたはB2Dデバイス(Smart Cacheを除く)内に存在すること。
- 復元チェーンが完全であること。つまり、それを構成するすべてのオブジェクトバージョンのステータスが`Completed`または`Completed/Errors`であり、これらのオブジェクトバージョンを保持するすべてのメディアが使用可能であるということです。
- 必要なバックアップデバイスが構成されていて、メディアが準備されています。
- オブジェクト集約セッションに参加するすべてのシステムに、Media Agentをインストールしておく必要があります。
- オブジェクト集約セッションを開始するための適切なユーザー権限が付与されている必要があります。バックアップの場合と同じユーザー権限が適用されます。
- 仮想フルバックアップを実行するには、すべてのバックアップ(フル、増分、および仮想フル)が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内にある必要があります。

制限事項

- あて先デバイスのブロックサイズは、ソースデバイスのブロックサイズ以上でなければなりません。
- 同じオブジェクト集約セッションで、ソースメディアとターゲットメディアに同じメディアを使用することはできません。
- ソースメディアの読み取り中、これらを復元に使用することはできません
- オブジェクト集約は、AES 256ビット暗号化を使用してバックアップされたオブジェクトには使用できません。

  オブジェクト集約はSmart Cacheを除くすべてのB2Dデバイスでサポートされます。

> **注:**
> バックアップ仕様の[ソフトウェア圧縮]または[暗号化]オプションを変更したときは常に、フルバックアップを実行してそれ以降のオブジェクト集約の基準にする必要があります。

オブジェクトを対話型に集約する

対話型集約に使用するオブジェクトは、必要に応じてオブジェクトまたはセッションの開始ポイントから選択できます。対話型オブジェクト集約仕様を保存することはできません。オブジェクト集約セッションの開始のみができます。

手順

1. コンテキストリストで**[オブジェクト操作]**をクリックします。
2. Scopingペインで、**[集約]**を展開し、**[対話型]**を展開します。
3. **[オブジェクト]**または**[セッション]**をクリックしてウィザードを起動します。
   - **[オブジェクト]**をクリックすると、オブジェクトのリストが表示されます。
   - **[セッション]**をクリックすると、オブジェクトがメディアに書き込まれたセッションのリストが表示されます。
4. 目的のオブジェクトを集約する時点を選択します。フルバックアップはそのように集約できないため、選択することができません。

   ある時点を選択すると、復元チェーン全体が選択されます。同じ時点にいくつかの復元チェーンが存在する場合は、それらすべてが選択されますが、実際にはその中の1つだけが使用されます。選択内容は青色でマークされて、復元チェーンを構成する他の増分は黒でマークされ、対応するフルバックアップは灰色でマークされます(淡色表示されます)。青いチェックマークは、集約される時点を示します。

   集約にはいくつかの時点を選択することができ、復元チェーンはオーバーラップすることがあります。すでに黒いチェックマークの付いた時点を選択すると、そのチェックマークは青色になります。

   選択した復元チェーンをクリアするには、青いチェックマークをクリックします。いくつかのオブジェクトバージョンが別の復元チェーンの一部ではない限り、復元チェーン全体がクリアされます。別の復元チェーンの一部である場合は、黒いチェックマークが付いて選択されたままの状態になります。

   [次へ]をクリックします。

5. 増分バックアップおよびフルバックアップを読み取るデバイスを指定します。

   特定のファイルライブラリまたはB2Dデバイス(Smart Cacheを除く)を増分バックアップ用の読み取りデバイスとして選択することによって、これらのライブラリまたはデバイスにオブジェクト集約を制限します。指定したデバイス内に存在するオブジェクトだけが集約されます。

   デフォルトでは、フルバックアップの読み取りデバイスは、選択されたバックアップ仕様でのバックアップに使用されるものになります。必要に応じて、これらのデバイスは変更できます。**[次へ]**をクリックします。
6. オブジェクト集約操作のあて先デバイスを選択します。Data Protectorは、ここでユーザーが指定するデバイスの中から最適のデバイスを選択します。**[次へ]**をクリックします。
7. 必要に応じてオプションを指定します。**[次へ]**をクリックします。
8. 選択したオブジェクトが含まれているメディアのリストが表示されます。

   メディアの位置の優先順位を変更すると、同じオブジェクトが複数のメディアセット内に存在する場合のメディアの選択を制御できます。

   [次へ]をクリックします。
9. 操作に使用するオブジェクトバージョンを確認します。代替復元チェーンの場合、リストされたオブジェクトバージョンの一部が実際には使用されないことがあります。**[次へ]**をクリックします。
10. 選択した時点のサマリーを確認します。特定の時点のオプションを変更するには、リストで変更対象の時点を選択し、**[プロパティ]**をクリックします。
11. **[完了]**をクリックしてウィザードを終了します。

ポストバックアップのオブジェクト集約を構成する

ポストバックアップのオブジェクト集約は、自動オブジェクト集約仕様のバックアップ仕様の名前で指定されたバックアップセッションの完了後に実行されます。指定した条件に一致する特定のバックアップセッションでバックアップされたオブジェクトが集約されます。

手順

1. コンテキストリストで**[オブジェクト操作]**をクリックします。
2. Scopingペインで、**[集約]**を展開し、**[自動]**を展開します。
3. **[ポストバックアップ]**を右クリックし、**[追加]**をクリックしてウィザードを起動します。
4. 集約するオブジェクトを含むバックアップ仕様を選択します。**[次へ]**をクリックします。
5. オブジェクト集約操作に使用するオブジェクトフィルターを指定します。**[次へ]**をクリックします。
6. 増分バックアップおよびフルバックアップを読み取るデバイスを指定します。

   特定のファイルライブラリまたはB2Dデバイス(Smart Cacheを除く)を増分バックアップ用の読み取りデバイスとして選択することによって、これらのライブラリまたはデバイスにオブジェクト集約を制限します。指定したデバイス内に存在するオブジェクトだけが集約されます。

   デフォルトでは、フルバックアップの読み取りデバイスは、選択されたバックアップ仕様でのバックアップに使用されるものになります。必要に応じて、これらのデバイスは変更できます。**[次へ]**をクリックします。
7. オブジェクト集約操作のあて先デバイスを選択します。Data Protectorは、ここでユーザーが指定す

るデバイスの中から最適のデバイスを選択します。**[次へ]**をクリックします。

8. 必要に応じてオプションを指定します。**[次へ]**をクリックします。
9. **[別名で保存...]**をクリックし、仕様の名前を入力し、**[OK]**をクリックして、ポストバックアップのオブジェクト集約仕様を保存します。

オブジェクト集約のスケジュールを設定する

スケジュール済みのオブジェクト集約は、ユーザー定義のタイミングで実行されます。指定された条件に一致するオブジェクトが集約されます。別のバックアップセッションでバックアップされたオブジェクトを、単独のスケジュール済みのオブジェクト集約セッションで集約できます。

Data Protectorでは、選択可能な復元チェーンが多数ある場合は、最新のオブジェクトバージョンを含むものが集約されます。たとえば、次のようなバックアップセッションがあるとします。フル、増分1、増分2、増分2、増分2。この場合、3つの復元チェーンが発生しますが、Data Protectorではフル、増分1、および最新の増分2からなる復元チェーンのみが集約されます。

手順

1. コンテキストリストで**[オブジェクト操作]**をクリックします。
2. Scopingペインで、**[集約]**を展開し、**[自動]**を展開します。
3. **[スケジュール済み]**を右クリックし、**[追加]**をクリックしてウィザードを起動します。
4. 集約するオブジェクトを含むバックアップ仕様を選択します。**[次へ]**をクリックします。
5. オブジェクト集約操作に使用する時間フィルターを指定します。指定の時間枠にバックアップされたオブジェクトだけが集約されます。**[次へ]**をクリックします。
6. オブジェクト集約操作に使用するオブジェクトフィルターを指定します。**[次へ]**をクリックします。
7. 増分バックアップおよびフルバックアップを読み取るデバイスを指定します。

   特定のファイルライブラリまたはB2Dデバイス(Smart Cacheを除く)を増分バックアップ用の読み取りデバイスとして選択することによって、これらのライブラリまたはデバイスにオブジェクト集約を制限します。指定したデバイス内に存在するオブジェクトだけが集約されます。

   デフォルトでは、フルバックアップの読み取りデバイスは、選択されたバックアップ仕様でのバックアップに使用されるものになります。必要に応じて、これらのデバイスは変更できます。**[次へ]**をクリックします。
8. オブジェクト集約操作のあて先デバイスを選択します。Data Protectorは、ここでユーザーが指定するデバイスの中から最適のデバイスを選択します。**[次へ]**をクリックします。
9. 必要に応じてオプションを指定します。**[次へ]**をクリックします。
10. **[保存とスケジュール...]**をクリックします。仕様の名前を入力し、**[OK]**をクリックして、スケジュール済みのオブジェクト集約仕様を保存します。仕様を保存すると、スケジュールウィザードが開きます。ウィザードに表示される手順に従って仕様をスケジュールします。

    スケジューラーを使用してData Protectorでスケジュールの作成および編集を行う方法については、「*スケジューラー、ページ 103*」を参照してください。

    > **重要:**
    > Data Protector10.00では、基本スケジューラーとアドバンストスケジューラーは終了しており、新しいWebベースのスケジューラーが用意されています。特定の日時に実行するようバック

> アップセッションをスケジュールすることで、無人バックアップを構成できます。
>
> Data Protectorのアップグレード時、すべての既存のData Protectorスケジュールは自動的に新しいスケジューラーに移行されます。

オブジェクト集約仕様をコピーする

構成して保存したオブジェクト集約仕様をコピーできます。

手順

1. コンテキストリストで**[オブジェクト操作]**をクリックします。
2. Scopingペインで、**[集約]**、**[自動]**、を展開してから、**[ポストバックアップ]**を展開します。保存されたすべてのオブジェクト集約仕様が表示されます。
3. [結果エリア]で、コピーするオブジェクト集約仕様を右クリックし、**[別名でコピー]**をクリックします。[別名でコピー]ダイアログボックスが表示されます。
4. オブジェクト集約仕様のコピーに付ける名前を[名前]テキストボックスに入力します。
5. **[OK]**をクリックします。

コピーしたオブジェクト集約仕様は、Scopingペインの[オブジェクト操作]コンテキストと[結果エリア]に新しい名前で表示されます。

第 12章： コピー

バックアップデータの複 製 について

バックアップデータの複 製 には、いくつかの利 点 があります。 データをコピーすると、データの安 全 性 や可 用 性 が向 上 し、また運 用 面 での利 便 性 も高 まります。

Data Protectorには、バックアップデータの複 製 用 に以 下 の方 法 が用 意 されています。オブジェクトコピー、オブジェクトミラー、メディアコピー、ディスクへのバックアップ(B2D)デバイス上 での複 製 。

	オブジェクトコピー	複 製	オブジェクトミラー	メディアコピー
複 製 の対 象	オブジェクト のバージョンの任 意 の組 み合 わせ(1つ以 上 のバックアップセッションより)、オブジェクトコピーセッション、またはオブジェクト集 約 セッションの	バックアップセッション、オブジェクトコピーセッション、またはオブジェクト集 約 セッションのオブジェクト セット	バックアップセッションのオブジェクトセット	メディア全 体
複 製 のタイミング	バックアップ終 了 後 の任 意 のタイミング	バックアップ終 了 後 の任 意 のタイミング	バックアップ中	バックアップ終 了 後 の任 意 のタイミング
ソースメディアとターゲットメディアのメディアの種 類	同じでなくてよい	同じ種 類 のB2Dデバイスのみに複 製 可 能	同じでなくてよい	同じでなければならない
ソースメディアとターゲットメディアのサイズ	同じでなくてよい	ターゲットデバイスに重 複 排 除 済 みデータ用 の十 分 な空 き領 域 が必 要	同じでなくてよい	同じでなければならない
ターゲットメディアを追 加 可 能 かどうか	可	不 可	可	不 可 [1]
作 成 される内 容	選 択 したオブジェ	ターゲットB2Dデ	選 択 したオブジェ	ソースメディアと同

[1] 複 製 先 に使 用 できるのは、未 フォーマット のメディア、空 のメディア、または保 護 期 限 の切 れたメディアに限 られます。 操 作 後 、ソースメディアとターゲットメディアは追 加 不 可 能 になります。

複 製 方 法 を組 み合 わせて使 用 することもできます。 たとえば、オブジェクトミラーによって作 成 されたデータのオブジェクトコピーやメディアコピーを作 成 できます。 また、オブジェクトコピーを含 むメディア全 体 をコピーすることもできます。

	クトバージョンを含むメディア	バイス上に格納された同一のコピー	クトバージョンを含むメディア	じメディア

オブジェクトコピーについて

オブジェクトコピーとは

Data Protectorには、選択し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ための、オブジェクトコピー機能が用意されています。オブジェクトバージョンは、1つまたは複数のバックアップセッション、オブジェクトコピーセッション、またはオブジェクト集約セッションから選択できます。オブジェクトコピーセッションでは、コピー元メディアから読み取られData Protectorたデータが転送されて、コピー先メディアに書き込まれます。

オブジェクトコピーセッションの結果、指定したオブジェクトバージョンのコピーを含んだメディアセットが作成されます。

以下は、オブジェクトコピー機能の概要です。

- セッションの開始

  オブジェクトコピーセッションは対話式または自動的に開始できます。
- メディアの選択

  バックアップを含んだ元のメディアセット、オブジェクトコピーを含んだメディアセット、またはメディアコピーを含んだメディアセットをソースメディアとして使用できます。

  ただし、オブジェクトコピーセッションの開始後にメディアセットを選択することはできません。マウント要求があった場合は、Data Protectorから要求された特定のメディア、または(メディアコピー機能を使って作成された)そのメディアのコピーを用意する必要があります。
- メディアの種類

  異なる種類のメディアにオブジェクトをコピーできます。また、あて先デバイスのブロックサイズをソースデバイスのブロックサイズ以上にすることもできます。
- メディアポリシー

  既にバックアップまたはオブジェクトコピーが格納されているメディアにデータを追加できます。
- 保護ポリシー

  ソースオブジェクトとオブジェクトコピーの保護期間は、独立に設定できます。

オブジェクトコピーセッションを対話式に開始するか、またはセッションの自動開始を指定することができます。

オブジェクトの自動コピー

オブジェクトの自動コピー仕様には、コピー対象のオブジェクトバージョンの選択条件を1つまたは複数指定することができます。

- バックアップ仕様 - ある特定のバックアップ仕様を使用してバックアップされたオブジェクトバージョンのみをコピーします。
- オブジェクトコピー仕様 - 特定のオブジェクトコピー仕様を使用してコピーされたオブジェクトバージョンの

みをコピーします。

- オブジェクト集約仕様 - 特定のオブジェクト集約仕様を使用して集約されたオブジェクトバージョンのみをコピーします。
- データ保護 - 保護されたオブジェクトバージョンのみをコピーします。
- 既存コピーの数 - コピー数が指定数以下であるオブジェクトバージョンのみをコピーします。
- ライブラリ - 指定ライブラリ内のメディアに存在するオブジェクトバージョンのみをコピーします。
- 時間枠(スケジュールされたオブジェクトコピー仕様においてのみ) - 指定期間内にバックアップされたオブジェクトバージョンのみをコピーします。

Data Protectorには、ポストバックアップのオブジェクトコピーとスケジュール方式のオブジェクトコピーの、2種類の自動オブジェクトコピー機能があります。

ポストバックアップのオブジェクトコピー

ポストバックアップ、およびポストバックアップオブジェクトコピーのサブセットであるポストコピーおよびポスト集約オブジェクトコピーは、自動オブジェクトコピー仕様で指定されたセッションの完了後に行われます。この場合は、その特定のバックアップセッションで作成された自動オブジェクトコピー仕様に従って、選択されているオブジェクトがコピーされます。

スケジュール設定されたオブジェクトコピー

スケジュール設定されたオブジェクトコピーは、ユーザー定義のタイミングで実行されます。さまざまなセッションからのオブジェクトを、スケジュールされた1つのオブジェクトコピーセッションにおいてコピーできます。

オブジェクトのコピー方法

最初に、オブジェクトコピー仕様を作成します。仕様では、コピーするオブジェクト、使用するメディアとデバイス、セッションオプション、およびメディア位置の優先順位(同じオブジェクトが複数のメディアセットに存在する場合、Data Protectorが選択するメディアセットがこの優先順位で決まります)を選択します。

デバイスの選択

コピー元メディアとコピー先メディアには、別々のデバイスを使用する必要があります。あて先デバイスのブロックサイズは、ソースデバイスのブロックサイズより大きくすることができます。ただし、パフォーマンスへの影響を避けるためには、ブロックサイズが同じデバイスを用意し、それらを同じシステムまたはSAN環境に接続することをお勧めします。

オブジェクトコピーは、デフォルトで負荷調整が行われます。Data Protectorは、できる限り多くのデバイスを使用して、使用可能なデバイスを最大限有効に活用します。

オブジェクトコピー仕様で使用するソースデバイスを指定しなかった場合は、Data Protectorではデフォルトのデバイスが使用されます。デフォルトでは、オブジェクトの書き込みに使用されたデバイスがソースデバイスとして使用されます。ソースデバイスは必要に応じて変更できます。オブジェクトごとにあて先デバイスが指定されていない場合は、オブジェクトコピー仕様で選択されているデバイスかData Protectorら最適なデバイスが自動的に選択されます。

各デバイスはセッションの開始時にロックされます。セッションを開始した後にデバイスをロックすることはできません。そのため、開始時に使用不能であったデバイスは、そのセッションでは使用できません。メディアエラーが発生すると、そのコピーセッション内では、エラーの発生したデバイスが回避されます。

オブジェクトコピーのオプション

ソースオブジェクトのフィルター処理を有効にし、オブジェクトコピー仕様中のオブジェクトコピーに対するデータ保護、カタログ保護、およびロギングレベルを指定できます。これらのオプションのほとんどがバックアップにも使用されます。

ポリシーによって、バックアップオブジェクトとコピーに同じオプション値が指定される場合と、別のオプション値が指定される場合があります。たとえば、バックアップのパフォーマンスを高めるため、バックアップオブジェクトに**[記録しない]**を指定し、以降のオブジェクトコピーセッションでは同じオブジェクトに対して**[すべてログに記録]**を指定できます。

バックアップオブジェクトと同一のコピーを作成するには、オブジェクトコピーに同じログレベルを指定します。オブジェクトコピーのロギングレベルが[記録しない]より高い場合、IDBのサイズに影響するため、注意してください。

コピー元のメディアセットの選択

コピー対象のオブジェクトバージョンが、Data Protectorのデータ複製方法で作成された複数のメディアセットに存在する場合、そのメディアセットはコピー元として使用できます。Data Protectorのデフォルトでは、使用するメディアセットが自動的に選択されます。メディアの位置の優先順位を指定すると、メディアセットの選択を制御できます。

メディアを選択するプロセス全体は、復元と同じです。オブジェクトを対話式にコピーする場合、開始ポイントが[オブジェクト]または[セッション]であれば、コピー元のメディアセットを手動で選択できます。オブジェクトのバックアップは後で実行されることが多いため、自動オブジェクトコピーの構成時にメディアを選択することはできません。

オブジェクトコピーの完了ステータス

オブジェクトのコピー

オブジェクトが格納されているすべてのメディアがIDBにログとして記録されている場合、ステータスが[Completed]または[Completed/Errors]のオブジェクトをコピーできます。コピー操作が成功した場合、コピーしたオブジェクトのステータスは対応するバックアップオブジェクトのステータスと同じになります。

オブジェクトコピーセッションが中止された場合、またはほかの理由で失敗した場合、そのようなセッションの結果となるオブジェクトコピーのステータスは[Failed]となります。ステータスが[Failed]のオブジェクトコピーを再度コピーすることはできません。そのデータ保護とカタログ保護は[None]に設定されます。

ソースオブジェクト

オブジェクトコピーセッションが失敗した場合、コピーされたソースオブジェクトは変更されません。

オブジェクトコピーセッションがエラーを出して完了した場合、正常にコピーされたソースオブジェクトのデータおよびカタログ保護は、ソースオブジェクトオプションに指定された値に設定されます。

オブジェクトコピーセッションを中止した場合、allソースオブジェクトのデータおよびカタログ保護は変更されません。この場合、コピーされたオブジェクトの保護を変更したければ、IDB内で手動で行う必要があります。

オブジェクトコピーの所有権

コピーされたバックアップオブジェクトのオーナーは、元のバックアップオブジェクトのオーナーであり、オブジェクトコピーセッションを起動したData Protectorユーザーではありません。

標準オブジェクトコピータスク

オブジェクトコピー機能には、以下の前提条件と制限事項があります。

前提条件

- オブジェクトコピーセッションに関与するすべてのシステムに、Media Agentをインストールしておく必要があります。
- Data Protectorセル内に少なくとも2つのバックアップデバイスを構成しておく必要があります。
- オブジェクトコピーセッションに使用するメディアを準備しておく必要があります。
- オブジェクトコピーセッションを実行するために適切なユーザー権限が付与されている必要があります。

制限事項

- バックアップされたオブジェクトをコピーするのに、ディスクへのZDBやNDMPバックアップの機能は使用できません。
- 1回のオブジェクトコピーセッションでは、1つのオブジェクトバージョンの複数のコピーは作成できません。
- あて先デバイスのブロックサイズは、ソースデバイスのブロックサイズ以上でなければなりません。
- 同じオブジェクトコピーセッションで、ソースメディアとターゲットメディアに同じメディアを使用することはできません。
- オブジェクトのコピー中は、ソースとして使用しているメディアを復元に使用できません。
- SAP MaxDB、DB2 UDB、SQL用の統合オブジェクトは逆多重化できません。
- ウィザードの最後のページから対話式で実行されたセッション中にバックアップ、コピー、または集約されたオブジェクトをコピーすることはできません。
- 同じオブジェクトコピー仕様から2つ以上のオブジェクトコピーセッションを並行して開始することはできません。

重要:
以下の点に注意してください。

- Data Protector SAP MaxDB、DB2 UDB、およびMicrosoft SQL Serverの統合は、相互に依存したデータストリームです。そのため、オブジェクトコピー操作では、メディア上のオブジェクトのレイアウトが、復元できるよう維持されなければなりません。このために、コピーする際にはこれらの統合ソフトウェアのすべてのオブジェクトを同じバックアップIDで選択します。そうしなければ、コピーからの復元ができなくなります。
- SAP MaxDB、DB2 UDB、Microsoft SQL Serverの統合オブジェクトのコピー操作に必要なデバイスの最小数は、バックアップに使用されるデバイスの数と同じです。これらのオブジェクトの

バックアップとコピーに使用されるデバイスの同時処理数は同じでなければなりません。

- [コピーが正常に実行された後でデータとカタログ保護を変更]オプションを、ディスク+テープへのZDBセッションからオブジェクトをコピーする際に選択した場合、指定した期間が過ぎると、ソースオブジェクトが上書きされる可能性があることに注意してください。メディアが上書きされると、GUIを使用したこのバックアップからのインスタントリカバリは実行できなくなります。
- オブジェクトコピーセッションを中止した場合、すべてのソースオブジェクトのデータおよびカタログ保護は変更されません。この場合、コピーされたオブジェクトの保護を変更したければ、IDB内で手動で行う必要があります。

オブジェクトを対話式にコピーする

オブジェクトがバックアップされた後、そのオブジェクトを新しいメディアセットにコピーできます。

必要に応じて、メディア、オブジェクト、またはセッションの開始ポイントから対話型コピーのオブジェクトを選択できます。対話型オブジェクトコピー仕様を保存することはできません。オブジェクトコピーセッションを開始することのみです。

手順

1. コンテキストリストで**[オブジェクト操作]**をクリックします。
2. Scopingペインで、**[コピー]**、**[オブジェクトコピー]**、**[対話型]**を順に展開します。
3. **[メディア]**、**[オブジェクト]**、または**[セッション]**をクリックしてウィザードを起動します。
   - **[メディア]**をクリックすると、メディアプールとメディアのリストが表示されます。
   - **[オブジェクト]**をクリックすると、ファイルシステムやデータベースなど、バックアップデータの種類のリストが表示されます。
   - **[セッション]**をクリックすると、オブジェクトがメディアに書き込まれたセッションのリストが表示されます。
4. コピー対象のオブジェクトを選択します。

   前の手順で[セッション]を選択した場合、統合オブジェクトを右クリックし、**[バックアップセットを選択]**をクリックすると、同じバックアップIDを持つすべての統合オブジェクトを選択できます。

   > **注:**
   > VMwareバックアップ用のData Protector 10.00以降からは、仮想マシンディスクは並行して実行されるオブジェクトとして見なされます。メディアに戻された仮想マシンディスクを把握するために、仮想マシンのディスクオブジェクトは**[メディア]**リストに一覧されますが無効化されています。コピーまたは検証操作は仮想マシンオブジェクトに対して実行され、それに関連するすべてのディスクオブジェクトは内部と見なされます。
   >
   > VMware統合用のData Protector 10.00以降からは、**[次へ]**オプションは、**[メディア]**リストで仮想マシンオブジェクトを選択した後にのみ有効になります。

   [次へ]をクリックします。
5. デフォルトでは、選択したオブジェクトの書き込みに使用されるデバイスがオブジェクトコピー操作のソースデバイスとして使用されます。必要に応じて、このページでソースデバイスを変更できます。元のデバイスを選択し、**[変更]**をクリックします。新しいデバイスの名前が[デバイスのステータス]の下に表示されます。新しいデバイスは、このセッションでのみ使用されます。

デバイスに関する詳細を表示するには、デバイスを右クリックして**[情報]**を選択します。

選択したデバイスを(無効または使用中などの理由で)オブジェクトコピーに使用できない場合のData Protectorでの処理を指定します。[デバイスの自動選択]または[元のデバイスの選択]を選択します。

[次へ]をクリックします。

6. オブジェクトコピー操作のあて先デバイスを選択します。

   [サマリー]ページのオブジェクトごとに、ここで指定したデバイスのリストからデバイスを指定できます。オブジェクトごとにデバイスを指定しない場合は、リストから最も適したデバイスが選択されます。Data Protector

   [次へ]をクリックします。

7. 必要に応じて、ソースオブジェクトオプション、ターゲットオブジェクトオプション、およびターゲットメディアオプションを指定します。**[次へ]**をクリックします。

   必要に応じて、コピーの代わりに2つのB2Dデバイス間での複製を有効にするには、[複製を使用]を選択します。[複製を使用]を選択すると、[外部セルに複製]が有効になります。

8. 選択したオブジェクトが含まれているメディアのリストが表示されます。

   開始ポイントが[オブジェクト]または[セッション]の場合は、メディア位置の優先順位のリストも表示されます。メディアの位置の優先順位を変更すると、同じオブジェクトが複数のメディアセット内に存在する場合のメディアの選択を制御できます。

   [次へ]をクリックします。

9. 選択したオブジェクトのサマリーを確認します。特定のオブジェクトのオプションを変更するには、リストで変更対象のオブジェクトを選択し、**[プロパティ]**をクリックします。

   ソースオブジェクトオプション、ターゲットオブジェクトオプション、およびあて先デバイスを指定できます。[オブジェクト]または[セッション]の開始ポイントが使用されている場合、複数のコピーが存在する場合に使用するオブジェクトバージョンのコピーを手動で選択できます。

10. **[完了]**をクリックし、コピーセッションを開始します。

ポストバックアップのオブジェクトコピーを構成する

ポストバックアップのオブジェクトコピーは、自動オブジェクトコピー仕様のバックアップ、オブジェクトコピー、またはオブジェクト集約仕様の名前で指定されたバックアップセッション、オブジェクトコピーセッション、またはオブジェクト集約セッションの完了後に実行されます。コピーされるのは、指定された条件に一致するセッションのオブジェクトです。

バックアップセッションが失敗した場合は、ポストバックアップのオブジェクトコピーのセッションは開始しません。バックアップセッションが中止され、バックアップセッションに完了したオブジェクトが含まれる場合、デフォルトでは、完了したオブジェクトがポストバックアップのオブジェクトコピーセッションでコピーされます。中止されたセッションのコピーを無効にするには、グローバルオプション`CopyStartPostBackupOnAbortedSession`を0に設定します。

手順

1. コンテキストリストで**[オブジェクト操作]**をクリックします。
2. Scopingペインで、**[コピー]**、**[オブジェクトコピー]**、**[自動]**を順に展開します。
3. **[ポストバックアップ]**を右クリックし、**[追加]**をクリックしてウィザードを起動します。

4. コピーしたいオブジェクトを含むバックアップ、オブジェクトコピー、またはオブジェクト集約仕様を選択します。**[次へ]**をクリックします。
5. オブジェクトコピー操作に使用するオブジェクトフィルターを指定します。指定した条件に一致するオブジェクトだけがコピーされます。**[次へ]**をクリックします。
6. オブジェクトコピー操作に使用するライブラリフィルターを指定します。指定したライブラリ内のメディアに存在するオブジェクトだけがコピーされます。**[次へ]**をクリックします。
7. デフォルトでは、選択したバックアップ仕様でバックアップ用に使用されるデバイスがオブジェクトコピー操作のソースデバイスとして使用されます。必要に応じて、このページでソースデバイスを変更できます。**[次へ]**をクリックします。
8. オブジェクトコピー操作のあて先デバイスを選択します。Data Protectorは、ここでユーザーが指定するデバイスの中から最適のデバイスを選択します。**[次へ]**をクリックします。
9. 必要に応じて、ソースオブジェクトオプション、ターゲットオブジェクトオプション、およびターゲットメディアオプションを指定します。**[次へ]**をクリックします。

   必要に応じて、コピーの代わりに2つのB2Dデバイス間での複製を有効にするには、[複製を使用]を選択します。
10. **[別名で保存...]**をクリックし、仕様の名前を入力し、**[OK]**をクリックして、ポストバックアップのオブジェクトコピー仕様を保存します。

オブジェクトコピーのスケジュールを設定する

スケジュール済みのオブジェクトコピーは、ユーザー定義のタイミングで実行されます。さまざまなバックアップセッション、オブジェクトコピーセッション、またはオブジェクト集約セッションのオブジェクトを、スケジュールされた1つのオブジェクトコピーセッションでコピーできます。

> **ヒント:**
> Webベースのスケジューラーで、詳細設定を使用したオブジェクトコピーセッションをスケジュール設定することもできます。コンテキストリストでスケジューラーにアクセスするには、**ホーム**をクリックし、左ペインで**スケジューラー**をクリックします。

手順

1. コンテキストリストで**[オブジェクト操作]**をクリックします。
2. Scopingペインで、**[コピー]**、**[オブジェクトコピー]**、**[自動]**を順に展開します。
3. **[スケジュール済み]**を右クリックし、**[追加]**をクリックしてウィザードを起動します。
4. コピーしたいオブジェクトを含むバックアップ、オブジェクトコピー、またはオブジェクト集約仕様を選択します。

   バックアップ仕様は、バックアップグループごとに表示することもできます。これにより、バックアップグループに対してバックアップ仕様を追加または削除した場合、オブジェクトコピー機能はその変更を自動的に認識するので、オブジェクトコピー仕様を手動で変更する必要はありません。

   グループビューからその他のビューに変更した場合、ビューを変更すると現在の選択がすべて解除されるという警告メッセージが表示されます。続行すると、それまでの選択はすべてクリアされます。

   [次へ]をクリックします。
5. オブジェクトコピー操作に使用するオブジェクトフィルターを指定します。指定した条件に一致するオブジェクトだけがコピーされます。**[次へ]**をクリックします。

6. オブジェクトコピー操作に使用するライブラリフィルターを指定します。指定したライブラリ内のメディアに存在するオブジェクトだけがコピーされます。**[次へ]**をクリックします。
7. デフォルトでは、選択したバックアップ仕様でバックアップ用に使用されるデバイスがオブジェクトコピー操作のソースデバイスとして使用されます。必要に応じて、このページでソースデバイスを変更できます。**[次へ]**をクリックします。
8. オブジェクトコピー操作のあて先デバイスを選択します。Data Protectorは、ここでユーザーが指定するデバイスの中から最適のデバイスを選択します。**[次へ]**をクリックします。
9. 必要に応じて、ソースオブジェクトオプション、ターゲットオブジェクトオプション、およびターゲットメディアオプションを指定します。**[次へ]**をクリックします。

   必要に応じて、コピーの代わりに2つのB2Dデバイス間での複製を有効にするには、[複製を使用]を選択します。
10. **[保存とスケジュール...]**をクリックします。仕様の名前を入力し、**[OK]**をクリックして、スケジュール済みのオブジェクトコピー仕様を保存します。仕様を保存すると、スケジュールウィザードが開きます。ウィザードに表示される手順に従って仕様をスケジュールします。

    スケジューラーを使用してData Protectorでスケジュールの作成および編集を行う方法については、「*スケジューラー、ページ 103*」を参照してください。

失敗したオブジェクトコピーセッションを再開する

ネットワーク接続の問題またはシステムの非可用性のため、オブジェクトコピーセッション中に一部のオブジェクトが失敗する可能性があります。障害を解決した後、問題のセッションを再開できます。この操作では、失敗したオブジェクトのみ再開されます。

前提条件

- Data Protector Admin ユーザーグループに追加されているか、Data Protectorモニターユーザー権限が付与されていることが必要です。

制限事項

- 対話式で実行されていたセッションが失敗した場合、未保存のオブジェクトコピー仕様に基づくことになり、セッションを再開することはできません。
- 一度に複数のセッションを再開することはできません。

> **重要:**
> 失敗したオブジェクトコピーセッションを再開する前に、オブジェクトコピー仕様を変更しないでください。変更すると、すべてのオブジェクトを再開できなくなります。

手順

1. 通常のCell Managerを使用している場合、コンテキストリストで**[内部データベース]**をクリックします。

   Manager-of-Managersを使用している場合は、コンテキストリストで**[クライアント]**を選択し、**[エンタープライズクライアント]**を展開します。問題のセッションのCell Managerを選択します。[ツール]メニューの**[データベース管理]**を選択します。新しいData Protector GUIウィンドウに、[内部データベース]コンテキストが表示されます。

2. Scopingペインで**[内部データベース]**を展開し、**[セッション]**をクリックします。

   [結果エリア]に、セッションのリストが表示されます。各セッションのステータスが[ステータス]列に示されます。
3. 失敗したセッション、中止したセッション、または失敗やエラーで終了したセッションを右クリックし、**[失敗したオブジェクトの再開]**を選択し、失敗したオブジェクトをコピーします。
4. **[はい]**をクリックして処理を実行します。

オブジェクトコピー仕様をコピーする

構成して保存したオブジェクトコピー仕様をコピーできます。

手順

1. コンテキストリストで**[オブジェクト操作]**をクリックします。
2. Scopingペインで、**[コピー]**、**[オブジェクトコピー]**、**[自動]**を展開してから、**[ポストバックアップ]**を展開します。保存されたすべてのオブジェクトコピー仕様が表示されます。
3. [結果エリア]で、コピーするオブジェクトコピー仕様を右クリックし、**[別名でコピー]**をクリックします。[別名でコピー]ダイアログボックスが表示されます。
4. オブジェクトコピー仕様のコピーに付ける名前を[名前]テキストボックスに入力します。
5. **[OK]**をクリックします。

コピーしたオブジェクトコピー仕様は、Scopingペインの[オブジェクト操作]コンテキストと[結果エリア]に新しい名前で表示されます。

拡張オブジェクトコピータスク

以下のような目的で、バックアップデータの追加コピーを作成します。

- ボールティング

  バックアップ、コピー、または集約されたオブジェクトのコピーを作成し、それらを複数の場所に保管できます。
- メディアの解放

  メディア上の保護されたオブジェクトバージョンだけを保管するために、保護されたオブジェクトバージョンをコピーし、メディアを上書きできるようにしておくことができます。
- メディアの逆多重化

  オブジェクトをコピーして、インターリーブされたデータを削減できます。
- 復元チェーンの集約

  復元に必要なすべてのオブジェクトバージョンを1つのメディアセットにコピーできます。
- 別の種類のメディアへの移動

  異なる種類のメディアにバックアップをコピーできます。
- 拡張バックアップの概念のサポート

  ディスクステージングなどのバックアップ概念を使用できます。

メディアを解放する

メディアには、保護期間が異なるバックアップされたオブジェクトが含まれることがあります。保護されたオブジェクトは、少量のメディアスペースしか消費しないこともあります。しかし、そのようなメディアも、すべてのオブジェクトの保護の期限が切れるまで、これらのメディアを再使用することはできません。

メディアを効率的に使用するために、オブジェクトコピー機能を使用して、保護されたオブジェクトがいくつか格納されているだけのメディアを解放することができます。保護されたオブジェクトは、新しいメディアセットにコピーされ、メディアが再使用可能になります。失敗したオブジェクトからメディアを解放することもできます。このようなオブジェクトは、オブジェクトコピーセッションではコピーされません。

手順

1. コンテキストリストで**[オブジェクト操作]**をクリックします。
2. Scopingペインで、**[コピー]**、**[オブジェクトコピー]**、**[対話型]**を順に展開します。
3. **[メディア]**をクリックしてウィザードを起動します。
4. [オブジェクト]ページで、[保護されたオブジェクトだけ選択可能にする]を選択します。メディアプールを展開して、解放するメディアを選択します。**[次へ]**をクリックします。
5. デフォルトでは、選択したオブジェクトの書き込みに使用されるデバイスがオブジェクトコピー操作のソースデバイスとして使用されます。必要に応じて、このページでソースデバイスを変更できます。**[次へ]**をクリックします。
6. オブジェクトコピー操作のあて先デバイスを選択します。

   [サマリー]ページのオブジェクトごとに、ここで指定したデバイスのリストからデバイスを指定できます。オブジェクトごとにデバイスを指定しない場合は、リストから最も適したデバイスが選択されます。

   [次へ]をクリックします。
7. [オプション]ページの[ソースオブジェクトオプション]の下で、[コピーが正常に実行された後でデータとカタログ保護を変更]を選択して、コピーされたソースオブジェクトの保護を解放します。[コピーが正常に実行された後で、失敗したソースオブジェクトのデータとカタログ保護をリサイクル]を選択して、失敗したソースオブジェクトの保護を解放します(これらのオブジェクトはコピーされません)。必要に応じて、他のオプションを指定します。**[次へ]**をクリックします。
8. 選択したオブジェクトが含まれているメディアのリストが表示されます。**[次へ]**をクリックします。
9. 選択したオブジェクトのサマリーを確認します。特定のオブジェクトのオプションを変更するには、リストで変更対象のオブジェクトを選択し、**[プロパティ]**をクリックします。ソースオブジェクトオプション、ターゲットオブジェクトオプション、およびあて先デバイスを指定できます。
10. **[完了]**をクリックし、コピーセッションを開始します。

メディアを逆多重化する

多重化メディアには、複数のオブジェクトが含まれます。バックアップセッションのデバイス同時処理数に1より大きい値を設定すると、このように多重化されたメディアが生成されます。多重化メディアでは、バックアップデータの機密性が低下する可能性があるほか、復元にも時間がかかります。

オブジェクトコピーの機能を使用すると、メディアを逆多重化できます。多重化されたメディアのオブジェクトは、複数のメディアにコピーされます。

制限事項

Data Protectorが実行するソースメディアの読み取りは1回だけです。メディア上のすべてのオブジェクトの逆多重化を有効にする場合、操作に必要なあて先デバイスの最小数はオブジェクトの書き込みに使用されたデバイスの同時処理数と同じになります。使用可能なデバイス数がこれより少ない場合、いくつかのオブジェクトがターゲットメディア上で多重化されたままになります。

手順

1. コンテキストリストで**[オブジェクト操作]**をクリックします。
2. Scopingペインで、**[コピー]**、**[オブジェクトコピー]**、**[対話型]**を順に展開します。
3. **[セッション]**をクリックしてウィザードを起動します。
4. 必要なセッションを展開し、コピーするオブジェクトを選択します。**[次へ]**をクリックします。
5. 逆多重化操作によって通常のバックアップ用に構成されたデバイスを占有しない場合、および逆多重化操作でデータを読み取るデバイスを1つしか使用しない場合は、以下の手順を実行します。

   ソースデバイスを単一デバイスにマッピングします。

   > **重要:**
   > ソースデバイスとしてスタンドアロンファイルデバイスを使用した場合は、この手順をスキップします。ソースデバイスとしてファイルジュークボックスデバイスまたはファイルライブラリデバイスを使用した場合は、ソースデバイスを同じファイルジュークボックスまたはファイルライブラリ内のデバイスにマッピングしてください。

   各デバイスを右クリックし、**[デバイスの変更]**をクリックします。新しいデバイスを選択し、**[OK]**をクリックします。
6. **[次へ]**をクリックします。
7. オブジェクトコピー操作のあて先デバイスを選択します。必要なデバイスの数は、オブジェクトの書き込み時に使用されたデバイスの同時処理数によって異なります。

   選択した各ドライブを右クリックし、**[プロパティ]**をクリックします。**[同時処理数]**オプションを1に設定します。**[OK]**をクリックします。

   [サマリー]ページのオブジェクトごとに、ここで指定したデバイスのリストからデバイスを指定できます。オブジェクトごとにデバイスを指定しない場合は、リストから最も適したデバイスが選択されます。Data Protector

   [次へ]をクリックします。
8. 必要に応じて、ソースオブジェクトオプション、ターゲットオブジェクトオプション、およびターゲットメディアオプションを指定します。**[次へ]**をクリックします。
9. 選択したオブジェクトが含まれているメディアのリストが表示されます。

   メディアの位置の優先順位を変更すると、同じオブジェクトが複数のメディアセット内に存在する場合のメディアの選択を制御できます。

   [次へ]をクリックします。
10. 選択したオブジェクトのサマリーを確認します。特定のオブジェクトのオプションを変更するには、リストで変更対象のオブジェクトを選択し、**[プロパティ]**をクリックします。

ソースオブジェクトオプション、ターゲットオブジェクトオプション、およびあて先デバイスを指定できます。また、複数のコピーが存在する場合に使用するオブジェクトバージョンのコピーを手動で選択できます。

11. **[完了]**をクリックし、コピーセッションを開始します。

復元チェーンを集約する

オブジェクトコピーの機能を使用すると、オブジェクトバージョンの復元チェーンを新しいメディアセットにコピーできます。このようなメディアセットを使用すると、複数のメディアをロードしたり、必要なオブジェクトバージョンをシークしたりする必要がないため、すばやく、効率的に復元を実行できます。

> **注:**
> Data Protectorには、オブジェクト集約というさらに強力な機能もあります。オブジェクトコピーでは復元チェーンのすべてのバックアップをシーケンスにコピーできるのに対して、オブジェクト集約ではバックアップを新しいオブジェクトバージョンにマージできます。これを合成フルバックアップといいます。

制限事項

統合オブジェクトでは、復元チェーンを選択できません。

手順

1. コンテキストリストで**[オブジェクト操作]**をクリックします。
2. Scopingペインで、**[コピー]**、**[オブジェクトコピー]**、**[対話型]**を順に展開します。
3. **[オブジェクト]**をクリックしてウィザードを起動します。
4. [オブジェクト]ページでデータの種類を展開し、次にクライアントと論理ディスク、またはマウントポイントを展開して、オブジェクトバージョンを表示します。コピーするオブジェクトを右クリックして、**[復元チェーンを選択]**をクリックします。**[次へ]**をクリックします。
5. デフォルトでは、選択したオブジェクトの書き込みに使用されるデバイスがオブジェクトコピー操作のソースデバイスとして使用されます。必要に応じて、このページでソースデバイスを変更できます。**[次へ]**をクリックします。
6. オブジェクトコピー操作のあて先デバイスを選択します。

   [サマリー]ページのオブジェクトごとに、ここで指定したデバイスのリストからデバイスを指定できます。オブジェクトごとにデバイスを指定しない場合は、リストから最も適したデバイスが選択されます。Data Protector

   [次へ]をクリックします。
7. 必要に応じて、ソースオブジェクトオプション、ターゲットオブジェクトオプション、およびターゲットメディアオプションを指定します。**[次へ]**をクリックします。
8. 選択したオブジェクトが含まれているメディアのリストが表示されます。

   メディアの位置の優先順位を変更すると、同じオブジェクトが複数のメディアセット内に存在する場合のメディアの選択を制御できます。

   [次へ]をクリックします。
9. 選択したオブジェクトのサマリーを確認します。特定のオブジェクトのオプションを変更するには、リストで変更対象のオブジェクトを選択し、**[プロパティ]**をクリックします。

ソースオブジェクトオプション、ターゲットオブジェクトオプション、およびあて先デバイスを指定できます。また、複数のコピーが存在する場合に使用するオブジェクトバージョンのコピーを手動で選択できます。

10. **[完了]**をクリックし、コピーセッションを開始します。

別のメディアの種類に移行する

オブジェクトコピー機能を使用して、バックアップしたデータを、ブロックサイズが同じかまたは大きい別のメディアの種類に移行できます。

手順

1. コンテキストリストで**[オブジェクト操作]**をクリックします。
2. Scopingペインで、**[コピー]**、**[オブジェクトコピー]**、**[対話型]**を順に展開します。
3. **[メディア]**をクリックしてウィザードを起動します。
4. コピーするオブジェクトを選択し、**[次へ]**をクリックします。
5. デフォルトでは、選択したオブジェクトの書き込みに使用されるデバイスがオブジェクトコピー操作のソースデバイスとして使用されます。必要に応じて、このページでソースデバイスを変更できます。**[次へ]**をクリックします。
6. オブジェクトコピー操作のあて先デバイスを選択します。

   [サマリー]ページのオブジェクトごとに、ここで指定したデバイスのリストからデバイスを指定できます。オブジェクトごとにデバイスを指定しない場合は、リストから最も適したデバイスが選択されます。Data Protector

   [次へ]をクリックします。
7. 必要に応じて、ソースオブジェクトオプション、ターゲットオブジェクトオプション、およびターゲットメディアオプションを指定します。**[次へ]**をクリックします。
8. 選択したオブジェクトが含まれているメディアのリストが表示されます。**[次へ]**をクリックします。
9. 選択したオブジェクトのサマリーを確認します。特定のオブジェクトのオプションを変更するには、リストで変更対象のオブジェクトを選択し、**[プロパティ]**をクリックします。

   ソースオブジェクトオプション、ターゲットオブジェクトオプション、およびあて先デバイスを指定できます。
10. **[完了]**をクリックし、コピーセッションを開始します。

ディスクステージングについて

ディスクステージングとは

ディスクステージングのコンセプトは、複数の段階(ステージ)に分けてデータをバックアップすることです。バックアップステージは、ある種類のメディアにデータをバックアップし、その後、そのデータを別の種類のメディアにコピーするという操作で構成されています。この機能は一般的に次のように使用されます。

1. 最初の段階では、高性能でアクセスも容易ではあるが容量に限りがあるメディア(システムディスクなど)にデータをバックアップします。通常バックアップしたデータは、高速な復元が必要になる可能性が最も高いバックアップ後の一定期間のみ、アクセスが容易なこれらのメディア上に保管しておきます。

2. 一定の期間が経過した後、データは、オブジェクトコピー機能を使って、パフォーマンスとアクセシビリティは低いが大容量の保存用メディアに移動されます。

このようなディスクステージングは、この目的専用に構成されたスケジュール済みオブジェクトコピー仕様を使って実現できます。

別の手段として、次のような方法もあります。

1. パフォーマンスが高いメディアにデータをバックアップするバックアップ仕様を作成し、復元能力が必要とされる全期間にわたる保護を設定します。
2. バックアップしたデータをパフォーマンスが低いメディアにコピーする自動的なポストバックアップのコピー仕様を作成し、元のバックアップの維持期間を、高速復元能力が必要なクリティカルな期間に設定し直します。デフォルトでは、2番目のコピーは元のバックアップ仕様に指定された保護期間の間維持されます。

この方法では、クリティカルな期間中に2つのコピーが存在するため、セキュリティが高まります。

ディスクステージングを実行する理由

ディスクステージングのコンセプトを使用すると、以下の利点があります。

- バックアップと復元のパフォーマンスが向上します。
- バックアップデータの保存コストが低減されます。
- 復元のためのデータの可用性が向上します。

ディスクステージングと小規模バックアップの繰り返し

ディスクステージングを使用すると、テープに小さい多数のオブジェクトを頻繁にバックアップする必要がなくなります。このようなバックアップは、メディアが頻繁にロードまたはアンロードされるため、効率がよくありません。ディスクステージングを使用すると、バックアップ時間を短縮でき、メディアの劣化を防止できます。

オブジェクト操作セッションのトラブルシューティング

オブジェクトコピーに関する問題

コピーされたオブジェクトの数が想定された数より少ない

問題
ポストバックアップのオブジェクトコピーまたはスケジュール済みのオブジェクトコピーでは、選択したフィルターに一致するオブジェクトの数が実際にコピーされるオブジェクトの数よりも多くなります。 以下のメッセージが表示されます。 `Too many objects match specified filters.`
対処方法
• オブジェクトバージョンの選択条件を絞り込みます。

- グローバルオプションファイル内のCopyAutomatedMaxObjects変数の値を大きくして、同一セッション内でコピーされるオブジェクトの最大数を増やします。

選択したライブラリ内の一部のオブジェクトしかコピーされない

問題
ポストバックアップのオブジェクトコピーまたはスケジュール済みのオブジェクトコピーで、選択したライブラリ内のメディアに格納されている一部のオブジェクトがコピーされません。この問題は、選択したライブラリにオブジェクトの完全なメディアセットが存在しない場合に発生します。
対処方法
選択したライブラリに不足しているメディアを挿入するか、これらのオブジェクトの完全なメディアセットが存在するライブラリを選択します。

追加のメディアに対するマウント要求が発行される

問題
[メディア]開始ポイントからの対話型オブジェクトコピーセッションで、特定のメディアを選択しました。これにより、追加メディアのマウント要求が発行されます。この現象は、メディア上のオブジェクトが他のメディアにまたがっている場合に発生します。
対処方法
必要なメディアをデバイスに挿入し、マウント要求を確認します。

オブジェクトコピーを作成したときに、保護の終了時間が延長される

問題
オブジェクトコピーを作成したときに、元のオブジェクトから保護の終了時間が継承されません。保護期間はコピーされますが、開始時間が、オブジェクトの作成時間ではなく、オブジェクトコピーの作成時間に設定されます。その結果、元のオブジェクトより保護期間が延長されます。元のバックアップが作成されてからオブジェクトコピーセッションを行うまでの時間が長いほど、保護終了時間の差は大きくなります。 たとえば、オブジェクトを9月5日に作成し、保護期間を14日間に設定した場合、保護期間は9月19日に期限切れとなります。オブジェクトコピーセッションを9月10日に開始した場合、オブジェクトコピー保護期間は9月24日に期限切れとなります。 場合によっては、このような動作は望ましくなく、保護の終了時間を維持しなければならないこともあります。
対処方法
グローバルオプションCopyDataProtectionEndtimeEqualToBackupを1に設定すると、オブジェクトコピー保護の終了時間がバックアップのオブジェクト保護の終了時間に等しくなります。このオプションは、デフォルトでは0に設定されています。許容されるファイルの最大数を増やします。

複数のオブジェクトを含むセッションを複製すると、応答が停止する

問題

別のデバイスにセッションを複製しようとすると、セッションが応答を停止します。セッションの出力には、以下の情報が含まれます。
`[Normal] From: BMA@company.com "d2d1_1_gw1 [GW 26177:1:15198446278003495809]" Time: 3/21/2013 9:13:06 AM`
`COMPLETED Media Agent "d2d1_1_gw1 [GW 26177:1:15198446278003495809]"`
問題は、デュアルIPスタックネットワーク構成でHP-UX Media Agentを使用する場合に発生します。

対処方法

デュアルIPスタックネットワークで、Media Agentクライアント上の`/etc/hosts`ファイルに、IPv6 localhostアドレスの独立したエントリを追加します。
たとえば、`hosts`ファイルに以下のエントリが存在する場合を考えます。
`::1 localhost loopback`
問題を解決するには、IPv6アドレス用に以下の行を追加します。
`::1 ipv6-localhost ipv6-loopback`

データドメインブーストデバイス上の複製セッションが再試行期間中に中止操作に応答できない

問題
あるデータドメインブーストバックアップデバイスから別のデバイスにセッションを複製しているときに、デバイスに利用可能なストリームが十分にないと、複製セッションが再試行期間中に中止操作に応答できません。
対処方法
この問題は、`omnirc DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMIT`が`0`(サポートされていません)に設定されている場合に発生することがわかっています。 この変数は、データドメインブーストデバイスに利用可能なストリームが十分にない場合、複製セッションが再試行を開始するまでに待機する間隔を定義します。この間隔が大きすぎたり、`0`に設定されたりしている場合、セッションが中止操作に応答できません。 `DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMIT`のデフォルト値は60秒です。 `DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMIT`の詳細な説明については、`omnirc`ファイルを参照してください。

オブジェクト集約に関する問題

多くの時点のオブジェクト集約を行うと、上限を超える数のファイルが開かれる

問題

多くの時点のオブジェクト集約操作を開始した場合、Data Protectorは操作を実行するために必要なすべてのメディアを読み取ります。この場合、すべてのファイルが同時に開かれます。Data Protectorが開いたファイルの数が、オペレーティングシステムで許容される上限を超えた場合、次のようなメッセージが表示されます。
`|Major| From: RMA@computer.company.com "AFL1_ConsolidateConc2_bs128" Time: time /omni/temp/Cons_Media/AFL1/`
`0a1109ab54417fab351d15500c6.fd`
`Cannot open device ([24] Too many open files)`

対処方法

許容されるファイルの最大数を増やします。
HP-UXシステムの場合:
1. System Administration Manager (SAM)を使用して、開けるファイルの最大数を設定します:
a. **[カーネル構成]**→**[構成可能パラメーター]**を選択し、次に、**[アクション]**→**[構成可能パラメーターの変更]**を選択します。
b. **formula/value**フィールドに**maxfiles_lim**と**maxfiles**の新しい値を入力します。
2. 新しい値を適用した後、コンピューターを再起動します。
Solarisシステムの場合:
1. `/etc/system`ファイルを編集して、開けるファイルの最大数を設定します: 以下の行を追加します。
`set rlim_fd_cur=value`
`set rlim_fd_max=value`
2. 新しい値を適用した後、コンピューターを再起動します。

B2Dデバイスへのオブジェクト集約が2回目の試行で失敗した

問題
最初のオブジェクトの集約後に増分バックアップを実行し、2回目のオブジェクト集約を実行すると、操作が失敗します。
対処方法
2回目の集約を正常に完了させるには、最初のオブジェクト集約を実行した後にフルバックアップを実行します。その後、増分バックアップを実行して、後で集約できるようにします。

複製について

Data Protectorの複製機能では、Media Agentを介してデータを転送することなく、複製に対応した2つのディスクへのバックアップ(B2D)デバイス間でオブジェクトを複製することができます。バックアップセッション、オブジェクトコピーセッション、またはオブジェクト集約セッションのいずれかを選択することができます。複製セッションで、Data Protectorは、複製対象のセッションからオブジェクトを読み取り、ソースB2Dデバイスからターゲットデバイスへの複製を実行します。

複製セッションを実行すると、指定したセッションのすべてのオブジェクトがコピーされます。

以下は、複製機能の概要です。

- セッションの開始

  複製セッションは対話形式で開始することも、自動的に開始させることもできます。
- ターゲットデバイスの選択

  複製に対応したデバイスをフィルター処理して、適切なデバイスを選択することができます。
- 保護ポリシー

  ソースオブジェクトとオブジェクトコピーの保護期間は、独立に設定できます。

複製セッションを対話式に開始するか、またはセッションの自動開始を指定することができます。

自動複製

自動複製仕様では、コピー対象のオブジェクトバージョンの選択条件を1つまたは複数指定することができます。

- バックアップ仕様 - ある特定のバックアップ仕様を使用してバックアップされたオブジェクトバージョンのみをコピーします。
- オブジェクトコピー仕様 - 特定のオブジェクトコピー仕様を使用してコピーされたオブジェクトバージョンのみをコピーします。
- オブジェクト集約仕様 - 特定のオブジェクト集約仕様を使用して集約されたオブジェクトバージョンのみをコピーします。
- データ保護 - 保護されたオブジェクトバージョンのみをコピーします。
- 既存コピーの数 - コピー数が指定数以下であるオブジェクトバージョンのみをコピーします。
- ライブラリ - 指定ライブラリ内のメディアに存在するオブジェクトバージョンのみをコピーします。
- 時間枠(スケジュールされたオブジェクトコピー仕様においてのみ) - 指定期間内にバックアップされたオブジェクトバージョンのみをコピーします。

Data Protectorには、2種類の自動複製機能が用意されています。ポストバックアップ複製と、スケジュール方式の複製です。

ポストバックアップ複製

ポストバックアップ、およびポストバックアップ複製のサブセットであるポストコピーおよびポスト集約複製は、自動複製コピー仕様で指定されたセッションの完了後に行われます。その特定のバックアップセッションで作成された自動複製コピー仕様に従って選択されているオブジェクトが、コピーされます。

スケジュール設定した複製

スケジュール設定した複製は、ユーザー定義のタイミングで実行されます。さまざまなセッションからのオブジェクトを、スケジュールされた1つの複製セッションで複製できます。

制限事項

- 複製では、バックアップ、オブジェクトコピー、オブジェクト集約、またはオブジェクト複製のセッションのみを選択できます。個々のオブジェクトの選択はサポートされていません。
- ソースデバイスまたはターゲットデバイスで異なるブロックサイズを使用することはできません。
- 対話型セッションを構成する場合、一度に選択できるセッションは1つだけです。

考慮事項

- 複製はセッションベースであるため、個々のオブジェクトに対する設定は無視されます。たとえば、セッションに含まれるオブジェクトのコピーが既に複数存在している場合、Data Protectorは**[次のコピー数を下回るオブジェクトのみを含む]**オプションを無視し、オブジェクトのコピー数がこのオプションの許容値を超える場合でも、このオブジェクトを含むセッション内のすべてのオブジェクトを複製します。
- デフォルトでは、Data Protectorは元のオブジェクトのバージョン(同じオブジェクトの複数のコピーが見つかった場合)をソースデバイスとして選択します。状況によっては、元のバージョンのメディアタイプが異なるために、元のバージョンを複製できないことがあります。

  複製可能なライブラリを選択するか特定のライブラリを選択して、正しいソースデバイスを選択します。

複製を使用可能にする方法

B2Dデバイス間での複製を可能にするには、次の手順で*オブジェクトコピー仕様を作成する必要があります。*

1. ソースデバイスとターゲットデバイスが複製に対応していることを確認します。**[複製可能]**フィルターを使用して、デバイスをフィルター処理するか、特定のB2Dデバイスを明示的に選択します。
2. コピー操作オプションの設定時に、**[複製を使用]**を選択します。

詳細な手順については、「標準オブジェクトコピータスク」を参照してください。

自動複製同期

Data Protectorの複製機能では、Media Agentを介してデータを転送することなく、複製に対応した2つのディスクへのバックアップ(B2D)デバイス間でオブジェクトを複製することができます。自動複製同期機能は、通常の複製の拡張機能です。この機能を使用すると、異なるCell Managerが管理する2つの重複排除アプライアンス間のバックアップメタデータを複製することができます。この機能により、2つの重複排除デバイス間のバックアップデータとその他のメタデータを容易に交換できます。

前提条件

ソースのCell Manager上のData Protectorユーザー(CRSを実行しているアカウントを持つユーザー)がターゲットのCell Managerに必ずアクセスできるようになります。

考慮事項

統合バックアップでは、一部失敗したバックアップセッション(完了したが、エラーが発生しているバックアップセッション)から、自動複製同期手順を実行しないでください。複製は正常に終了しますが、複製されたセッションからの復元が失敗する可能性があります。

制限事項

- 通常の複製機能に適用されるすべての制限事項を考慮してください。
- ターゲットのCell Managerは、ソースのCell Managerのバージョンと同じバージョンか、より新しいバージョンでなければなりません。
- 複製のために選択するソースのCell Managerと外部のCell Manager(ターゲットのCell Manager)内のデバイスは、同じ物理デバイスとデータストアを指し示す必要があります。
- 一度に複製できる最大メディア数は、ターゲットデバイス上で利用可能な空き接続数によって決まります。たとえば、ターゲットデバイスに100の空き接続がある場合、同時に複製するメディアの数は100を超えないようにすることを推奨します。また、他の操作に対してターゲットデバイスを使用する場合は、同時に複製できるメディア数を利用可能な空き接続より少なくする必要があります。

  StoreOnceおよびデータドメインブーストデバイスの場合、利用できるデータ接続と複製ストリームをそれぞれ確認してください。サポートされているストリームの詳細については、各デバイスのマニュアルを参照してください。
- 古いGUIを使用する自動複製同期リストはサポートされていません。次のメッセージが返されることがあります。`"Error parsing Copy Specification file. The file may be corrupted or invalid."`このメッセージは、古いバージョンのData Protector GUIが新しいリストをサポートしていないことを示します。
- 自動複製同期手順では、**[次のコピー数を下回るオブジェクトのみを含む]**オプションはサポートされていません。

自動複製同期では次の2つの手順があります。

1. 外部のCell Managerのインポート
2. オブジェクトコピーセッションの実行

外部のCell Managerのインポート

自動複製同期をトリガーする最初の手順は、外部のCell ManagerのソースCell Managerへのインポートです。外部のCell Managerをインポートするには、以下を実行します。

1. コンテキストリストで**[クライアント]**をクリックします。
2. Scopingペインで**[クライアント]**を右クリックし、**[クライアントのインポート]**をクリックします。
3. インポートするクライアント名を入力します。Windows GUIを使用している場合は、ネットワークを参照して目的のクライアントを選択することもできます。重複排除アプライアンスを管理するCell Managerをインポートする場合は、**[Data Protector外部Cell Manager]**を選択します。

   > **注: 注記**: 自動複製同期手順を実行する場合、上記の手順が関係します。

4. **[完了]**をクリックしてクライアントをインポートします。

インポートしたクライアントの名前が[結果エリア]に表示されます。

> **注: 注記**: インポートしたCell Manager上では、自動複製同期アクションのみを実行できます。このCell Managerを使用して他の操作を実行することはできません。

オブジェクトコピーセッションの実行

外部のCell ManagerをソースのCell Managerにインポートした後に、オブジェクトコピーセッションを実行してバックアップデータおよびその他のメタデータを外部のCell Managerにコピーすることができます。要件に基づいてスケジュール済みコピー、ポストバックアップコピー、または対話型オブジェクトコピーを実行できます。

オブジェクトコピーセッションを実行するには、次の手順を実行します。

1. コンテキストリストで**[オブジェクト操作]**をクリックします。
2. Scopingペインで、**[コピー]** > **[オブジェクトコピー]** > **[自動]** を順に展開します。
3. **[スケジュール済み]**を右クリックし、**[追加]**をクリックしてウィザードを起動します。また、対話型コピー、ポストバックアップコピー、オブジェクトコピーセッションも実行できます。
4. コピーしたいオブジェクトを含むバックアップ、オブジェクトコピー、またはオブジェクト集約仕様を選択します。**[次へ]**をクリックします。
5. オブジェクトコピー操作に使用するオブジェクトフィルターを指定します。指定した条件に一致するオブジェクトだけがコピーされます。**[次へ]**をクリックします。
6. オブジェクトコピー操作に使用するライブラリフィルターを指定します。指定したライブラリ内のメディアに存在するオブジェクトだけがコピーされます。**[次へ]**をクリックします。
7. デフォルトでは、選択したバックアップ仕様でバックアップ用に使用されるデバイスがオブジェクトコピー操作のソースデバイスとして使用されます。必要に応じて、このページでソースデバイスを変更できます。**[次へ]**をクリックします。
8. オブジェクトコピー操作のあて先デバイスを選択します。Data Protectorは、ここでユーザーが指定するデバイスの中から最適のデバイスを選択します。**[次へ]**をクリックします。

   ディスクへのバックアップ(重複排除)デバイスのあるデバイスのみを選択するには、**[複製可能の表示]** チェックボックスを選択します。複製はディスクへのバックアップデバイスでのみ実行可能です。
9. 必要に応じて、ソースオブジェクトオプション、ターゲットオブジェクトオプション、およびターゲットメディアオプションを指定します。

   コピーの代わりに2つのB2Dデバイス間での複製を有効にするには、**[複製を使用]**を選択します。

   前にインポートした外部のCellサーバーへのオブジェクトの複製(このCell Managerには2つ目の重複排除デバイスが含まれる)を有効にするには、**[外部セルに複製]**を選択します。

   [次へ]をクリックします。
10. ドロップダウンメニューから前にインポートした外部のCellサーバーを選択します。ディスクストアへのバックアップにリンクされているデバイスが一覧されます。

    ターゲットCell Managerから作成され、同じストア名を持つすべてのデバイスがここに表示されます。したがって、複製用に正しいストア名を持つデバイスを選択するようにしてください。

    必要なデバイスまたはゲートウェイを選択し、**[次へ]**をクリックします。
11. **[保存とスケジュール...]**をクリックします。仕様の名前を入力し、**[OK]**をクリックして、スケジュール済みのオブジェクトコピー仕様を保存します。仕様を保存すると、スケジュールウィザードが開きます。ウィザードに表示される手順に従って仕様をスケジュールします。

    スケジューラーを使用してData Protectorでスケジュールの作成および編集を行う方法については、「*スケジューラー、ページ 103*」を参照してください。

スケジュール済みオブジェクトコピーセッションを実行して、自動複製同期手順を完了します。

オブジェクトのミラーリングについて

Data Protectorには、バックアップセッション中に同一データを複数のメディアセットに同時に書き込むための、オブジェクトミラー機能が用意されています。この機能を使用すると、一部またはすべてのバックアップオブジェクトのミラーを、1つまたは複数の追加のメディアセット上に作成できます。

オブジェクトのミラーリングを使用したバックアップセッションが成功すると、バックアップされたオブジェクトを含む1つのメディアセットと、ミラーリングされたオブジェクトを含む追加メディアセットが作成されます。これらのメディアセット上のミラーリングされたオブジェクトは、オブジェクトコピーとして扱われます。

オブジェクトのミラーリングの利点

オブジェクトミラー機能は、以下の目的に役立ちます。

- 複数のコピーが存在するため、バックアップデータの可用性が向上します。
- バックアップデータをリモートサイトにミラー化できるため、複数の場所へのボールティングが容易になります。
- 同じデータが複数のメディアに書き込まれるため、バックアップのフォールトトレランスが強化されます。1つのメディア上でメディア障害が発生しても、他のミラーの作成には影響しません。

制限事項

- ディスクへのZDBまたはNDMPバックアップ機能を使用してバックアップされたオブジェクトは、ミラーリング対象外です。
- 1回のセッションで同じデバイスにオブジェクトを複数回ミラーリングすることはできません。
- デバイスのブロックサイズは、ミラーチェーン内で小さくすることはできません。以下のようになります。
  - ミラー1の書き込みに使用するデバイスのブロックサイズは、バックアップに使用するデバイスのブロックサイズ以上でなければなりません。
  - ミラー2の書き込みに使用するデバイスのブロックサイズは、ミラー1の書き込みに使用するデバイスのブロックサイズ以上でなければなりません。

オブジェクトのミラーリングの使用方法

オブジェクトのミラーリングは、バックアップ仕様の構成時に指定します。バックアップ仕様では、ミラーリングするオブジェクトを選択し、ミラーの数を指定します。6つ以上のミラーを指定できるようにするには、`MaxNumberOfMirrors`グローバルオプションの値を大きくします。

バックアップおよび各ミラーに別のデバイスを指定します。オブジェクトミラーリングを伴うバックアップセッションが開始されると、Data Protectorは、バックアップ仕様に指定されているデバイスの中からデバイスを選択します。パフォーマンスへの影響を避けるため、ブロックサイズが同じデバイスを用意し、デバイスを同じシステムまたはSAN環境に接続することをお勧めします。SAP MaxDB、DB2 UDB、またはMicrosoft SQL Server統合ソフトウェアオブジェクトのミラー操作に必要なデバイスの最小数は、バックアップに使用されるデバイスの数と同じです。

オブジェクトのミラーリングは、デフォルトで負荷調整が行われます。Data Protectorは、できる限り多くのデバイスを使用して、使用可能なデバイスを最大限有効に活用します。コマンドラインからオブジェクトミラー操作を実行した場合は、負荷調整を使用できません。

メディアをコピーする

メディアをアーカイブまたはボールティングの目的でコピーできます。メディアのコピーセッションでは複数のメディアを同時にコピーできないため、各メディアのコピーを個別に開始する必要があります。

スタンドアロン デバイスのメディアをコピーする

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を展開し、コピーするメディアが格納されているデバイスを右クリックして、**[コピー]**をクリックします。
3. ターゲットメディアが格納されているデバイス(ライブラリのドライブとスロット)を選択し、**[次へ]**をクリックします。
4. メディアコピーの追加先となるメディアプールを選択し、**[次へ]**をクリックします。
5. 必要に応じて、メディアコピーの説明と収納場所を指定し、**[次へ]**をクリックします。
6. セッションに適用するその他のオプションを指定します。**[強制操作]**オプションを選択して、メディアのサイズとメディア保護を指定できます。

   > **ヒント:**
   > ターゲットメディアがData Protectorで認識する形式(tar、OmniBack Iなど)以外の形式である場合や、保護されていないData Protectorメディアの場合は、**[強制操作]**オプションを使います。

7. **[完了]**をクリックして、ウィザードを終了します。これにより、コピー処理が開始します。

[セッション情報]メッセージにメディアコピーの進行状況が表示されます。

ライブラリ デバイスのメディアをコピーする

手順

1. コンテキストリストで**[デバイス/メディア]**をクリックします。
2. Scopingペインの**[メディア]**で、**[プール]**を展開し、コピーするメディアが格納されているメディアプールを展開します。メディアを右クリックし、**[コピー]**をクリックしてウィザードを起動します。
3. コピー対象のメディアのドライブを選択し、**[次へ]**をクリックします。ライブラリにドライブが1つしかない場合、この手順はスキップされます。
4. ターゲットメディアが格納されているデバイス(ライブラリのドライブとスロット)を選択し、**[次へ]**をクリックします。
5. メディアコピーの追加先となるメディアプールを選択し、**[次へ]**をクリックします。
6. 必要に応じて、メディアコピーの説明と収納場所を指定し、**[次へ]**をクリックします。

7. セッションに適用するその他のオプションを指定します。**[強制操作]**オプションを選択して、メディアのサイズとメディア保護を指定できます。

> **ヒント:**
> ターゲットメディアがData Protectorで認識する形式(tar、OmniBack Iなど)以外の形式である場合や、保護されていないData Protectorメディアの場合は、**[強制操作]**オプションを使います。

8. **[完了]**をクリックして、ウィザードを終了します。これにより、コピー処理が開始します。

[セッション情報]メッセージにメディアコピーの進行状況が表示されます。

第13章: オブジェクト検証

オブジェクト検証について

Data Protectorオブジェクト検証機能を使用すると、バックアップオブジェクトを確認できます。この機能の使用により、1つの完全バックアップメディアのみを対話的に検証する必要がなくなります。スケジュールされたセッションまたは操作後セッションで1つまたは複数のメディア上の1つまたは複数のオブジェクトを対話的に確認できるようになりました。

確認されるオブジェクトは、オリジナルのバックアップオブジェクト、オブジェクトコピー、および集約されたオブジェクトです。

データ検証

オブジェクト検証セッション中には、Data Protectorがメディアを検証する時に使用される方法と同様の方法で個々のバックアップオブジェクトのデータを検証します。

ホストへの送信

デフォルトでは、データ検証処理を実行するターゲットホストは、オリジナルのバックアップソースホストです。これは、バックアップデータをMedia Agentホストからそのホストに送信するData Protectorの機能を検証します。あるいは、別のターゲットホストを指定することも、ネットワークを使用せずにMedia Agentホスト上で検証を実行することもできます。

オブジェクト検証セッションの種類

オブジェクト検証セッションを対話式に開始するか、またはセッションに自動開始を指定することができます。Data Protectorには、2種類の自動オブジェクト検証があります。ポストバックアップのオブジェクト検証とスケジュールされたオブジェクト検証です。

ポストバックアップのオブジェクト検証

ポストバックアップオブジェクト検証は、バックアップ、オブジェクトコピー、または集約セッションの完了直後に行われ、そのセッション中に作成されたオブジェクトが確認されます。検証するオブジェクトは、ポストバックアップオブジェクト検証仕様で指定します。これは、作成されたオブジェクトを定義しているバックアップ、オブジェクトコピー、またはオブジェクト集約仕様を指定し、オブジェクトのフィルター条件を提供します。1つのポストバックアップオブジェクト検証仕様に、複数のバックアップ、オブジェクトコピー、または集約仕様を含めることができます。

スケジュールされたオブジェクト検証

スケジュールされたオブジェクト検証は、Data Protectorスケジューラーで指定された時刻に実行され、指定時間中に作成されたバックアップ、コピー、または集約オブジェクトバージョンが確認されます。検証するオブジェクトと、オブジェクトバージョン作成の有効期間は、スケジュールされたオブジェクト検証仕様に指定されます。これは、作成されたオブジェクトを定義しているバックアップ、オブジェクトコピー、またはオブジェクト集約仕様を指定

し、オブジェクトのフィルター条件を提供します。1つのスケジュールされたオブジェクト検証仕様に、複数のバックアップ、オブジェクトコピー、または集約仕様を含めることができます。

オブジェクトの検証方法

最初に、対話型セッションを開始するか、オブジェクト検証仕様を作成します。検証対象のバックアップオブジェクト、ソースデバイス、メディア、および検証ターゲットホストを選択します。

オブジェクトの選択

自動処理

自動化されたオブジェクト確認仕様の場合、確認するオブジェクトを選択するには、バックアップ、オブジェクトコピー、または集約仕様を選択してから保護、コピー数、使用可能ライブラリ、またはタイムフレーム(スケジュールの場合のみ)に従ってフィルターを実行します。この場合、検証に個々のオブジェクトバージョンを選択することはできません。Data Protectorは、フィルター条件に一致するすべてのオブジェクトバージョンを検証します。

対話型操作

対話型セッションの場合、個々のオブジェクトをメディア、セッション、またはIDB内のオブジェクト選択ウィザードリストから選択できます。この場合、確認の必要なオブジェクトバージョンの個々のコピーを選択することができます。

ソースデバイスの選択

デフォルトで、Data Protectorは自動でデバイス選択を行います。または、オリジナルのデバイス選択を強制選択することも、新しいデバイスを選択することもできます。

ターゲットホストの選択

デフォルトで、Data Protectorはソースホスト、つまりオリジナルバックアップのソースオブジェクトがあったホストに対して確認プロセスを実行し、オブジェクトデータおよびその送信を検証します。また、代替のリモートホスト、またはMedia Agentホストを指定して、オブジェクトデータのみを確認することもできます。選択したターゲットホストにData Protector Disk Agentがインストールされている必要があります。

スケジュール設定

スケジュールされた検証操作のスケジュール設定は、Data Protectorスケジューラーを使用してバックアップに対する方法と同じ方法で行われます。

スケジューラーを使用して、Data Protectorでスケジュールを作成および編集する方法の詳細については、「*スケジューラー、ページ 103*」を参照してください。

> **重要:**
> Data Protector10.00では、基本スケジューラーとアドバンストスケジューラーは廃止され、代わりに新しいWebベーススケジューラーが導入されました。特定の日時に実行するようバックアップセッションをスケジュールすることで、無人バックアップを構成できます。Data Protectorのアップグレード中に、すべての既存のData Protectorスケジュールが新しいスケジューラーに自動的に移行されます。

標準オブジェクト検証タスク

オブジェクト検証機能には、以下の前提条件と制限事項があります。

前提条件

- オブジェクト検証セッションのソースホストとして機能するすべてのシステムにMedia Agentをインストールする必要があります。
- オブジェクト検証セッションのターゲットホストとして機能するすべてのシステムにDisk Agentをインストールする必要があります。
- オブジェクト検証処理に関係するすべてのDisk Agentは、A.06.11以降でなくてはなりません。
- 必要なデバイスが構成されており、メディアが準備されている必要があります。
- オブジェクト検証セッションを実行するために適切なユーザー権限がソースおよびあて先ホストの両方に必要です。これらは、[復元の開始]と[別のユーザーから復元]のユーザー権限です
- あて先ホストがUNIXホストである場合、[ルートユーザーとして復元]が必要です。

制限事項

- ソースメディアの読み取り中、これらを復元に使用することはできません
- アプリケーション統合オブジェクトのオブジェクト検証では、オブジェクトデータがターゲットホストに送信されることと、Data Protectorフォーマットの観点から一貫性があることを確認します。アプリケーション統合に固有のチェックは実行されません。
- オブジェクト検証は、ディスクへのZDB、またはディスク+テープへのZDBのディスク部分を使用してバックアップされたオブジェクトには使用できません。

オブジェクトを対話型で検証する

オブジェクトは、必要に応じてメディア、オブジェクト、またはセッションの開始ポイントから対話型検証用に選択できます。対話型オブジェクト検証仕様を保存することはできません。オブジェクト検証セッションの開始のみが可能です。

手順

1. コンテキストリストで**[オブジェクト操作]**をクリックします。
2. Scopingペインで、**[検証]**を展開してから**[オブジェクト検証]**を展開します。
3. [対話型]を展**開します。**
4. **[メディア]**、**[オブジェクト]**、または**[セッション]**をクリックしてウィザードを起動します。
   - **[メディア]**をクリックすると、オブジェクトが書き込まれた使用可能メディアがリストに表示されます。
   - **[オブジェクト]**をクリックすると、使用可能メディアに書き込まれたオブジェクトがリストに表示されます。
   - **[セッション]**をクリックすると、使用可能メディアにオブジェクトが書き込まれたセッションがリストに表示されます。
5. 確認対象のオブジェクトを選択します。

   > **注:**
   > VMwareバックアップ用のData Protector10.00以降からは、仮想マシンディスクは並行して実行されるオブジェクトとして見なされます。メディアに戻された仮想マシンディスクを把握するために、仮想マシンのディスクオブジェクトは**[メディア]**リストに一覧されますが無効化されています。コピーまたは検証操作は仮想マシンオブジェクトに対して実行され、それに関連するすべてのディスクオブジェクトは内部と見なされます。
   >
   > VMware統合用のData Protector10.00以降からは、**[次へ]**オプションは、**[メディア]**リストで仮想マシンオブジェクトを選択した後にのみ有効になります。

   [次へ]をクリックします。
6. オブジェクトを読み込む元のソースデバイスを選択します。デフォルトで、自動デバイス選択が選択されます。

   元のデバイス選択を強制することも、**[元のデバイス]**を右クリックして**[デバイスの変更]**を選択することによって、別のドライブに置き換えることも可能です。

   [次へ]をクリックします。
7. オブジェクト検証操作のターゲットホストを選択します。このホストには、Data Protector Disk Agentが必要なバージョンレベルでインストールされている必要があります。

   デフォルトでは、オリジナルのバックアップソースホストが選択されます。選択したソースデバイスがインストールされているMedia Agentホストを選択することも、Disk Agentを必要なバージョンレベルでインストールしているセルから任意のホストを選択することもできます。**[次へ]**をクリックします。
8. 選択したオブジェクトが含まれているメディアのリストが表示されます。メディアの位置の優先順位を変更すると、同じオブジェクトが複数のメディアセット内に存在する場合のメディアの選択を制御できます。

   [次へ]をクリックします。
9. 確認のため選択されたオブジェクトバージョンのサマリーが表示されます。
   - 特定のオブジェクトバージョンの詳細を表示するには、リストでオブジェクトバージョンを選択し、**[プロパティ]**をクリックします。

オブジェクトバージョンのコピーが複数存在する場合は、デフォルトでData Protectorは検証に最適なコピーを選択します。検証するコピーは、[プロパティ]で手動で選択できます。

[OK]をクリックします。

- オブジェクトバージョンをリストから削除するには、リスト内で選択し、**[削除]**をクリックします。

10. **[完了]**をクリックして、ウィザードを終了します。これによって、確認が開始されます。

ポストバックアップのオブジェクト検証を構成する

ポストバックアップのオブジェクト検証は、バックアップセッション、オブジェクトコピーセッション、またはオブジェクト集約セッションの終了後に実行されるように構成されます。

該当するバックアップ、オブジェクトコピー、集約仕様の名前は、オブジェクト自動検証仕様で選択されます。これらの選択した仕様を使用するセッションを実行する場合、Data Protectorはオブジェクト検証仕様で指定された基準を使用して、そのセッションの完了後にセッション中に生成されたオブジェクトを検証します。

手順

1. コンテキストリストで**[オブジェクト操作]**をクリックします。
2. Scopingペインで、**[検証]**を展開してから**[オブジェクト検証]**を展開します。
3. **[自動化]**を展開し、**[ポストバックアップ]**を右クリックし、**[追加]**を選択してウィザードを起動します。
4. オブジェクト検証仕様を直後に実行する対象となる任意のバックアップ仕様を選択します。**[次へ]**をクリックします。
5. オブジェクト検証仕様を直後に実行する対象となる任意のオブジェクトコピー仕様を選択します。**[次へ]**をクリックします。
6. オブジェクト検証仕様を直後に実行する対象となる任意の集約仕様を選択します。**[次へ]**をクリックします。
7. 必要に応じて、オブジェクト検証操作に使用するオブジェクトフィルターを指定します。指定した条件に一致するオブジェクトのみが確認されます。**[次へ]**をクリックします。
8. 必要に応じて、オブジェクト検証操作に使用するライブラリフィルターを指定します。指定したライブラリ内のメディアに含まれるオブジェクトだけが確認されます。**[次へ]**をクリックします。
9. オブジェクトを読み込む元のソースデバイスを選択します。デフォルトで、Data Protectorは自動でデバイス選択を使用します。

   または、元のデバイスから強制選択することができます。つまり、デバイスが使用できない場合は、使用可能になるまでData Protectorが待機します。オリジナル用に別のドライブを置き換えることもできます。たとえば、元のデバイスを新しいデバイスに交換した後に、**[元のデバイス]**を右クリックして**[デバイスの変更]**を選択します。

   [次へ]をクリックします。
10. オブジェクト検証操作のターゲットホストを選択します。このホストには、Data Protector Disk Agentがインストールされている必要があります。

    以下を選択できます。

- オリジナルのバックアップオブジェクトが生成されたホスト(デフォルト選択)。これは、ネットワークパス内のData Protectorコンポーネントも検証します。
- Media Agentホスト。つまり、ネットワークを必要とせずソースデバイスがあるホスト。
- 代替リモートホスト。そのホストへのネットワークパス内のData Protectorコンポーネントを検証します。

[次へ]をクリックします。

11. **[別名で保存...]**をクリックし、仕様の名前を入力し、**[OK]**をクリックして検証仕様を保存します。

スケジュール済みのオブジェクト検証を構成する

スケジュール済みのオブジェクト検証は、ユーザー定義のタイミングで実行されます。異なるバックアップセッション、オブジェクトコピーセッション、またはオブジェクト集約セッションによって生成されたオブジェクトは、スケジュールされた単一のオブジェクト検証セッション内で確認できます。

手順

1. コンテキストリストで**[オブジェクト操作]**をクリックします。
2. Scopingペインで、**[検証]**を展開してから**[オブジェクト検証]**を展開します。
3. **[自動]**を展開し、**[スケジュール済み]**を右クリックし、**[追加]**を選択してウィザードを起動します。
4. 検証をスケジュールする対象の出力オブジェクトを定義する任意のバックアップ仕様を選択します。**[次へ]**をクリックします。
5. 検証をスケジュールする出力オブジェクトを定義するオブジェクトコピー仕様を選択します。**[次へ]**をクリックします。
6. 検証をスケジュールする対象の出力オブジェクトを定義する任意の集約仕様を選択します。**[次へ]**をクリックします。
7. 必要に応じて、オブジェクト検証操作に使用するオブジェクト フィルターを指定します。

   これにより、保護、コピー数、または作成時間に従って使用可能なオブジェクトにフィルターを実行できます。フィルター条件に一致するすべてのオブジェクトバージョンが確認されます。

   [次へ]をクリックします。
8. 必要に応じて、オブジェクト検証操作に使用するライブラリフィルターを指定します。指定したライブラリ内のメディアに含まれるオブジェクトだけが確認されます。**[次へ]**をクリックします。
9. オブジェクトを読み込む元のソースデバイスを選択します。デフォルトで、Data Protectorは自動でデバイス選択を使用します。

   または、元のデバイスから強制選択することができます。つまり、デバイスが使用できない場合は、使用可能になるまでData Protectorが待機します。オリジナル用に別のドライブを置き換えることもできます。たとえば、元のデバイスを新しいデバイスに交換した後に、**[元のデバイス]**を右クリックして**[デバイスの変更]**を選択します。

   [次へ]をクリックします。
10. オブジェクト検証操作のターゲットホストを選択します。このホストには、Data Protector Disk Agentが

インストールされている必要があります。

以下を選択できます。

- オリジナルのバックアップオブジェクトが生成されたホスト(デフォルト選択)。これは、ネットワークパス内のData Protectorコンポーネントも検証します。
- Media Agentホスト。つまり、ネットワークを必要とせずソースデバイスがあるホスト。
- 代替リモートホスト。そのホストへのネットワークパス内のData Protectorコンポーネントを検証します。

[次へ]をクリックします。

11. **[保存とスケジュール...]**をクリックします。仕様の名前を入力し、**[OK]**をクリックして検証仕様を保存します。仕様を保存すると、スケジュールウィザードが開きます。ウィザードに表示される手順に従って仕様をスケジュールします。

    スケジューラーを使用してData Protectorでスケジュールの作成および編集を行う方法については、「*スケジューラー、ページ 103*」を参照してください。

オブジェクト検証環境をカスタマイズする

オブジェクト検証環境をカスタマイズするには、確認セッションを確認するオブジェクトがない場合に生成されるメッセージレベルおよびセッション状態を変更します。これを実現するためには、`SessionStatusWhenNoObjectToVerify` グローバルオプションを変更します。

第14章: 復元

復元について

復元とは、バックアップコピーからオリジナルのデータを再作成して、ディスクにコピーするプロセスです。このプロセスには、復元の準備と実際の復元が含まれます。必要に応じて、データを利用可能な状態にするなどの処理を復元後に実行することもできます。

復元のコンセプトの詳細については、『*HPE Data Protectorコンセプトガイド*』と『*HPE Data Protectorインテグレーションガイド*』を参照してください。

これらの機能の指定方法と利用可能なオプションはプラットフォームによって異なります。

Oracle、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server、Informix Server、IBM DB2 UDB、Sybaseなどのアプリケーションとの統合ソフトウェアの復元方法については、『*HPE Data Protectorインテグレーションガイド*』を参照してください。

標準復元手順

標準復元手順では、段階を踏んだ操作を行います。

1. 復元対象のデータを選択する
2. 必要なメディアを見つける
3. 復元セッションを開始する

   その他のオプションはバックアッププロセスに従って事前定義されていますが、必要に応じて修正できます。

前提条件

復元を行うには、適切なユーザー権限が必要です。この権限は、ユーザーグループに基づいて定義されます。

復元対象のデータを選択する

復元対象のデータは、2通りの方法で選択できます。バックアップオブジェクトのリストをブラウズする方法か、セッションのリストをブラウズする方法です。この2つの違いは、復元用に提示されるディレクトリおよびファイルの範囲にあります。

- セル内のクライアントシステム別、およびデータの種類別に(ファイルシステム、ディスクイメージ、内部データベースなど)分類された、バックアップ済みオブジェクトのリストを使用する、**[復元オブジェクト]**。復元にまだ利用できるバックアップ済みのディレクトリ、ファイル、バージョンを、すべてブラウズすることができます。
- バックアップ済みのオブジェクトを含んでいるファイルシステムセッションのリストを使用する、**[復元セッション]**。昨年、先月、または先週のセッションのみを表示することができます。このセッションでバックアップされたすべてのオブジェクト(バックアップ仕様に指定された全クライアントからのドライブと同様に)と、この復元チェーンのすべてのバージョンをブラウズすることができます。デフォルトでは、選択したディレクトリまたはファイルの復元チェーン全体が復元されますが、単一セッションだけのデータを復元することもできます。

前提条件

オブジェクトをブラウズしてディレクトリまたは特定のファイルを選択するには、バックアップ時にロギングレベルが[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]、または[すべてログに記録]に設定されていることが必要条件となります。

バックアップオブジェクトのリストからデータを選択する

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインで、[復元オブジェクト]の下にある適切なデータの種類(**[ファイルシステム]**など)を展開します。
3. 復元するデータのあるクライアントシステムを展開し、データのあるオブジェクト(UNIXシステムではマウントポイント、Windowsシステムではドライブ)をクリックします。
4. [ソース]プロパティページで、オブジェクトを展開し、復元対象のディレクトリまたはファイルを選択します。

   ディレクトリ全体を選択した場合、デフォルトでは、前回のバックアップセッションでバックアップされたディレクトリ/ファイルだけが復元対象として選択されます。ツリー構造内に含まれているディレクトリおよびファイルのうち、前回のバックアップセッションでバックアップされたもの以外は淡色表示されます。他のバックアップセッションでバックアップしたデータを復元したい場合は、選択したディレクトリを右クリックし、**[バージョンの復元]**をクリックします。復元するバックアップバージョンをドロップダウンリストから選択します。

> **ヒント:**
> 上の手順を繰り返して複数のオブジェクト(マウントポイントやドライブ)のデータを選択すると、並行復元を実行できます。

バックアップセッションのリストからデータを選択する

制限事項

- オンラインデータベース統合ソフトウェアの復元を、特定のバックアップセッションから実行することはできません。
- "復元セッション"モードを使用してコピーセッションから復元を実行することはできません。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインの**[復元セッション]**を展開して、クライアントを表示し、次に特定のクライアントでバックアップされたオブジェクトを表示します。オブジェクトをクリックして、オブジェクトのプロパティページを開きます。
3. **[ソース]**ページで、復元するディレクトリとファイルを選択します。

デフォルトで、復元チェーン全体が復元されます([**フルチェーンを表示**]が選択されています)。このセッションのデータだけを復元するには、[**このセッションのみを表示**]を選択します。

4. 復元先を指定し、復元オプションを設定します。
5. [**復元**]をクリックして復元セッションを開始します。

> **ヒント:**
> 並行復元を実行するには、復元を開始する前に、追加するオブジェクトごとに手順2～4を繰り返します。

特定のバックアップバージョンを選択する

復元するデータを選択した後に、復元対象のバックアップバージョンを選択することができます。

ファイルまたはディレクトリ別にバックアップバージョンを選択する

手順

1. コンテキストリストで[**復元**]をクリックします。
2. Scopingペインで、[復元オブジェクト]の下にある適切なデータの種類([ファイルシステム]など)を展開します。
3. 復元するデータがあるクライアントシステムを展開し、データが格納されているオブジェクトをクリックします。
4. [ソース]プロパティページで、復元対象のオブジェクトを選択します。デフォルトでは、最新のバックアップバージョンが復元対象として選択されます。
5. オブジェクトを右クリックし、[**バージョンの復元**]を選択します。
6. 復元するバックアップバージョンをドロップダウンリストから選択します。バックアップバージョンの詳細情報を表示するには、[**...**]をクリックします。ただし、"**...**"ボタンが有効になるのは、属性を記録するログレベルで実行されたバックアップの場合です。
7. [**OK**]をクリックします。

復元するバージョンを選択した後は、[ソース]プロパティページではそのバージョンのファイルおよびディレクトリだけが復元可能として表示されます。他のファイルおよびディレクトリは灰色で表示され、復元されません。

複数のファイルまたはディレクトリで同時にバックアップバージョンを選択する

手順

1. コンテキストリストで[**復元**]をクリックします。
2. Scopingペインで、[復元オブジェクト]の下にある適切なデータの種類([**ファイルシステム**]など)を展開します。
3. 復元するデータがあるクライアントシステムを展開し、データが格納されているオブジェクトをクリックし

ます。

4. [ソース]プロパティページで、復元する複数のオブジェクトを選択します。デフォルトでは、最新のバックアップバージョンが復元対象として選択されます。
5. **[復元サマリー]**タブをクリックしてすべてのオブジェクトを選択し、選択部分を右クリックして**[時間によってバージョンを選択...]**を選択します。
6. **[日時によってバージョンを選択]**オプションをクリックして、ポップアップメニューから日付を選択します。
7. **[日時によってバージョンを選択]**ドロップダウンリストに表示される中から、時間を選択入力します。
8. **[バックアップ時間の相違]**では、どの選択オブジェクトにも選択した日時に対応するバックアップバージョンが存在しない場合に必要な調整を行います。
9. **[選択された日時が選択された基準に一致しない場合]**では、どの選択オブジェクトにも、選択した日時および**[バックアップ時間の相違]**で修正した日時に対応するバックアップバージョンが存在しない場合に、必要な調整を行います。
10. **[OK]**をクリックします。

復元に関する条件を指定した後、[ソース]プロパティページでは、選択内容と一致したバックアップバージョンが各復元オブジェクトの隣に表示されます。

ファイルの重複を処理する

ディスク上の既存のファイルバージョンとバックアップに含まれるファイルバージョンが重複している場合の処理方法は選択可能です。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインで、[復元オブジェクト]の下にある適切なデータの種類(**[ファイルシステム]**など)を展開します。
3. 復元するデータがあるクライアントシステムを展開し、データが格納されているオブジェクトをクリックします。
4. [ソース]プロパティページで、復元するディスク、ディレクトリ、またはファイルを選択します。
5. **[あて先]**タブをクリックし、[ファイル重複時の処理]のオプションのいずれかを選択します。
   - **最新ファイルを保持**
   - **上書きしない**
   - **上書き**

復元に使用するデバイスを選択する

Data Protectorのデフォルト設定では、バックアップ中に使用されたデバイスと同じデバイスを使用して選択済みデータを復元します。ただし、復元に別のデバイスを選択することもできます。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインで、[復元オブジェクト]の下にある適切なデータの種類(**[ファイルシステム]**など)を展開します。
3. 復元するデータがあるクライアントシステムを展開し、データが格納されているオブジェクトをクリックします。
4. [ソース]プロパティページで、オブジェクトを展開し、復元対象を選択します。
5. **[デバイス]**タブをクリックして[デバイス]プロパティページを表示します。

   ここでは、バックアップ中に使用されたデバイスが表示されます。

   別のデバイスを使用してデータを復元するには、元のデバイスを選択し、**[変更]**をクリックします。[新しいデバイスを選択]ダイアログボックスで、別のデバイスを選択し、**[OK]**をクリックします。新しいデバイスの名前が[デバイスのステータス]の下に表示されます。新しいデバイスは、このセッションでのみ使用されます。

   デバイスに関する詳細を表示するには、デバイスを右クリックして**[情報]**を選択します。

   選択したデバイスを(無効または使用中などの理由で)復元に使用できない場合のData Protectorでの処理を指定します。**[デバイスの自動選択]**または**[元のデバイスの選択]**を選択します。

復元に必要なメディアを検索する

復元対象のデータを選択したら、データが格納されているメディアのリストを取得する必要があります。スタンドアロンデバイスを使用している場合やメディアをライブラリの外に保管している場合は、この操作が不可欠です。

復元対象のオブジェクトバージョンが複数のメディアセット上に存在する場合は、メディアの位置の優先順位を設定して復元に使用するメディアセットの選択を制御するか、または使用するメディアセットを手動で選択できます。

合成バックアップを使用する場合、同一時点におけるオブジェクトの復元チェーンが複数存在することがよくあります。デフォルトでは、Data Protectorによって、最も有用な復元チェーンが選択され、その復元チェーンの中で最も適切なメディアが選択されます。

> **注:**
> メディアコピー機能を使って取得したコピーは、必要なメディアとして表示されません。メディアコピーは、オリジナルのメディア(コピー元として使用されたメディア)が使用不可能な場合にのみ使用できます。

制限事項

- 一部の統合ソフトウェアでは、[復元]コンテキストでメディアの位置の優先順位を設定できません。これらの統合ソフトウェアについては、GUIに[メディア]タブが表示されません。
- 統合オブジェクトの復元時に、メディアセットを手動で選択することはできません。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインで、[復元オブジェクト]の下にある適切なデータの種類(**[ファイルシステム]**など)を展開します。
3. 復元するデータがあるクライアントシステムを展開し、データが格納されているオブジェクトをクリックします。
4. [ソース]プロパティページで、オブジェクトを展開し、復元対象を選択します。
5. **[メディア]**タブをクリックして[メディア]プロパティページを表示します。必要なメディアが表示されます。メディアに関する詳細を表示するには、メディアを右クリックして**[情報]**を選択します。

   復元対象のオブジェクトバージョンが複数のメディアセット上に存在する場合は、そのオブジェクトバージョンが含まれているすべてのメディアセットが表示されます。メディアセットの選択は、Data Protectorのメディアセット選択の内部アルゴリズムと、メディアの位置の優先順位の設定に依存しています。

   - メディアの位置の優先順位の設定を置き換えるには、位置を選択し、**[優先順位の変更]**をクリックします。別の位置の優先順位を選択し、**[OK]**をクリックします。
   - 復元元のメディアセットを手動で選択するには、**[コピー]**タブをクリックします。[コピー]プロパティページで、目的のオブジェクトバージョンを選択し、**[プロパティ]**をクリックします。**[ソースコピーを手動で選択]**オプションを選択し、ドロップダウンリストで目的のコピーを選択して、**[OK]**をクリックします。
6. 必要に応じて、メディアをデバイスに挿入します。

> **ヒント:**
> [復元セッションの開始]ダイアログボックスで**[必要なメディア]**をクリックする方法で、復元に必要なメディア(選択したオブジェクトのオブジェクトコピーが格納されているメディアなど)を表示することもできます。このダイアログボックスは、復元の開始時に表示されます。

復元をプレビューして開始する

前提条件

- 必要なメディアが利用可能になっている(デバイス内にロードされている)ことを確認します。

制限事項

- Data Protector内部データベースの復元、およびData Protectorアプリケーションの統合プログラムの復元セッションでは、プレビューは利用できません。

手順

1. 復元対象を選択します。[復元]プロパティページで、使用するデバイスを選択するなど、必要なオプションを指定します。
2. どのメディアが復元に必要かをチェックします。

3. **[アクション]**メニューを開きます。復元プロセスをプレビューするには**[復元のプレビュー]**をクリックし、復元プロセスを開始するには**[復元の開始]**をクリックします。**[プロパティ]**ページで**[プレビュー]**ボタンや**[復元]**ボタンをクリックするという方法もあります。
4. [セッションの開始]ウィザードで、選択を確認して**[レポートレベル]**オプション、**[ネットワーク負荷]**オプション、**[再開可能な復元を使用可能にする]**オプションを指定します。

復元の進捗が復元モニターに表示されます。

復元を中止する

復元セッションを中止すると、復元が停止します。セッションを中止する前に処理が完了していたデータは、指定の場所に復元されます。

手順

1. 復元セッションを中止するには、**[アクション]**メニューの**[中止]**を選択します。

> **ヒント:**
> 復元セッションは、Data Protectorの[モニター]コンテキストからも中止できます。

復元先オプション

Data Protectorのデフォルト設定では、データのバックアップ元のクライアントとディレクトリがデータの復元先になります。これらのデフォルト設定を変更するには、[あて先]プロパティページでデータの復元先を明示的に指定します。

- このとき、適切なユーザー権限を使ってデータを別のクライアントシステムに復元できます。
- データを別のディレクトリに復元できます。

全般的な復元先はオブジェクト別に設定できます。

さらに、Data Protectorの**[別名で復元/復元先]**オプションを使うと、同じバックアップオブジェクトに含まれているファイルとディレクトリのそれぞれについて異なる復元先を指定できます。

復元先を選択する

復元対象のデータを選択した後、データの復元先を選択できます。データを他のクライアントシステムに復元したり、ディレクトリパスを変更したりすることができます。指定した復元先は、復元対象のオブジェクト全体に適用されます。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインで、[復元オブジェクト]の下にある適切なデータの種類を展開します。
3. 復元するデータがあるクライアントシステムを展開し、データが格納されているオブジェクトをクリックします。
4. [ソース]プロパティページで、復元対象のオブジェクトを選択します。

5. **[あて先]**タブをクリックし、**[ターゲットクライアント]**ドロップダウンリストから復元先のクライアントシステムを選択します。デフォルトでは、オリジナAルのディレクトリ構造を維持したままデータが復元されます。たとえば、データをシステムC:\temp上のBディレクトリからバックアップしたのであれば、そのデータはシステムC:\temp上のData Protectorディレクトリに復元されます。
6. 復元のディレクトリパスを変更するには、**[新しいディレクトリに復元]**オプションを選択し、上位ディレクトリを入力するか、またはブラウズして選択します。この上位ディレクトリの下層にバックアップ時のディレクトリパスが追加されます。たとえば、C:\sound\songsディレクトリからバックアップしたデータに対し、新しいパスとして\users\bingと入力すると、そのデータはC:\users\bing\sound\songsディレクトリに復元されます。

個々のファイルとディレクトリに対して復元先を指定する

各オブジェクト内のディレクトリまたはファイルの復元パスは個別に指定できます。**[別名で復元/復元先]**オプションで指定した位置は、[あて先]プロパティページで指定された位置よりも優先されます。

この機能は、最初に選択されたツリーノード(ディレクトリ)において、また、すでに選択されているツリーノードに階層的に依存しないツリーノードにおいて、利用することができます。選択されているツリーノードは青のチェックマークで示され、依存するツリーノードは黒のチェックマークで示されます。

復元先を指定して復元

[復元先を指定して復元]を選択すると、バックアップのパスがここで指定した新しい復元先に追加されます。新しい復元先は既存のディレクトリでなければなりません。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインで、[復元オブジェクト]の下にある適切なデータの種類を展開します。
3. 復元するデータがあるクライアントシステムを展開し、データが格納されているオブジェクトをクリックします。
4. [ソース]プロパティページで、復元対象のオブジェクトを選択します。
5. 目的のファイルまたはディレクトリを右クリックして、**[別名で復元/復元先]**をクリックします。
6. [あて先]タブの[復元]ドロップダウンリストから**[復元先]**を選択します。
7. Windowsシステムのオプションとして、[ドライブ]テキストボックスでデータの復元先に別のドライブを選択できます。別のクライアントシステムに復元する場合は、**[ブラウズ]**をクリックします。
8. [位置]テキストボックスにファイルまたはディレクトリの新しいパスを入力します。新しいパスに元のパスが追加されます。たとえば、colors.mp3というファイルをC:\sound\songsディレクトリからバックアップして、新しいパスとして\users\bingと入力した場合、このファイルはC:\users\bing\sound\songsディレクトリに復元されます。
9. **[OK]**をクリックします。

別名で復元

[別名で復元]を選択すると、バックアップのパスがここで指定した新しい復元先に変更されます。復元先パスは、新しいディレクトリでも既存のディレクトリでも構いません。復元対象のファイルやディレクトリの名前は変更できます。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインで、[復元オブジェクト]の下にある適切なデータの種類を展開します。
3. 復元するデータがあるクライアントシステムを展開し、データが格納されているオブジェクトをクリックします。
4. [ソース]プロパティページで、復元対象のオブジェクトを選択します。
5. 目的のファイルまたはディレクトリを右クリックして、**[別名で復元/復元先]**をクリックします。
6. [あて先]タブの[復元]ドロップダウンリストから**[ファイル名]**を選択します。
7. Windowsシステムのオプションとして、[ドライブ]テキストボックスでデータの復元先に別のドライブを選択できます。別のクライアントシステムに復元する場合は、**[ブラウズ]**をクリックします。
8. [位置]テキストボックスにファイルまたはディレクトリの新しいパスを入力します。たとえば、`colors.mp3`というファイルを`C:\sound\songs`ディレクトリからバックアップして、新しいパスとして`\users\bing\colors.mp`と入力した場合、このファイルは`C:\users\bing`ディレクトリに復元されます。

   > **注意:**
   > **[上書き]**オプションが有効に設定されているデータが削除される危険があることに注意してください。
   > - 既存のファイル/ディレクトリ名を指定して復元した場合
   > - ファイルまたはディレクトリ名を指定しないで既存のパスを指定した場合
   >
   > たとえば、[位置]テキストボックスに、`colors.mp`ファイルの復元先として新しいパス`\users\bing`を入力して、ファイル名を入力しなかった場合、`colors.mp`ファイルは`bing`という名前で復元されます。この場合、`bing`という元のディレクトリは削除され、復元されたファイルに置き換わります。

9. **[OK]**をクリックします。

失敗したセッションの再開について

バックアップセッションや復元セッションが次のいずれかの理由で失敗した場合、Data Protectorのセッション再開機能を使用して再開できます。

- ネットワーク接続の問題
- 致命的なDisk Agentの問題
- 致命的なMedia Agentの問題
- 致命的なセッションマネージャーの問題
- 致命的なメディアの問題(テープ傷など)
- GUIから中止コマンドが発行された

ただし、障害となる問題をまず解決する必要があります。

失敗したセッションを再開する場合、Data Protectorは、失敗したセッションが中止されたところから始めて、バックアップまたは復元を続行します。再開されたセッションは、元のセッションのオプションをすべて継承します。

すべての種類のセッションを再開できるわけではありません。Data Protectorでは、以下を再開できます。

- ファイルシステムのバックアップセッション
- ファイルシステムの復元セッション
- Data Protector Oracle用統合ソフトウェア、バックアップセット
- Data Protector Oracle Server統合復元セッション

ファイルシステムのバックアップセッション

ファイルシステムバックアップセッションの再開セッション機能は、内部データベースに書き込まれているチェックポイントファイル情報に基づきます。バックアップセッションが失敗すると、最後にバックアップされたファイルは内部データベース内にチェックポイントとしてマークされます。このため、バックアップセッションを再開すると、バックアップセッションは失敗した場所から続行できます。失敗した場所にあるファイルが最初からバックアップされ、残りのデータは元のバックアップセッションにその増分バックアップとして追加されます。再開されたセッションは、元のセッションのオプションを自動的に継承します。

チェックポイントとしてマークされたファイルがファイルシステムから削除された場合でも、再開機能はバックアップされていないデータを判断できます。バックアップセッションが正常に完了するまで、失敗したバックアップセッションは何度でも再開できます。

グラフィカルユーザーインターフェイスでは、失敗したセッションのコンテキストメニューを使用してセッションを再開できます。コマンドラインインターフェイスでは、`omnib -resume`オプションを使用してセッションを開始できます。

制限事項

- 再開はディザスタリカバリではサポートされていません。
- 再開は、NDMPメディアデータ形式オブジェクトを含むセッションではサポートされていません。
- 次のバックアップクライアントシステムでバックアップされたオブジェクトは再開できません: Solaris 9、SCO OpenServer、OpenVMS。

ファイルシステムの復元セッション

ファイルシステム復元セッションのセッション再開機能は、復元セッション中に作成されるチェックポイントファイルに基づいています。このファイルには、セッションで使用される復元オプションと、正常に復元されたファイルが記録されています。新しいファイルが復元されると、すぐに該当するチェックポイントファイルが更新されます。

デフォルトでは、チェックポイントファイルはCell Managerとあて先クライアントの両方に作成されます(復元オプションに関する情報を含むチェックポイントファイルはCell Manager上にのみ作成されます)。

Cell Manager上のチェックポイントファイルは、次の場所に作成されます。

Windowsシステムの場合: `\config\server\sessions\checkpoint`

UNIXシステムの場合: `/var/opt/omni/server/sessions/checkpoint`

クライアント上のチェックポイントファイルは、デフォルトのData Protector一時ファイルディレクトリの`Checkpoint`サブディレクトリに作成されます。

機能の動作方法

失敗した復元セッションを再開する場合、Data Protectorはチェックポイントファイルから情報を読み込んで、失敗した復元セッションが中止したところから復元を続行します。実際には、復元セッションを再開すると、そのセッションのチェックポイントファイルが再開した復元セッションのチェックポイントファイルディレクトリに移動され、チェックポイントファイルの更新が続行されます。その結果、失敗した復元セッションは一回のみ再開できます。失敗したセッションを2度目に再開しようとすると、チェックポイントファイルがないため操作が失敗します。

考慮事項

- クラスター環境では、チェックポイントファイルを必ず共有ディスクに作成して、両方のクラスターノードがファイルにアクセスできるようにします。チェックポイントファイルの場所を変更するには、`OB2CHECKPOINTDIR` omnircオプションを使用します。オプションは、両方のクラスターノードに設定する必要があり、同じディレクトリを指し示す必要があります。
- チェックポイントファイルが作成されないようにするには、復元セッションを開始する前に、**[再開可能な復元を有効化]**オプションをクリアします(このオプションは、復元ウィザードの最後の[復元セッションの開始]ダイアログボックスにあります)。ただし、この場合、復元セッションが失敗すると、チェックポイントファイルがないため再開することはできません。正常に完了したセッションも、セッションの最後にData Protectorによりチェックポイントファイルが削除されるため、再開できません。
- 再開した復元セッションが正常に完了しなかった場合も、再開可能です。これは、再開済み復元セッションがチェックポイントファイルを元のセッションから引き継ぐためです。したがって、このセッションは**[再開可能な復元を使用可能にする]**オプションなど、元のセッションで使用されていたすべての復元オプションを引き継ぎます。
- 復元セッションがIDBから削除されると(デフォルトではセッションは30日後に削除されます)、そのチェックポイントファイルも削除されます。`omnidbinit`コマンドでIDBを初期化した場合も、チェックポイントファイルは削除されます。
- 失敗したセッションで**[上書きしない]**オプションを使用してオブジェクトが復元されていた場合、そのセッションを再開する前に、`omnirc`オプション`OB2NOOVERWRITE_TRAVERSEDIROBJ`を1に設定する必要があります。

制限事項

- あて先クライアントがクラッシュしたために復元セッションが失敗した場合、セッション再開機能が正常に機能しない可能性があります。これは、クライアントがクラッシュしたときにチェックポイントファイルがメモリからディスクに正常にフラッシュされたかどうかによります。
- ハードリンクされたファイルを復元している最中に復元セッションが失敗した場合、セッションの再開機能で残りのハードリンクされたファイルを復元できない可能性があります。これは、バックアップ中にData Protectorがハードリンクされたファイルを1回しかバックアップしないためです。ハードリンクされているその他のファイルの場合、ファイルへの参照のみをバックアップします。つまり、ハードリンクされたファイルの復元は相互に連携しているため、ファイルをすべて同時に復元する必要があります。ハードリンクされたファイルを復元する前か、それらを正常に復元した後に復元セッションが失敗する場合、この問題は発生しません。
- たとえば、次のセッションでバックアップされたツリーを復元するとします。フル、増分、増分。バックアップセッションのいずれかで作成されたツリーバックアップオブジェクトが使用できない(例:最後の増分バックアップセッション内で使用されたバックアップメディアが破損したなど)ために復元セッションが失敗する場合、そのバックアップオブジェクトのコピーを提供する必要があります。そのようなオブジェクトコピーが存在

しない場合、失われたバックアップオブジェクトの合成フルバックアップが存在したとしても、失敗した復元セッションを再開できません。

Data Protector Oracle Server統合バックアップおよび復元セッション

Data Protector Oracle Server統合バックアップおよび復元セッションのセッション再開機能は、『*HPE Data Protectorインテグレーションガイド*』に記載されています。

失敗したセッションを再開する

バックアップセッションや復元セッションがネットワーク接続の問題などによって正常に完了しなかった場合、Data Protectorのセッション再開機能を使用して再開できます。失敗したセッションを再開する場合、Data Protectorは、失敗したセッションが中止されたところから始めて、バックアップまたは復元を続行します。

前提条件

- Data Protector Admin ユーザーグループに追加されているか、Data Protectorモニターユーザー権限が付与されていることが必要です。

手順

1. 通常のCell Managerを使用している場合、コンテキストリストで**[内部データベース]**をクリックします。

   Manager-of-Managersを使用している場合は、コンテキストリストで**[クライアント]**を選択し、**[エンタープライズクライアント]**を展開します。問題のセッションのCell Managerを選択します。[ツール]メニューの**[データベース管理]**を選択します。新しいData Protector GUIウィンドウに、[内部データベース]コンテキストが表示されます。
2. Scopingペインで**[内部データベース]**を展開し、**[セッション]**をクリックします。

   [結果エリア]に、セッションのリストが表示されます。各セッションのステータスが[ステータス]列に示されます。
3. 失敗したセッションを右クリックして、**[セッションの再開]**を選択します。

拡張復元タスク

復元は、さまざまな方法で制御できます。Data Protectorでは、WindowsシステムおよびUNIXシステムに対応した拡張復元タスクをサポートしています。

前提条件

- 復元を行うには、適切なユーザー権限が必要です。この権限は、ユーザーグループに基づいて定義されます。
- 拡張復元タスクを実施する前に、標準復元手順を考慮してください。

拡張復元タスク

拡張復元タスクでは、あまり頻繁に使用されないオプションを指定したり、標準復元手順とは異なる操作を実行することができます。拡張復元タスクを行う場合でも、データの復元時には標準復元手順に含まれる操作の大半を実行する必要があります。

標準復元手順にどの程度まで従うかは、実行する拡張タスクによって異なります。たとえば、ブラウズすることなくデータを復元できます。このとき、必要なファイルの指定は別の方法で行う必要がありますが、その他の点については標準復元手順どおりです。

- 復元対象から除外するファイルを指定する
- 条件に一致するファイルだけを復元対象として選択する
- 開いているファイルを復元対象に指定する
- 復元中のファイルへのアクセスを拒否する
- 復元対象のファイルを検索する
- Windowsの共有ディスクを復元対象に指定する
- 複数のオブジェクトを並行して復元する
- ディスクイメージの復元
- 保管場所に移動したメディアからデータを復元する
- Webサーバーの復元
- ブラウズなしの復元

復元対象から除外するファイルを指定する

Data Protectorでは、バックアップしたファイルのうち復元不要のファイルを復元対象から除外することができます。パターンは、ワイルドカード文字を使って指定できます。

> **注:**
> Data Protectorサーバー用統合ソフトウェアでは、復元対象からのファイルの除外はサポートされていません。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインで、対応するデータの種類(**[ファイルシステム]**など)を展開します。
3. 復元するデータのあるクライアントシステムを展開し、データのあるオブジェクト(UNIXシステムではマウントポイント、Windowsシステムではドライブ)をクリックします。
4. [ソース]プロパティページで、復元するディレクトリを選択します。
5. ディレクトリを右クリックし、**[プロパティ]**をクリックします。
6. **[スキップ]**タブをクリックします。
7. テキストボックスにファイル名を入力するか、またはスキップ対象となるファイルに一致する基準(`*.mp3`など)を入力し、**[追加]**をクリックします。この例では、`mp3`ファイルは復元されません。他にも検索条

件を追加するには、この手順を繰り返します。

8. **[OK]**をクリックします。

条件に一致するファイルだけを復元対象として選択する

Data Protectorでは、バックアップに含まれているファイルのうち、特定のパターンに一致するファイルのみを復元することができます。使用するパターンは、ワイルドカード文字を使って指定できます。

> **注:**
> この機能は、Data ProtectorのNDMPサーバー用統合ソフトウェアではサポートされていません。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインで、データの種類([ファイルシステム]など)を展開します。
3. 復元するデータのあるクライアントシステムを展開し、データのあるオブジェクト(UNIXシステムではマウントポイント、Windowsシステムではドライブ)をクリックします。
4. [ソース]プロパティページで、復元するディレクトリを選択します。
5. ディレクトリを右クリックし、**[プロパティ]**をクリックします。
6. **[復元のみ]**タブをクリックします。
7. テキストボックスにファイル名を入力するか、または復元対象となるファイルに一致する基準(`*.mp3`など)を入力し、**[追加]**をクリックします。これで`mp3`ファイルのみが復元されます。他にも検索条件を追加するには、この手順を繰り返します。
8. **[OK]**をクリックします。

開いているファイルを復元対象に指定する

Data Protectorのデフォルト動作では、他のアプリケーションが使用しているファイル(開いているファイル)は復元対象から除外されます。開いているファイルを復元するには、以下の手順に従ってください。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインで、対応するデータの種類(**[ファイルシステム]**など)を展開します。
3. 復元するデータのあるクライアントシステムを展開し、データのあるオブジェクト(UNIXシステムではマウントポイント、Windowsシステムではドライブ)をクリックします。
4. [ソース]プロパティページで、オブジェクトを展開し、復元対象を選択します。
5. **[オプション]**タブをクリックし、**[使用中のファイルを移動]**オプションを選択します。

復元中のファイルへのアクセスを拒否する

Data Protectorのデフォルト動作では、ファイルをロックせずに復元します。この動作は変更可能です。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインで、対応するデータの種類(**[ファイルシステム]**など)を展開します。
3. 復元するデータのあるクライアントシステムを展開し、データのあるオブジェクト(UNIXシステムではマウントポイント、Windowsシステムではドライブ)をクリックします。
4. [ソース]プロパティページで、オブジェクトを展開し、復元対象を選択します。
5. **[オプション]**タブをクリックし、**[復元時にファイルをロック]**オプションを選択します。

復元対象のファイルを検索する

復元するファイルのフルパス名が不明の場合は、IDBを通じてファイルを検索できます。そのためには、バックアップ時にロギングレベルが、[ファイルレベルまでログに記録]か[すべてログに記録]のどちらかに設定されていることが必要条件となります。ファイル名の一部がわかっている場合は、**[照会ごとに復元]**タスクを使ってファイルとディレクトリを検索することができます。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインの下部にある**[タスク]**ナビゲーションタブをクリックします。定義済みの復元タスクのリストがScopingペインに表示されます。
3. **[照会ごとに復元]**をクリックしてウィザードを起動します。
4. ワイルドカード文字を使用して、ファイル名の一部を指定します。

   たとえば、拡張子が.exeのすべてのバックアップファイルを検索するには、`*.exe`と入力します。

   非ASCII文字を指定する場合は、Data Protector GUIでの現在のエンコードと検索対象のファイルが作成されたときに使用されたエンコードが一致していることを確認してください。一致していないと、Data Protectorでファイルを検索できません。

   UNIX Cell Managerが存在する環境では、ワイルドカード文字`?`を1つだけ使用してマルチバイト文字を検索すると、希望どおりの結果が得られません。複数のワイルドカード文字`?`を指定する必要があります。。たとえば、現在のエンコードで3バイトを使用してマルチバイト文字を表している場合、文字列に`???`を追加します。

   ディレクトリが分かっている場合は、ファイル名のみをパターンで比較します。ディレクトリが分からない場合は、フルパス名をパターンで比較します。
5. 必要に応じて、他のパラメーターを指定します。**[次へ]**をクリックします。
6. 必要に応じて、時間枠と変更時間を指定します。**[次へ]**をクリックします。

   Data Protector指定した条件に一致するファイルとディレクトリがすべて表示されます。
7. 選択条件に一致するファイルのリストから、復元対象のファイルを選択します。他のオプションを指

定するには、対応するタブをクリックします。**[レポートレベル]**、**[ネットワーク負荷]**、および**[再開可能な復元を使用可能にする]**オプションを指定するには、**[次へ]**をクリックします。復元を開始するには、**[完了]**をクリックします。

Windowsの共有ディスクを復元対象に指定する

Data Protectorでは、データのバックアップ元が共有ディスクではなかった場合でも、共有ディスクへの復元を行えます。

以下のような場合は、UNIXまたはWindowsのファイルシステムをWindowsの共有ディスクに復元します。

- システムがData Protectorのセルの一部ではなく、Data Protector Disk Agentがインストールされていない場合。
- Data Protectorで直接サポートされていないプラットフォーム(Windows for WorkgroupsやWindows 3.1など)を復元する場合。
- データを複数のシステムから利用できるようにしたい場合。

バックアップ元とは異なるファイルシステムに(例: UNIXシステムからWindowsシステムへ)データを復元すると、ファイルシステム固有の属性が失われます。

前提条件

復元対象の共有ディスクにアクセスするための適切なパーミッションが付与されるように、Disk Agentクライアント上のData Protector Inetアカウントを変更しておく必要があります。このアカウントには、ローカルクライアントシステムとリモート共有ディスクの両方にアクセスできるパーミッションが付与されていなければなりません。さらに、システムアカウントではなく、特定のユーザーアカウントを使用する必要があります。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインで、適切なデータの種類を展開します。
3. 復元するデータが維持されているクライアントシステムを展開し、データが格納されているオブジェクトをクリックします。
4. [ソース]プロパティページで、オブジェクトを展開し、復元対象を選択します。
5. **[あて先]**タブをクリックします。
6. **[ターゲットクライアント]**ドロップダウンリストで、復元に使用するDisk Agentが稼動しているWindowsクライアントシステムを選択します。

> **ヒント:**
> リモートディスクのUNC共有名を`\\COMPUTER_NAME\SHARE_NAME`の形式(`\\TUZLA\TEMP`など)で**[新しいディレクトリに復元]**テキストボックスに指定して、ネットワークパスを手動で入力すれば、これ以降の手順は不要になります。
>
> UNIXシステム上のGUIを使用している場合は、Windows共有ドライブの存在をシステムから確認したりブラウズしたりすることができないため、この手順が必要になります。したがって、ドライブとディレクトリが使用可能であり、正しく指定されていることを手動で確認してください。このことを確認しておかないと、復元が失敗する可能性があります。

7. **[新しいディレクトリに復元]**オプションを選択し、**[ブラウズ]**をクリックして**[ドライブのブラウズ]**ダイアログボックスを開きます。
8. **[Microsoft Windows Network]**を展開し、データの復元先の共有ディスクを選択します。
9. **[OK]**をクリックします。

複数のオブジェクトを並行して復元する

並行復元では、複数のオブジェクトのデータを複数のディスクまたはファイルシステムに並行して復元できます。メディアの読み取りが実行されるのは1度だけなので、復元速度が向上します

前提条件

同時処理数を2以上に設定して異なるオブジェクトのデータを同じデバイスに転送して作成したバックアップであること。

制限事項

同じオブジェクトを並行して復元することはできません。たとえば、同じ復元に対して、**[復元オブジェクト]**の下であるオブジェクトを選択し、次に**[復元セッション]**の下で同じオブジェクトを含むセッションを選択すると、このオブジェクトは1回だけ復元され、警告が表示されます。

手順

1. 単一のオブジェクトを復元する場合と同様に、復元するデータを選択します。復元先やオプションなどを指定することもできます。
2. Scopingペインの[復元]コンテキストに戻り、復元する他のオブジェクトのデータに対して手順1を繰り返します。
3. **[アクション]**メニューの**[復元の開始]**を選択します。複数のオブジェクトを選択したことが示されます。
4. **[選択したすべてのオブジェクト(並行復元)]**オプションを選択して、**[次へ]**をクリックします。
5. 「セッションの開始」ウィザードの指示に従って、選択内容を確認します。**[次へ]**をクリックします。
6. **[レポートレベル]**、**[ネットワーク負荷]**、および**[再開可能な復元を使用可能にする]**オプションを指定し、**[完了]**をクリックすると、オブジェクトの並行復元が開始されます。

ディスクイメージの復元

ディスクイメージの復元では、ディスクイメージのバックアップを高速に復元します。Data Protectorは、選択したファイルまたはディレクトリではなく、特定の時刻におけるディスクの完全なイメージをセクター単位で復元します。

UNIXまたはWindowsのディスクイメージを復元するには、[復元]コンテキストの**[ディスクイメージ]**オブジェクトを展開し、標準復元手順を使って復元します。

前提条件

- 復元するバックアップの種類は、ディスクイメージでなければなりません。
- UNIXシステムの場合は、ディスクイメージの復元を開始する前にディスクのマウントを解除し、復元の完了後にディスクを再マウントする必要があります。この処理には、実行前/実行後コマンドを使用できます(例: 実行前コマンドとして`umount /dev/rdsk/disk1`、実行後コマンドとして`mount /dev/rdsk/disk1 /mount_dir`)。
- ディスクイメージをバックアップ元とは異なるディスクに復元する場合、復元先のディスクはバックアップ元と同じか、それより大きいサイズでなければなりません。

保管場所に移動したメディアからデータを復元する

保管場所に移動したメディアを使ってデータを復元する手順は、他のメディアから復元する場合とほぼ同じですが、データ保護とカタログ保護の期限が切れている場合は、異なる操作が必要になります。

- ライブラリがある場合は、メディアを入力してスキャンします。
- メディアのカタログ保護がまだ有効であれば、Data Protectorユーザーインターフェイスで復元対象のデータを選択して、データを復元します。
- メディアのカタログ保護期限が切れている場合は、そのメディアにバックアップしたデータに関する情報が内部データベData Protectorースからすでに削除されています。このため、必要なファイルやディレクトリを指定するか、。

> **ヒント:**
> カタログ保護の期限が切れたメディアにバックアップされているファイルとディレクトリの詳細情報を内部データベースに反映させるには、そのメディアをいったんエクスポートしてからインポートし直します。次に、詳細なカタログデータを読み込むように指定します。これにより、Data Protectorユーザーインターフェイスを使ってファイルとディレクトリを選択できるようになります。

Webサーバーの復元

Webサーバーを復元するには、標準復元手順でファイル、ディレクトリ、およびクライアントを復元します。さらに、以下のことを考慮する必要があります。

- すべてのデータをオリジナルの場所に復元する必要があります。
- 構成ファイルとルートディレクトリは常に復元対象に含める必要があります。
- 復元中には、Webサーバーを休止する必要がありますが、オペレーティングシステムは稼動させておく必要があります。復元後にWebサーバーを再起動してください。

OracleやInformix Serverなどのデータベースが Webサーバー上に置かれている場合は、そのデータベースに固有の復元手順を使用してください。

ブラウズなしの復元

データのカタログ保護が期限切れになっていたり、[記録しない]または[ディレクトリレベルまでログに記録]オプションを使ってバックアップを実行した場合は、復元対象のファイルまたはディレクトリを手作業で追加できます。

ファイルやディレクトリの名前がわからない場合は、オブジェクト全体を復元し、その後必要な部分だけを抽出することができます。または、**[復元のみ]**オプションを使って特定の条件を満たすファイルだけを復元し、必要な部分を抽出することで対処できます。

オブジェクト全体を復元して必要な部分を抽出する

復元対象のファイルまたはディレクトリをブラウズ操作で選択できない場合は、オブジェクト全体を復元し、その後、必要な部分だけを抽出することができます。

前提条件

オブジェクト全体を復元するには、オブジェクト全体を十分格納できる大きさの一時記憶域が必要です。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインで、[復元オブジェクト]の下にある適切なデータの種類(**[ファイルシステム]**など)を展開します。
3. 復元するデータが維持されているクライアントシステムを展開し、データが格納されているオブジェクトをクリックします。
4. **[あて先]**タブをクリックします。オブジェクト全体を十分格納できる大きさの一時ディレクトリを選択します。
5. 他の復元プロパティページで、使用するデバイスを選択するなど、必要なオプションを指定します。
6. **[アクション]**メニューを開きます。復元プロセスをプレビューするには**[復元のプレビュー]**をクリックし、復元プロセスを開始するには**[復元の開始]**をクリックします。
7. [セッションの開始]ウィザードで、選択を確認して**[レポートレベル]**オプション、**[ネットワーク負荷]**オプション、**[再開可能な復元を使用可能にする]**オプションを指定します。復元の進捗が復元モニターに表示されます。
8. 復元が完了したオブジェクトのうち、必要な部分だけを抽出して、目的の場所にコピーすることができます。なお、この操作は、Data Protectorのユーザーインターフェイスを使わずに行います。

[復元のみ]オプションを使ってバックアップオブジェクトの一部を復元する

復元対象のファイルまたはディレクトリをブラウズできない場合、パターンを指定することにより、特定のパターンに一致するディレクトリ(またはファイルや上位レベルのディレクトリ)のみを復元できます。これにより、オブジェクトの中で復元対象としない部分が復元されるのを避けることができます。使用するパターンは、ワイルドカード文字を使って指定できます。

> **注:**
> この機能は、Data ProtectorのNDMPサーバー用統合ソフトウェアではサポートされていません。

前提条件

- 上記の機能を十分活用するには、パターンを詳しく指定することが必要です。
- 復元された部分を一時的に保存するための領域が必要です。この領域のサイズは、復元されたオブジェクト部分のサイズによって異なります。つまり、このサイズも、指定するパターンがどれだけ絞り込まれているかに左右されます。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインで、[復元オブジェクト]の下にある適切なデータの種類(**[ファイルシステム]**など)を展開します。
3. 復元するデータが維持されているクライアントシステムを展開し、復元対象のオブジェクトをクリックします。
4. [ソース]プロパティページで復元元のオブジェクトを右クリックして、**[プロパティ]**をクリックします。
5. **[復元のみ]**タブをクリックし、復元対象のファイルのファイル名パターンをテキストボックスに入力して(例:「`*order*40*.ppt`")、**[追加]**をクリックします。複数のパターンを追加して、復元対象ファイルの種類を可能な限り詳しく指定してください。
6. **[OK]**をクリックします。
7. **[あて先]**タブをクリックします。バックアップ対象となるオブジェクト部分を十分格納できる大きさの一時ディレクトリを選択します。
8. 他の復元プロパティページで、使用するデバイスを選択するなど、必要なオプションを指定します。
9. **[アクション]**メニューを開きます。復元プロセスをプレビューするには**[復元のプレビュー]**をクリックし、復元プロセスを開始するには**[復元の開始]**をクリックします。
10. [セッションの開始]ウィザードで、選択を確認して[レポートレベル]オプション、[ネットワーク負荷]オプション、[再開可能な復元を使用可能にする]オプションを指定します。復元の進捗が復元モニターに表示されます。レポートレベルとして"注意域"を選択した場合は、ファイルとディレクトリのリストがIDData ProtectorBカタログに含まれていないため、警告メッセージが表示されます。この警告メッセージが表示されても、復元には影響しません。
11. 復元が完了したオブジェクトのうち、必要な部分だけを抽出して、目的の場所にコピーすることができます。なお、この操作は、Data Protectorのユーザーインターフェイスを使わずに行います。

ファイルまたはディレクトリを手作業で復元する

復元対象のファイルまたはディレクトリをブラウズ操作で選択できない場合は、ファイルまたはディレクトリを手動で指定できます。これは、カタログ保護が期限切れになっていた場合や、**[記録しない]**オプションを使用してバックアップを行っていた場合に発生します。

前提条件

ファイルまたはディレクトリを手動で追加するには、ファイルまたはディレクトリの正確なパスおよび名前を指定する必要があります。ファイル名およびパス名の大文字と小文字は区別されます。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインで、[復元オブジェクト]の下にある適切なデータの種類(**[ファイルシステム]**など)を展開します。
3. 復元するデータが維持されているクライアントシステムを展開して、手動で復元したいファイルまたはディレクトリが格納されているオブジェクトを右クリックし、**[プロパティ]**をクリックします。
4. **[復元サマリー]**タブをクリックし、パスの欠落部分と目的のファイルまたはディレクトリの名前をテキストボックスに入力します。
5. **[追加]**をクリックして設定内容を確定します。[バージョン]ウィンドウが表示されます。
6. [バージョン]ドロップダウンリストから目的のバックアップバージョンを選択し、**[OK]**をクリックします。オブジェクト名とバージョンが表示されます。
7. 他の復元プロパティページで、使用するデバイスを選択するなど、必要なオプションを指定します。
8. **[アクション]**メニューを開きます。復元プロセスをプレビューするには**[復元のプレビュー]**をクリックし、復元プロセスを開始するには**[復元の開始]**をクリックします。
9. [セッションの開始]ウィザードで、選択を確認して**[レポートレベル]**オプション、**[ネットワーク負荷]**オプション、**[再開可能な復元を使用可能にする]**オプションを指定します。

復元の進捗が復元モニターに表示されます。レポートレベルとして"注意域"を選択した場合は、ファイルとディレクトリのリストがIDData ProtectorBカタログに含まれていないため、警告メッセージが表示されます。この警告メッセージが表示されても、復元には影響しません。

復元オプション

Data Protectorは、復元を微調整するための総合的な復元オプションを備えています。復元オプションにはすべて、通常の復元に適したデフォルト値(オンまたはオフ)があります。

以下のオプションは、オブジェクト別に設定されます。実際に利用できる復元オプションは、復元対象のデータの種類によって異なります。

オプションの詳細については、『HPE Data Protectorヘルプ』を参照してください。

全般的な復元オプション

- **フルチェーンを表示:** 復元チェーンのすべてのファイルおよびディレクトリを表示します。デフォルトでは、このオプションが選択されていて、復元チェーン全体が復元されます。
- **このセッションのみを表示:** このセッションでバックアップされたファイルおよびディレクトリのみを表示します。これによって、復元チェーン全体を復元することなく、増分バックアップセッションからのファイルとディレクトリを復元できます。このオプションは、デフォルトで無効になっています。
- **ターゲットクライアント**: デフォルトでは、バックアップ元のクライアントシステムにデータが復元されます。セル内の他のシステムをドロップダウンリストから選択できます。選択したクライアントシステム上でDisk Agentが起動され、そのシステムにデータが復元されます。

  別のクライアントシステムへの復元を行うには、**[別のクライアントへ復元]**のユーザー権限が必要です。
- **削除済みファイルを除外**: このオプションが適切に機能するには、Cell Managerの時刻と、データを復元するシステムの時刻が同期している必要があります。

このオプションをオンにすると、Data Protectorにより、最後の増分バックアップセッションの時刻にバックアップされたディレクトリツリーの状態が再作成されます。それ以降に作成、または変更されたファイルは維持されます。フルバックアップ(復元チェーンを定義する初期セッション)から指定の増分バックアップまでの間に削除されたファイルは復元され、以降の増分復元中にフォルダー復元の時点で削除されます。

このオプションをオフにすると、Data Protectorにより、フルバックアップイメージに含まれ、フルバックアップ(復元チェーンを定義する初期セッション)と選択された増分バックアップ間に削除されたファイルも復元されます。

[別名で復元]や**[復元先]**をこのオプションとともに使用する場合には、既存ファイルを誤って削除しないように、復元位置を慎重に選んでください。

デフォルト: 選択されていません。

- **使用中のファイルを移動**: このオプションでは、復元でディスク上のファイルを置き換えるときに、そのファイルをアプリケーションが使用している場合の処理を設定します。このオプションは、アプリケーションまたは他のプロセスでの使用中にオペレーティングシステムによってロックされるファイルに適用されます。このオプションは、**[最新ファイルを保持]**オプションまたは**[上書き]**オプションとともに使用します。

  このオプションは、デフォルトで無効になっています。

  UNIXシステムの場合、使用中のファイル`filename`が`#filename`に移動されます(ファイル名の先頭に#記号が付加されます)。アプリケーションは、ファイルを閉じるまでそのままファイルの使用を続行します。その後で、復元したファイルが使用されます。

  Linuxシステムでは、このオプションはサポートされません。

  Windowsシステムの場合、ファイルは`filename.001.`として復元されます。ファイルを使用していたアプリケーションは、古いファイルをそのまま使用します。システムの再起動後は、古いファイルが復元されたファイルに置き換えられます。

- **復元されたデータをリスト**: オブジェクトの復元中に、ファイルやディレクトリの名前がモニターウィンドウに表示されます。このオプションは、デフォルトで無効になっています。

- **統計情報の表示**: バックアップまたは復元されている各オブジェクトに関する統計情報(サイズやパフォーマンスなど)が報告されるようになります。これらの情報は、モニターウィンドウで表示できます。このオプションは、デフォルトで無効になっています。

- **不要なオブジェクトバージョンの省略**: このオプションは、復元用にディレクトリが選択され、バックアップが**[すべてログに記録]**または**[ファイルレベルまでログに記録]**のロギングレベルで実行されている場合に適用されます。

  このオプションを選択すると、Data Protectorは復元チェーンの各バックアップについて、IDB内に復元するファイルがあるかどうかをチェックします。復元するオブジェクトバージョンが存在しないバックアップはスキップされます。このチェックには時間がかかる場合があることに留意してください。

  このオプションを選択しないと、前回のバックアップから変更がない場合でも、復元チェーン内の各バックアップが読み込まれます。

  空のディレクトリを復元する場合は、このオプションをクリアします。

  デフォルト: 選択されています。

- **スパースファイルの復元**: スパースファイルを元の圧縮形式で復元します。スパースファイルを元の形式で復元しない場合は、ディスク消費量が多くなることがあります。このオプションは、デフォルトで無効になっています。

  このオプションは、UNIXのスパースファイルにだけ適用されます。Windowsのスパースファイルは、必ずスパースファイルとして復元されます。

- **復元時にファイルをロック**: 復元中にファイルへのアクセスを拒否します。このオプションは、デフォルトで

無効になっています。

- **時刻属性の復元:** 復元する各ファイルの時刻属性の値を保持します。このオプションを無効にすると、復元するオブジェクトの時刻属性が現在の日時に設定されます。このオプションは、デフォルトで有効になっています。
- **保護属性の復元**: 復元する各ファイルの元の保護属性を保持します。このオプションを無効にすると、現在の復元セッションの保護属性が適用されます。このオプションは、デフォルトで有効になっています。

  Windowsシステムの場合、このオプションはファイル属性にのみ適用されます。このオプションの設定に関係なく、セキュリティ情報は常に復元対象になります。
- **ディレクトリ共有情報の復元:** 復元するディレクトリの共有情報を指定します。このオプションは、デフォルトで選択されています。

  バックアップ時にディレクトリがネットワークで共有されている場合、このオプションが選択されている場合は復元後もそのディレクトリは共有されます。ただし、そのバックアップで**[ディレクトリ共有情報のバックアップ]**オプションが選択されていた場合です。

実行前/実行後コマンド

- **実行前:** 各オブジェクトの復元を開始する前に実行するコマンド(またはスクリプト)を入力することができます。Data Protectorが復元を続行するには、このコマンド(またはスクリプト)が正常に終了する必要があります。

  実行前コマンド(またはスクリプト)は、Disk Agentを実行中のクライアントシステムで実行されます。Windowsシステムの場合、スクリプトを*Data_Protector_home*\binディレクトリまたはそのサブディレクトリに格納する必要があります。UNIXシステムの場合、スクリプトを/opt/omni/lbinディレクトリまたはそのサブディレクトリに格納する必要があります。

  Windowsシステムでサポートされている実行前スクリプトの拡張子は、.bat、.exe、および.cmd のみです。サポートされていない拡張子(.vbsなど)を使用した実行前スクリプトを実行するには、そのスクリプトを起動するバッチファイル(.bat)を作成します。そして、そのバッチファイルを実行前コマンドとして実行するようにData Protectorを構成します。これにより、サポートされていない拡張子のスクリプトが起動されます。
- **実行後**: 各オブジェクトの復元が完了した後に実行するコマンド(またはスクリプト)を入力することができます。実行後コマンド(またはスクリプト)は、Disk Agentを実行中のクライアントシステムで実行されます。

デバイスの選択

- **デバイスの自動選択:** 元のデバイスが復元またはオブジェクトコピーに使用できない場合に適用されます。このオプションを選択すると、元のデバイスと同じデバイスタグを持ち、復元またはオブジェクトコピー用に選択されている他のデバイスが、使用できないデバイスの代わりに自動的に使用されます。元のデバイスの代わりに使用できるデバイスの数が不足している場合は、バックアップ時に使用されたより少ない数のデバイスで復元またはオブジェクトコピーが開始されます。

  デフォルトでは、Data Protectorはまず元のデバイスの使用を試みます。元のデバイスが復元またはオブジェクトコピー用に選択されていない場合、グローバルオプションが考慮されます。代替デバイスを先に使用するか、元のデバイスをいっさい使用しないようにするには、グローバルオプション AutomaticDeviceSelectionOrderを変更します。

Data Protector SAP MaxDB、DB2 UDB、Microsoft SQL Server、およびMicrosoft SharePoint Server 2007/2010/2013用の統合ソフトウェアでは、使用可能なデバイス数がバックアップ中に使用されたデバイス数以上であることを確認してください。

デフォルト: 選択されています。

- **元のデバイスの選択**: 元のデバイスが復元またはオブジェクトコピーの時点で使用できない場合に適用されます。このオプションを選択すると、Data Protectorは選択されたデバイスが使用可能になるまで待機します。

  これは、Data Protector SAP MaxDB、IBM DB2 UDB、Microsoft SQL Server、およびMicrosoft SharePoint Server 2007/2010/2013用統合ソフトウェアで推奨されるオプションです。

  デフォルト: 選択されていません。

ファイルの重複を処理する

- **最新ファイルを保持** このオプションを選択すると、ファイルの最新バージョンが維持されます。ディスク上のファイルがバックアップされたバージョンよりも新しければ、バックアップされたバージョンは復元されません。ディスク上のファイルがバックアップされたファイルよりも古い場合は、そのファイルはバックアップされたファイルで上書きされます。このオプションは、デフォルトで有効になっています。
- **上書きしない:** このオプションを選択すると、ディスク上の既存のファイルが維持されます。つまり、バックアップに含まれているバージョンで既存のファイルが上書きされることがなくなります。存在しないファイルだけが、バックアップから復元されます。このオプションは、デフォルトで無効になっています。
- **上書き**このオプションを選択すると、ディスク上の既存のファイルがバックアップに含まれているファイルに置換されます。このオプションは、デフォルトで無効になっています。

Active Directory固有のオプション

複製モード

- **権限付き:** Active Directoryの復元に適用するWindows Server固有のオプションです。Active Directoryデータベースは、復元後に更新されず、復元されたデータによってターゲットでの既存データが上書きされます。権限付きの復元を行うには、復元セッション終了後にコマンドプロンプトから `ntdsutil.exe`を実行する必要があります。
- **権限なし:** Active Directoryデータベースは、復元後に通常の複製テクニックを使用して更新されます。**[権限なし]**オプションは、デフォルトの複製モードです。
- **プライマリ:** [プライマリ]複製モードでは、NTディレクトリサービスをオンラインのまま保持できます。このモードは、`FileReplicationService`をActive Directoryサービスと同時に復元する場合に使用します。複製した共有のすべての複製パートナーが失われている場合は、このオプションを使用する必要があります。Certificate ServerとActive Directoryサーバーの場合は、**[プライマリ]**は**[権限付き]**と同じになります。

復元オプションを設定する

復元対象のデータを選択した後、復元オプションを設定できます。復元オプションには、通常の復元に適したデフォルト値(オンまたはオフ)があります。利用可能な復元オプションの組み合わせは、復元する

データの種類によって異なります。たとえば、ファイルシステムの復元で使用可能な復元オプションは、ディスクイメージの復元では使用できません。

手順

1. コンテキストリストで**[復元]**をクリックします。
2. Scopingペインで、[復元オブジェクト]の下にある適切なデータの種類(**[ファイルシステム]**など)を展開します。
3. 復元するデータのあるクライアントシステムを展開し、データのあるオブジェクト(UNIXシステムではマウントポイント、Windowsシステムではドライブ)をクリックします。
4. [ソース]プロパティページで、復元対象のデータを選択します。
5. **[オプション]**タブをクリックして[オプション]プロパティページを表示します。オプションの横にあるボックスをクリックして、そのオプションを選択または選択解除します。

Windowsシステムの復元について

Data Protectorは、Windowsファイルシステムを復元する際に、ファイルおよびディレクトリ内のデータと、ファイルおよびディレクトリに関するWindows固有の情報を復元します。

以下のWindows固有の情報が復元されます。

- 完全なUNICODEファイル名
- FAT16、FAT32、VFAT

  NTFS属性
- 代替データストリームセット
- 共有情報

  バックアップ中にディレクトリがネットワークで共有されている場合、共有情報はバックアップメディアに保存されます。デフォルトでは、ディレクトリは復元後もネットワークで共有されます。ただし、同じ共有名の共有ディレクトリがすでにある場合は該当しません。復元するディレクトリの共有情報を復元しないようにするには、[ディレクトリ共有情報の復元]オプションの選択を解除します。

  ディレクトリ共有情報の復元には、[ファイル重複時の処理]オプションも適用されます。たとえば、[上書きしない]復元オプションを復元に使用すると、ディスク上に存在するディレクトリのディレクトリ共有情報が維持されます。
- NTFS代替データストリーム
- NTFSセキュリティデータ

NTFS 3.1ファイルシステムの機能

- NTFS 3.1ファイルシステムは、再解析ポイントをサポートしています。

  ボリュームマウントポイント、単一インスタンス記憶域(SIS)、およびディレクトリの接続は、再解析ポイントのコンセプトに基づいています。これらの再解析ポイントは、他のファイルシステムオブジェクトと同様に選択できます。
- NTFS 3.1ファイルシステムでは、Windows VistaおよびWindows Server 2008オペレーティングシステムで導入されたシンボリックリンクがサポートされます。

Data Protectorは、NTFS再解析ポイントと同じ方法でシンボリックリンクを処理します。

- NTFS 3.1ファイルシステムは、ディスクスペースの割り当て量を効率的に低減する手段としてスパースファイルをサポートしています。

  これらのファイルは、ディスクスペース節約のためスパースファイルとしてバックアップされます。スパースファイルのバックアップと復元は、NTFS 3.1ファイルシステムに対してのみ可能です。
- NTFS 3.1ファイルシステム固有の機能の一部は、独自のデータレコードを維持するシステムサービスによって制御されています。これらのデータ構造は、CONFIGURATIONの一部としてバックアップされます。
- 暗号化ファイル

  Microsoft方式で暗号化されたNTFS 3.1ファイルは暗号化された状態でバックアップと復元が行われ、そのファイルの中身は復号化されて初めてその内容が正しく表示されます。
- 圧縮ファイルはバックアップされ、圧縮状態で復元されます。

バックアップ元と異なる種類のファイルシステムにデータを復元する場合は、復元に対するファイルシステムの制限事項を考慮する必要があります。

共有ディスクとしてバックアップされたオブジェクトの復元

共有ディスクとしてバックアップされたオブジェクトは、そのバックアップに使用されたDisk Agentクライアントに関連づけられています。環境が変化していない場合、Windowsローカルファイルシステムと同じように共有ディスクを復元することができます。デフォルトの場合、共有ディスクのバックアップに使用されたのと同じDisk Agentクライアントを使って、データが元の位置に復元されます。

Windowsファイルシステムの復元に対する制限事項

バックアップが実行された種類とは別のファイルシステムの種類にデータを復元することができます。

開始	この行を、以下のように変更します。				
	FAT32	FAT16	CDFS	UDF	NTFS 3.1 [1]
FAT32	FC	FC	該当なし	該当なし	FC
FAT16	FC	FC	該当なし	該当なし	FC
CDFS	FC	FC	該当なし	該当なし	FC
UDF	FC	FC	該当なし	該当なし	FC
NTFS 3.1 [2]	*	*	該当なし	該当なし	FC

[1] Windows XP、Windows Vista、Windows 7、Windows 8、Windows Server 2003、Windows Server 2008、およびWindows Server 2012で使用されます。
[2] Windows XP、Windows Vista、Windows 7、Windows 8、Windows Server 2003、Windows Server 2008、およびWindows Server 2012で使用されます。

凡例	
FC	完全互換(Full Compatibility): ファイル属性が完全に維持されます。
*	再解析ポイント、スパースファイル、および暗号化ファイルは復元されません。ファイルの復元時に、セキュリティ情報と代替データストリームが失われます。

表に示したように、NTFS 3.1ファイルシステムオブジェクトはNTFS 3.1ファイルシステムに対してのみ完全に復元できます。バージョンが異なるファイルシステムに復元すると、ファイルシステム固有の属性と代替データストリームが失われます。

- Windowsの再解析ポイント(ディレクトリ接続点やボリュームマウントポイントなど)は、NTFS 3.1ファイルシステムに対してのみ復元可能です。UNIXの再解析ポイントをNTFS 3.1ファイルシステムに復元することはできません。
- SIS再解析ポイントが含まれているNTFS 3.1ファイルシステムを復元すると、ディスクが満量状態になることがあります。これは、オリジナルのファイルを複数のターゲットファイルに復元した結果、ディスクの空き容量がなくなった場合に発生します。
- スパースファイルは、NTFS 3.1ファイルシステムに対してのみスパースファイルとして復元されます。
- Data Protectorを使ってユーザーディスククォータを復元することはできません。
- ユーザーがスパースファイルをNTFS 3.1ファイルシステム以外のファイルに復元しようとすると、Data Protectorが警告メッセージを表示します。NTFS 3.1以外のファイルシステムに復元したスパースファイルには、ゼロセクションが含まれません。
- Microsoft方式で暗号化されたNTFS 3.1ファイルは、他のファイルシステムのドライバーで復元できないため、NTFS 3.1ファイルシステムにしか復元できません。

構成データの復元

Windows CONFIGURATIONを復元するには、`CONFIGURATION`オブジェクトまたはその一部を選択し、標準の復元手順を実行します。

CONFIGURATIONは、システムの動作に影響を及ぼすデータ構造で構成されています。したがってシステムは、このような復元処理に対応できなければなりません。そのための前提条件は、CONFIGURATION項目の内容とWindowsオペレーティングシステムのバージョンによって異なります。

制限事項

- Active DirectoryとSysVolはペアで復元しなければなりません。
- Data Protectorを使ってユーザーディスククォータを復元することはできません。Microsoft社製ユーティリティを使うと、バックアップされた情報を手動で復元できます。
- Data Protectorを使用して単一の構成オブジェクトを復元することはできますが、**お勧めできません**。**ディザスタリカバリ**手順の一部として、完全な構成オブジェクトの復元を実行することを強くお勧めします。

Windowsの構成オブジェクト

構成オブジェクトの詳細については、HPE Data Protectorヘルプを参照してください。

- Active Directoryサービス
- 証明書サーバー
- COM+クラス登録データベース(`ComPlusDatabase`)
- DFS
- DHCP
- DNSサーバー
- イベントログ
- ファイル複製サービス
- Internet Information Server (IIS)
- ユーザープロファイル(`Documents and Settings`)
- Windowsレジストリ
- リムーバブル記憶域の管理データベース
- SystemRecoveryData
- SysVol
- ターミナルサービスデータベース
- ユーザーディスククォータ(`QuotaInformation`)
- WINSサーバー

復元したデータを有効にするには、CONFIGURATIONオブジェクト全体の復元が終了してからシステムを再起動してください。

一部のオブジェクトについては、扱いに注意が必要で、付加的なタスクが必要になることがあります。

Active Directory

Active Directoryサービスを復元するには、ディレクトリサービス復元モードの[スタートアップ]オプションを使ってシステムを再起動する必要があります。システムをディレクトリサービス復元モードで起動すると、ドメインユーザーアカウントを使用できなくなります。ローカルシステムアカウントを使ってログオンするようにData Protector Inetと`crs`サービス(Cell Manager用)を構成し、サービスを再開してください。Active Directoryを復元すると、FRS(ファイル複製サービス)およびDFS(分散ファイルシステム)も復元されます。

Active Directoryは、以下の3つの複製モードのいずれかで復元できます(Windows固有オプション)。

- 権限なし
- 権限付き
- プライマリ

> **注:**
> **権限付き**モードで復元を実行するには、復元セッション終了後に`ntdsutil.exe`を実行する必要があります。たとえば、典型的な権限付き復元を実行するには、コマンドプロンプトに`ntdsutil`、`authoritative restore`、restore databaseの各コマンドを順に入力します。サーバーを再起動し、複製が行われるまで待機します。

> **ヒント:**
> Active Directoryの権限付き復元に必要な追加のアクションを実行する実行後コマンドを作成す

ることもできます。たとえば、ディレクトリ全体の権限付き復元を実行するには、次のような行を入力します。

```
ntdsutil "popups off" "authoritative restore" "restore database" quit quit
```

DFS

Data Protectorでは、WindowsのDFS(分散ファイルシステム)を以下のいずれかの項目の一部として復元します。

- Windowsレジストリ ー DFSがスタンドアロンモードで構成されている場合
- Windows Active Directory ー DFSがドメインモードで構成されている場合

プロファイル

- ユーザープロファイルは、各ユーザーが対話形式またはサービスとしてログオンしている場合は正しく復元できません。ユーザーが復元時にログオンした場合、Data Protectorはユーザーのレジストリのあるハイブを格納するNTUSER.DATファイルを復元できません。

  システムをログオフし、復元したいプロファイルが属するユーザーアカウントで実行されているサービスを停止する必要があります。別のシステムから復元セッションを開始することも、別のユーザーとして復元ターゲットシステムにログインして復元セッションを開始することもできます。
- すべてのユーザープロファイルを復元するには、ローカルシステムのアカウントで実行されていないサービスをすべて終了して、システムからログオフする必要があります。その後、別のクライアント上でData Protector GUIを使って、復元セッションをリモートで開始します。
- ユーザープロファイルは、システム上に定義されている場合にかぎり復元できます。既存のユーザープロファイルや削除されたプロファイルの個々のファイルの復元は、これらのファイルがシステムのプロファイルに存在している限り可能です。ユーザープロファイルをコントロールパネルから削除していたり、何か別の理由でシステム上に存在しない場合は、復元が正常に実行されず、以下のエラーメッセージが出力されます。

  ```
  [84:208] Configuration object not recognized by the system => not restored.
  ```

  このようなユーザープロファイルを復元するには、まずこのプロファイルのユーザーとしてログオンして、プロファイルを再作成する必要があります。システムによって、このユーザーのプロファイルにディレクトリが割り当てられ、デフォルトのプロファイルが作成されます。復元したファイルをマージされないようにするには、新たに作成されたファイル内のファイルを復元セッション実行前に削除します。次にログオフし、別のユーザーとしてログインするか、別のシステムを使用することによって、復元セッションを開始します。別のユーザー名をシステムが割り当てることがあります。この場合は、**[別名で復元]**オプションを使用し、新しく割り当てられた位置にファイルを復元します。
- ユーザープロファイルが復元されると、復元に関する仕様の[ファイル重複時の処理]オプションの指定に関係なく、ファイルは常に上書きされます。さらに、**[削除済みファイルを除外]**オプションは使用できません。現在ディスク上に存在していて、バックアップ時には存在しなかったファイルは、復元後もユーザープロファイル内に残ります。
- またユーザープロファイルは、**[別名で復元]**オプションを通じて復元できます。ファイルの一時的な保存場所を指定して、目的のファイルをユーザープロファイルのディレクトリに手動でコピーします。または、ユーザープロファイルのディレクトリに直接復元するには、**[使用中のファイルを移動]**オプションを使用します。これにより、ログオンしているユーザーによってファイルが使用中であっても、ユーザープロファイルを復元できます。ただしこの場合、使用中のファイルが置き換えられるのは、システムの再ブート後になることに注意してください。

レジストリ

Windows Registry全体を復元対象として選択した場合、レジストリキーの中には復元されないものや、復元時に特殊な方法で処理されるものがあります。これは、オペレーティングシステムがこれらのキーを使用しているためです。このようなキーは、以下のレジストリキーの下にあります。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\KeysNotToRestore

リムーバブル記憶域マネージャー データベース

取り外し可能記憶デバイス(CDを除く)が接続されているすべてのシステムでRSMサービスが稼動している必要があります。

サーバー構成オブジェクト

対応するサーバーがターゲットシステム上にインストールされ、稼動していなければなりません。Certificate Server以外のすべてのサーバーでは、データがオンラインで復元されます。

Certificate Serverのデータはオフラインで復元されます。復元を開始する前に、Certificate Serverサービスを停止してください。Certificate Serverの復元に使用できるモードは、権限付きモードだけです。

SysVol

SysVolの復元は、以下の3つのモードのいずれかで実行できます。

- 権限なし

  ドメイン内のドメインコントローラーが少なくとも1つ使用可能で動作していれば、ファイルは元の位置に復元されます。復元データは他のドメインコントローラーには伝播されません。

- 権限付き

  不可欠なSysVolデータがローカルドメインコントローラーから削除され、その削除が他のドメインコントローラーに伝播した場合は、権限付きの復元を実行します。

- プライマリ

  ドメイン内のドメインコントローラーをすべて喪失してしまい、ドメインコントローラーをバックアップから再構築しようとする場合、プライマリファイルの復元がFRSに通知され、ファイルが元の位置に復元されます。

Windows TCP/IPサービス

Microsoft TCP/IPプロトコルを実行し、WINS Server、DHCP Server、またはDNS Serverとして構成されているWindows Serverでは、ネットワーク通信を管理するサービスを復元することができます。

Windows TCP/IPサービスを復元するには、CONFIGURATION項目を展開してWNS、DHCP、またはDNSServerDatabaseを選択します。

これらのサービスはそれぞれ、復元前に自動的に停止します。

復元が終了したら、システムを再起動してください。

システム状態データの復元

常にシステム状態データの一部であるActive Directoryを使用する場合には、ディレクトリサービス復元モードでシステムを起動する必要があります。

Data Protectorから見たシステム状態データは、いくつかの特定のファイルシステムオブジェクトとCONFIGURATIONオブジェクトで構成されています。Windows Vista、Windows 7、Windows 8、Windows Server 2008、およびWindows Server 2012の場合は、システム状態には、インストールされる追加のサーバーの役割またはサービスに属しているデータも含まれます。「バックアップ」ウィザードでオブジェクトを選択する場合とは異なり、復元対象のオブジェクトの種類ごとに個別の「復元」ウィザードでオブジェクトを選択します。

[ソース]プロパティページで、以下の項目を選択します。

- CONFIGURATIONに所属しているシステム状態オブジェクト
  - `ActiveDirectoryService`
  - `CertificateServer`
  - `Cluster Service information`
  - `IIS Metadirectory`
  - `RemoteStorageService`
  - `RemovableStorageManagementDatabase`
  - `SystemFileProtection`
  - `SYSVOL directory`
  - `TerminalServiceDatabase`
- `SystemVolumeInformation` (システムファイル保護サービスを含む)
- ブートファイル(システムドライブ上)
- 特定のサーバーの役割やサービスに属しているデータが存在するボリューム、あるいはクライアントシステム全体(Windows Vista、Windows 7、Windows 8、Windows Server 2008、またはWindows Server 2012の場合)

復元が終了したら、システムを再起動してください。

リモートストレージサービス

リモートストレージサービス(RSS)は、アクセス頻度の低いファイルをローカルからリモートストレージへ自動的に移動するために使用されます。リモートファイルはファイルを開くと自動的に再呼び出しされます。

RSSデータベースはシステム状態データの一部ですが、復元は手動で行います。RSSデータベースの復元はオフラインで実行しなければなりません。実行前スクリプトおよび実行後スクリプトを追加してサービスの停止と再起動を行うか、復元の前後に手動で停止と再起動を行います。

復元時には以下のディレクトリを選択してください。

%SystemRoot%\system32\RemoteStorage

%SystemRoot%\system32\NtmsData

ファイルシステム保護

システムファイル保護サービスでは、コンピューターの再起動後に、保護されたすべてのシステムファイルのバージョンをスキャンおよび検証します。システムファイル保護サービスでは、保護ファイルが上書きされていることを見つけたら、正しいバージョンのファイルを検索して不正なファイルを置き換えます。Data Protectorでは、保護ファイルを上書きすることなく、バックアップして復元することができます。

UNIXシステムの復元について

バックアップ元の位置にファイルを復元する際、Data Protectorは、ファイル属性を含めてファイルを復元します。

ACL (アクセス制御リスト)など、UNIXシステム上のシステム固有データは、バックアップ元と同じ種類のファイルシステムとオペレーティングシステムにのみ復元されます。

UNIXシステム固有の情報

VxFSデータを復元する場合は、[別名で復元]オプションを使って、希望の場所にデータを復元できます。

HP OpenVMSシステムの復元について

HP OpenVMSファイルシステムの復元には、標準復元手順を使用します。

制限事項

- 他のオペレーティングシステム上に保存されたファイルとディレクトリに関しては、一部の属性が復元されず、ACLは一切復元されません。
- 復元中に作成されたディレクトリのうち、保存対象に含まれていないディレクトリに対しては、ディレクトリ内に最初に復元されたファイルの属性が適用されます。ただし、-no_protectionオプションで無効化した場合は該当しません。
- GUIで入力されるかCLIに渡されるファイル仕様は、UNIXスタイルの構文である必要があります。

  /disk/directory1/directory2/filename.ext.n

  先頭にスラッシュを入力し、ディスク、ディレクトリ、ファイル名をそれぞれスラッシュで区切って入力します。

  ディスク名の後ろにコロンを付けないでください。

  バージョン番号の前には、セミコロンではなくピリオドを使用します。

  OpenVMSファイルのファイル指定では、大文字と小文字が区別されます。以下に例を示します。

  1DGA100:[USERS.DOE]LOGIN.COM';1

  上記は以下の形式で指定する必要があります。

/1DGA100/Users/Doe/Login.Com.1

- 暗黙的なバージョン番号はありません。バージョン番号は常に明示的に指定する必要があります。復元されるのは、復元対象として選択したファイルバージョンだけです。ファイルの全バージョンを復元対象に含めるには、それらをすべてGUIウィンドウ内で選択するか、またはCLIで**[オンリー]** (-only)オプションにファイル指定を含めるときに、次の例のように、すべてのバージョン番号にマッチするワイルドカード文字を入力します。

  /DKA1/dir1/filename.txt.*

- バックアップ元とは異なる場所に復元した場合は、ディスクデバイスと開始ディレクトリだけが変更されます。復元先のパスに元のディレクトリパスを追加したものが新しい復元先のパスになります。
- **[時刻属性の復元]** (-notouch)オプションを無効にして復元を実行すると、ODS-5ディスク上では、最終アクセス日時が現在の日時に更新されます。ODS-2ディスクでは、ファイルに対し、元の日付が設定されます。
- ソフトリンクとして保存されたファイルは、DCL SET FILE/ENTERコマンドに対応するコマンドを使用して復元されます。その場合、データは一切復元されません。入力されたソフトリンクには、このファイルの保存時のプライマリパス/ファイル名が指定されます。プライマリパス/ファイル名が存在しないか、または復元されなかった場合、ソフトリンクの作成は失敗します。

  OpenVMSシステムディスクの復元されたコピーを起動可能にするには、ディスクの復元後に、OpenVMS WRITEBOOTユーティリティを使用してブートブロックを書き込む必要があります

- **[使用中のファイルを移動]** (-move)オプションおよび**[スパースファイルの復元]** (-sparse)オプションは、OpenVMSでは利用できません。
- 拡張ファイルシステム名(大文字と小文字、Unicode文字など)を持つOpenVMSシステムのODS-5ディスクからバックアップしたファイルは、ODS-2ディスクには復元されません。
- **[復元時にファイルをロック]** (-lock)オプションの有効/無効に関係なく、復元中のファイルは常にロックされます。
- 実行前コマンドプロシージャと実行後コマンドプロシージャのデバイスおよびディレクトリは、デフォルトでは/omni$root/binになります。コマンドプロシージャを他の場所に配置するには、デバイスとディレクトリのパスをUNIXスタイルの形式でファイル指定に含める必要があります。例:

  /SYS$MANAGER/DP_SAVE1.COM

- **[保護属性の復元]** (-no_protection)オプションが無効である場合、ファイルはデフォルトのオーナー、保護、およびACLによって作成されます。
- ワイルドカード文字を**[スキップ]** (-skip)または**[オンリー]** (-only)フィルターで指定するとき、複数の文字については'*'を使用し、単一の文字については'?'を使用します。
- OpenVMSシステムでは、ボリュームおData Protectorよびボリュームセット上のディスククォータはサポートされません。

  ディスククォータが有効なボリュームにあるデータの復元を実行するには、実行後スクリプトを構成して復元の開始前に関係するボリュームでディスククォータを無効にし、実行前スクリプトを構成して復元の完了後にディスククォータを有効にします。

復元されるファイルシステム情報

ディレクトリ構造およびファイルが、以下のファイルシステム情報とともに復元されます。

- ファイルおよびディレクトリの属性
- ACL (アクセス制御リスト) ー 使用可能な場合のみ(「制限事項」参照)

- セカンダリファイルエントリ

  OpenVMSファイルシステムバックアップでは、複数のディレクトリエントリがあるファイルは、プライマリパス名を使用して1回だけバックアップされます。セカンダリパスエントリは、ソフトリンクとして保存されます。

  たとえば、OpenVMSシステムディスク上のシステム固有のルートでは、SYSCOMMON.DIR;1パスがソフトリンクとして保存されます。このパスのデータは、[VMS$COMMON...]に保存されます。

  ファイルシステム復元では、これらのセカンダリパスエントリも復元されます。

ファイルは、マウントされているFILES-11、ODS-2、またはODS-5ボリュームに対してのみ復元できます。

第15章: モニター、レポート、通知、Data Protectorイベントログ

監視について

Data Protectorの監視を使用すると、実行中のセッションを管理して、マウント要求に応答できます。セッションの状態、種類、オーナー、セッションID、セッションの開始時間、および対応するバックアップ仕様の名前を表示できます。

対話型のバックアップ、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を実行すると、モニターウィンドウが開き、オブジェクト、バックアップデバイス、およびセッション中に生成されたメッセージが表示されます。ユーザーインターフェイスが閉じている場合でもセッションは継続します。

バックアップまたは復元セッション中に表示されるメッセージのレベルを変更するには、バックアップ仕様の構成中または復元セッションの開始時に、**[レポートレベル]**オプションを変更します。

Manager-of-Managers機能を使うと、複数のセルを同時にモニターできます。

現在実行中のセッションを表示する

[モニター]コンテキストで、現在実行されているセッションを表示できます。

> **注:**
> 現在実行中のセッションは、実行前スクリプトが終了した後で[モニター]コンテキストに表示されます。
>
> 現在実行中のセッションのリストは、一定のリフレッシュ間隔(デフォルトは5秒)で自動的に更新されて、新しいセッションの情報が表示されます。デフォルトのリフレッシュ間隔を変更するには、[ファイル]メニューの**[選択値]**をクリックし、[モニター]タブをクリックします。Cell ManagerとMoMのリフレッシュ間隔は、秒単位で指定できます。

前提条件

Adminユーザーグループに追加されているか、[モニター]のユーザー権限が付与されていることが必要です。

手順

1. コンテキストリストで、**[モニター]**をクリックします。

   [結果エリア]に、現在のセッションのステータスが表示されます。

   > **ヒント:**
   > 対応する列見出しをクリックして、(`status`、`type`、`owner`などを基準にして)セッションをソートできます。VMware用統合ソフトウェアの場合、セッションを`VM name`と`item name`でソートすることもできます。`VM name`とは、vCenterの仮想マシンの名前、`item name`とは、仮想マシンに関連付けられたディスクオブジェクトまたは構成の名前です。

2. 表示する実行中のセッションをダブルクリックします。

> **ヒント:**
> Scopingペインで、[モニター]コンテキストの[結果エリア]から終了したセッションまたは中止されたセッションをすべて削除するには、**[現在のセッション]**をクリックし、[アクション]メニューの**[セッションのクリア]**を選択します。現在のセッションのリストから終了したセッションまたは中止されたセッションを指定して削除するには、セッションを右クリックし、**[リストから削除]**を選択します。完了または中止されたセッションは、Data Protector GUIを再起動すると、自動的に[モニター]コンテキストの[結果エリア]から削除されます。

終了したセッションを表示する

終了したセッションは、[内部データベース]コンテキストで表示できます。

前提条件

Adminユーザーグループに追加されているか、[モニター]のユーザー権限が付与されていることが必要です。

手順

1. コンテキストリストで**[内部データベース]**をクリックします。

   Manager-of-Managersが稼動している場合は、コンテキストリストで**[モニター]**を選択し、内部データベースのコンテキストを表示するCell Managerを選択します。[ツール]メニューの**[データベース管理...]**を選択します。[内部データベース]コンテキストを選択した状態で新しいData Protector GUIが表示されます。
2. Scopingペインで、**[セッション]**を展開し、IDBに保存されているすべてのセッションを表示します。セッションは日付でソートされています。各セッションは、YY/MM/DD形式の日付に一意な番号を付加したIDで識別されます。
3. 特定のセッションを右クリックして**[プロパティ]**を選択すると、そのセッションの詳細が表示されます。
4. **[一般]**、**[メッセージ]**、または**[メディア]** タブをクリックして、それぞれセッションについての一般情報、セッションのメッセージ、またはこのセッションで使われるメディアについての情報を表示します。

実行中のセッションを中止する

バックアップ、復元、またはメディア管理操作を停止する場合は、セッションを中止します。セッションを中止する前にバックアップまたは復元が完了していたデータのバックアップコピーまたは復元データだけが保存されます。

前提条件

adminユーザーグループに追加されているか、[モニター]のユーザー権限が付与されていることが必要です。

手順

1. コンテキストリストで、**[モニター]**をクリックします。現在のセッションの進捗とステータスが[結果エリア]に表示されます。

   Manager-of-Managersを実行している場合は、Scopingペインで**[エンタープライズモニター]**を展開して、監視するCell Managerを選択します。現在のセッションの進捗とステータスが[結果エリア]に表示されます。
2. 列見出しをクリックすると、セッションの順番を並べ替えることができます。
3. セッションを右クリックし、**[中止]**を選択します。

バックアップ用に選択したディスクのサイズを確認中にバックアップセッションを中止した場合、セッションはすぐに中止されません。バックアップは、サイズの確認が終了した(ツリーウォークが完了した)時点で、バックアップが中止されます。

> **ヒント:**
> バックアップ、復元、メディア管理セッションを対話形式で起動した場合は、Data Protectorの[バックアップ]、[復元]、[デバイス/メディア]コンテキストからそれぞれセッションを中止することもできます。

レポートについて

Data Protectorのレポートは、バックアップ環境に関するさまざまな情報を提供します。たとえば、最後に行われたバックアップ、オブジェクトコピー、オブジェクト集約、またはオブジェクト検証の状態のチェック、バックアップ用に構成されていないネットワーク内のシステムのチェック、メディアプール内でのメディア使用状況のチェック、デバイスの状態のチェックなどを行うことができます。

レポートおよびレポートグループは、Data Protector GUIで構成できるほか、Javaをサポートしている任意のWebブラウザーで構成することもできます。レポートグループを使うと、レポートの管理が簡単になり、レポートのスケジュールを設定したり、特定の条件を満たすレポートをグループ化したりできます。

レポートをカスタマイズするためのパラメーターが用意されています。一部のパラメーターでは複数項目の選択が可能です。省略可能パラメーターを指定せずにレポートを構成すると、デフォルト値が適用されます。レポートを構成するときにオプションの入力パラメーター(オプションの選択肢)を指定しないと、デフォルト値が設定されます。デフォルト値は、オブジェクトの場合は`all`、時間枠の場合は`no time limit`となります。レポートまたはレポートグループを構成するには、以下の項目を設定する必要があります。

- レポートの名前
- レポートの種類
- 送信方法
- 受信者
- 形式

その他の入力パラメーターは、レポートの種類によって異なります。

> **注:**
> VADPレポート機能は、デフォルトで有効です。無効化するには、 `EnableDPAforVM`グローバル変数を`0`に設定します。

機能

- 複数のレポートをレポートグループに含めると、それらのレポートをスケジュール設定したり、対話式で開始したり、通知でトリガーしたりできます。
- レポートは、Data Protector GUI、Data Protector CLI、Data Protectorスケジューラー、通知イベント、またはレポートを開始するData Protector CLIが含まれている実行後スクリプトを使って開始できます。
- レポートは、Manager-of-Managers(MoM)機能を使うと、マルチセル構成でも利用できます。
- レポートは、さまざまな形式で出力できます。必要に応じて、入力パラメーターを表示することもできます。

レポートの形式

Data Protectorのレポートは、さまざまな形式で生成できます。

各レポートを個別に開始する場合、レポートはData Protector Managerで表示され、レポート形式を選択する必要はありません。

複数のレポートをレポートグループにまとめる場合は、各レポートの形式と受信者を指定する必要があります。

選択可能なレポート形式は、以下のとおりです。

- **[ASCII]** ー レポートをテキスト形式で生成します。
- **[HTML]** ー レポートをHTML形式で生成します。Webブラウザーでレポートを表示する場合に便利です。たとえば、イントラネットサイト上でシステムがバックアップ済みかどうかを確認するためのリンクを用意することなどが可能です。
- **[ショート]** ー レポートをテキスト形式の要約レポートとして生成します。重要度の高い情報のみが示されます。ブロードキャストメッセージの場合は、この形式をお勧めします。
- **[タブ]** ー フィールドをタブで区切った形式でレポートを生成します。レポートをほかのアプリケーション(Microsoft Excelなど)やスクリプトにインポートして詳細な分析を行う場合に便利です。

レポートの実際の出力は、選択した形式によって異なります。タブ形式でのみすべてのレポートのすべてのフィールドが表示され、他の形式では選択したフィールドだけを表示できます。

レポートの種類

バックアップ環境に関してどのような情報を取得するかに応じて、以下の各種レポートを生成できます。

構成レポート

構成レポートには、Data Protectorセルの構成、バックアップ用に使用されていないデバイス、バックアップ用に構成されていないシステムなどの構成に関する情報が示されます。

セル情報

説明:	Data Protectorセルに関連する情報(クライアント数、バックアップ仕様、メディア管理サーバー、ライセンスサーバー)のリストです。 Data Protector 8.14に導入されたVADP機能は、仮想マシン用の拡張レポートを提供します。VMware仮想マシンは、VADPクライアントと呼ばれるData Protectorクライアントとして表されます。VADPクライアントは、仮想マシンのゲストOSに関する情報を表示します。VMツールをインストールして実行し、VMの電源が投入されている場合、出力のホスト情報セクションには、オペレーティングシステム、IPアドレス、ホスト名などの情報が表示されます。 仮想マシン上に構成するVMホスト名には、DNS名を表示する必要があります。 VMにDNS名がなく、IPv4が使用可能な場合、VMホスト名にIPアドレスを表示する必要があります。 DNS名またはIPアドレスが使用できない場合、またはVMにIPv6アドレスしかない場合、VMホスト名にVM名を表示する必要があります。
必須の選択項目:	なし
省略可能な選択項目:	なし
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`cell_info`

クライアントバックアップ

説明:	指定したクライアントに関する情報のリストです。たとえば、ファイルシステムのうち構成されていないもの、すべてのオブジェクト、および、有効なバックアップ、バックアップ時間、平均サイズが指定されているすべてのオブジェクトなどの情報です。 クライアントバックアップレポートには、アプリケーション統合バックアップオブジェクトやバックアップ仕様についての情報は含まれません。
必須の選択項目:	hostname
省略可能な選択項目:	なし
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`host`

Data Protector向けに構成されていないクライアント

> **注：**
> ネットワークの状態によっては、このレポートが生成されるまでに多少時間がかかることがあります。ただし、この種類のレポートは中止できません。

説明:	選択したドメイン内のクライアントのうち、現在のセルの要素ではないもののリストです。
必須の選択項目:	ネットワーク範囲
省略可能な選択項目:	なし
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`hosts_not_conf`

Data Protectorが使用していない構成済みクライアント

説明:	構成済みのクライアントのうち、バックアップに使用されておらず、デバイスが構成されていないクライアントをすべて示します。
必須の選択項目:	なし
省略可能な選択項目:	なし
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`hosts_unused`

Data Protectorが使用していない構成済みデバイス

`Description:`	構成済みのあて先デバイスのうち、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でまったく使用されないデバイスのリストです。
必須の選択項目:	なし
省略可能な選択項目:	なし
サポートされている形式:	すべての形式

omnirptコマンドのオプション:	dev_unused

ライセンス

説明:	ライセンスの総数と使用可能なライセンス数のリストです。
必須の選択項目:	なし
省略可能な選択項目:	なし
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	licensing

スケジュールのチェック

説明:	今後1年までの間で、指定されている日数以内に開始するようにスケジュールされているバックアップ、オブジェクトコピー、オブジェクト集約、または検証仕様をすべて示します。
必須の選択項目:	日数
省略可能な選択項目:	なし
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	lookup_sch

IDBレポート

IDBレポートはIDBのサイズに関する情報を提供します。

IDBサイズ

説明:	メディア管理データベース、カタログデータベース、アーカイブログファイル、データファイル、詳細カタログのバイナリファイルディレクトリの統計値、SMBF(msgディレクトリ)、およびIDBのディスクスペースの最低水準を表形式で示します。

必須の選択項目:	なし
省略可能な選択項目:	なし
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`db_size`

> **重要:**
> このレポートの**[使用中]**列には、各IDB部分の使用中項目の割合(%)が示されます。この数字は、特定のIDB部分の最大項目数で現在の項目数を割り、パーセントで算出します。項目数が無制限の場合、この数は常に0%になります。
>
> IDBの特定部分のスペースが不足しているかどうかを見つけるには、追加で[IDBのスペース不足]通知を構成できます。

メディアとメディアプールに関するレポート

プールとメディアプールのレポートは、メディアプールと使われているメディアに関する情報を提供します。

メディアの拡張リスト

説明:	指定した検索条件に一致するメディアをすべて示すリストです。メディアID、メディアラベル、メディアの位置、メディアの状態、メディア保護、使用中および合計のスペース(MB)、メディアが最後にアクセスされた時間、メディアプールとメディアの種類、バックアップ、オブジェクトコピー、オブジェクト集約でメディアを使用しているセッション仕様、およびセッションの種類とサブタイプに関する情報をメディアごとに示します。
必須の選択項目:	なし
省略可能な選択項目:	セッション仕様、バックアップ仕様グループ、説明、位置、プール名、メディアの種類(DDSやDLTなど)、状態、期限、時間枠、ライブラリデバイス
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`media_list_extended`

メディアのリスト

説明:	指定した検索条件に一致するメディアをすべて示すリストです。メディアID、メディアラベル、メディアの位置、メディアの状態、メディア保護、使用中および合計のスペース(MB)、メディアが最後にアクセスされた時間、メディアプー

	ルとメディアの種類に関する情報をメディアごとに示します。
必須の選択項目:	なし
省略可能な選択項目:	説明、位置、プール名、メディアの種類(DDSやDLTなど)、状態、期限、時間枠、ライブラリデバイス
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`media_list`

プールのリスト

説明:	指定した検索条件に一致するプールをすべて示すリストです。プールごとに、プール名、説明、メディアの種類、メディアの総数、保護データが格納されている満量状態/追記可能メディアの数、保護データが格納されていないフリーメディアの数、[不良]/[普通]/[良好]の各状態のメディアの数を示します。
必須の選択項目:	なし
省略可能な選択項目:	プール名、位置、メディアの種類(DDSやDLTなど)、ライブラリデバイス、時間枠
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`pool_list`

メディア統計

説明:	検索条件に一致するメディアに関する統計情報のリストです。書き込まれたデータの量(単位:メディア数、スクラッチメディアの数、[保護]/[良好]/[普通]/[不良]の各状態のメディアの数、追記可能メディアの数、メディア上の総領域/使用領域/空き領域)を示します。
必須の選択項目:	なし
省略可能な選択項目:	説明、位置、プール名、メディアの種類(DDSやDLTなど)、状態、ステータス、期限、時間枠、ライブラリデバイス
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`media_statistics`

セッション仕様の使用法に関するレポート

セッション仕様レポートは、バックアップ、オブジェクトコピー、オブジェクト集約、またはオブジェクト検証に関する情報を提供します。たとえば、バックアップされたオブジェクトの平均サイズ、セッションのスケジュール、バックアップに関して構成されていないファイルシステムなどの情報です。

バックアップオブジェクトの平均サイズ

説明:	指定したバックアップ仕様に含まれているオブジェクトの平均サイズを示します。オブジェクトのフルバックアップおよび増分バックアップのサイズを示します。 Data Protector 8.14に導入されたVADP機能は、仮想マシン用の拡張レポートを提供します。VMware仮想マシンは、VADPクライアントと呼ばれるData Protectorクライアントとして表されます。VADPクライアントの新規オブジェクト名形式は以下のとおりです。 `<hostname>:/<vCenter>/<path>/<vmname> [<UUID>]` ここで、`<hostname>`はゲスト仮想マシンのDNSです。DNS名が不明の場合、IPアドレスまたはVM名が使用されます。
必須の選択項目:	なし
省略可能な選択項目:	バックアップ仕様、バックアップ仕様グループ、日数(レポートの開始時点から過去にさかのぼった日数)
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`obj_avesize`

バックアップに関して構成されていないファイルシステム

説明:	指定したバックアップ仕様のいずれにおいても構成されていないディスク(ファイルシステム)をすべて示します。
必須の選択項目:	なし
省略可能な選択項目:	バックアップ仕様、バックアップ仕様グループ
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`fs_not_conf`

オブジェクトの最新バックアップ

説明:	IDBのすべてのオブジェクトのリストです。オブジェクトごとに、最後の(フルおよび増分)バックアップの時間、最後の(フルおよび増分)オブジェクトコピーの時間、最後のオブジェクト集約の時間のリストを表示します。 Data Protector 8.14に導入されたVADP機能は、仮想マシン用の拡張レポートを提供します。VMware仮想マシンは、VADPクライアントと呼ばれるData Protectorクライアントとして表されます。VADPクライアントの新規オブジェクト名形式は以下のとおりです。 `<hostname>:/<vCenter>/<path>/<vmname> [<UUID>]` ここで、`<hostname>`はゲスト仮想マシンのDNS名です。DNS名が不明の場合、IPアドレスまたはVM名が使用されます。 バックアップ仕様のフィルターやオブジェクト作成時間のフィルターを使用して、リストのオブジェクトの範囲を絞り込むことができます(「`Optional Selections`」を参照してください)。ただし、以下の特殊事項を考慮してください。 • オブジェクトの種類がファイルシステム(ファイルシステムオブジェクト)の場合、オブジェクト作成時間のフィルターの条件に一致しないものでも表示されます。ただし、この場合、オブジェクト作成時間フィールドは空になります。 • バックアップ仕様から特定のファイルシステムオブジェクトをクリアした場合、そのファイルシステムオブジェクトはIDBに存在していてもレポートには含まれなくなります。 上記の留意事項は、オブジェクトの種類がBar(統合オブジェクト)の場合には適用されません。
必須の選択項目:	なし
省略可能な選択項目:	バックアップ仕様、バックアップ仕様グループ、日数(レポートの開始時点から過去にさかのぼった日数)
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`obj_lastbackup`

バックアップを持たないオブジェクト

説明:	バックアップ仕様に含まれているオブジェクトのうち、有効なバックアップが存在しないオブジェクトをすべて示します。バックアップが正常に完了したものや、保護の期限が切れていないものがこれに該当します。ただし、このレポートは、統合ソフトウェア用のバックアップ仕様には使用できません。

必須の選択項目:	なし
省略可能な選択項目:	バックアップ仕様、バックアップ仕様グループ、日数(レポートの開始時点から過去にさかのぼった日数)
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`obj_nobackup`

セッション仕様情報

説明:	選択したすべてのバックアップ、オブジェクトコピー、オブジェクト集約、オブジェクト検証仕様に関する情報を表示します。タイプ(IDB、MSESE、E2010など)、セッションの種類、セッション仕様名、グループ、オーナー、および実行前コマンドと実行後コマンドなどの情報が含まれます。
必須の選択項目:	なし
省略可能な選択項目:	セッション仕様、バックアップ仕様グループ
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`dl_info`

セッション仕様スケジュール

説明:	今後1年以内に指定されている各バックアップ、オブジェクトコピー、オブジェクト集約、およびオブジェクト検証の仕様の次の開始時間のリストです。
必須の選択項目:	なし
省略可能な選択項目:	セッション仕様、バックアップ仕様グループ
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`dl_sched`

バックアップ仕様のツリー

説明:	指定されたバックアップ仕様のすべてのツリーを示します。ドライブ名とツリー

	名も示します。 Data Protector 8.14に導入されたVADP機能は、仮想マシン用の拡張レポートを提供します。VMware仮想マシンは、VADPクライアントと呼ばれるData Protectorクライアントとして表されます。レポートは、VMwareオブジェクトのVM名をすべて表示します。
必須の選択項目:	なし
省略可能な選択項目:	バックアップ仕様、バックアップ仕様グループ
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	dl_trees

時間枠内のセッションに関するレポート

時間枠内のセッションに関するレポートは、指定した時間枠内に実行されたバックアップ、オブジェクトコピー、オブジェクト集約、またはオブジェクト検証のセッションに関する情報を提供します。

クライアント統計

説明:	クライアントとそのバックアップステータスの統計のリストです。検索条件に一致するクライアントだけが示されます。 Data Protector 8.14に導入されたVADP機能は、仮想マシン用の拡張レポートを提供します。VMware仮想マシンは、VADPクライアントと呼ばれるData Protectorクライアントとして表されます。VM名がクライアント名です。
必須の選択項目:	時間枠
省略可能な選択項目:	バックアップ仕様、バックアップ仕様グループ、ホスト名
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`host_statistics`

デバイスフロー

説明:	各デバイスの使用状況を示します。検索条件に一致するバックアップ、オブジェクトコピー、およびオブジェクト集約のセッションのフローチャートが示されます。`RptShowPhysicalDeviceInDeviceFlowReport`グローバルオプションを1に設定すると、同じ物理デバイス(ロック名およびシリアル番号で示される)が

	グループにまとめられます。ロック名もシリアル番号も指定されていない場合、論理名が表示されます。
必須の選択項目:	時間枠
省略可能な選択項目:	セッション仕様、バックアップ仕様グループ
サポートされている形式:	HTML
omnirptコマンドのオプション:	`device_flow`

使用メディアの拡張レポート

説明:	指定した時間枠内のバックアップ、オブジェクトコピー、オブジェクト集約のセッションで使用されたあて先メディア、およびセッションの種類とサブタイプに関する拡張情報が示されます。
必須の選択項目:	時間枠
省略可能な選択項目:	セッション仕様、バックアップ仕様グループ
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`used_media_extended`

セッションのリスト

説明:	指定した時間枠内のすべてのセッションとそれらの統計情報のリストです。
必須の選択項目:	時間枠
省略可能な選択項目:	セッション仕様、バックアップ仕様グループ
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`list_sessions`

オブジェクトコピー

説明:	指定した時間枠内のオブジェクトバージョンの有効なコピー数を示します。コピー数にはオリジナルオブジェクトのバージョンも含まれます。 VMware仮想マシンは、VADPクライアントと呼ばれるData Protectorクライアントとして表されます。VADPクライアントの新規オブジェクト名形式は以下のとおりです。 `<hostname>:/<vCenter>/<path>/<vmname> [<UUID>]` ここで、`<hostname>`はゲスト仮想マシンのDNS名です。DNS名が不明の場合、IPアドレスまたはVM名が使用されます。
必須の選択項目:	時間枠
省略可能な選択項目:	セッション仕様、バックアップ仕様グループ、コピー数
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`obj_copies`

使用メディアに関するレポート

説明:	指定した時間枠内のバックアップ、オブジェクトコピー、オブジェクト集約のセッションで使用されたあて先メディアを統計情報と共に示します。
必須の選択項目:	時間枠
省略可能な選択項目:	セッション仕様、バックアップ仕様グループ
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`used_media`

セッションエラー

説明:	バックアップ、オブジェクトコピー、オブジェクト集約、またはオブジェクト検証のセッション中に発生したエラーメッセージのリストを示します。クライアント別にメッセージを示します。
必須の選択項目:	時間枠
省略可能な選択項目:	セッション仕様、バックアップ仕様グループ、ホスト名、メッセージレベル
サポートされている形	すべての形式

式:	
omnirptコマンドのオプション:	`session_errors`

セッションフロー

説明:	検索条件に一致するバックアップセッションのフローチャートです。検索条件に一致するバックアップ、オブジェクトコピー、オブジェクト集約、およびオブジェクト検証のセッションのフローチャートが示されます。 このチャートでは、セッションの全体的なステータスが以下のように色分けして示されます。 • 赤:セッションに失敗したか、セッションが中止されました。 • 緑:セッションが正常に終了したか、エラーで終了しました。 • 黄:セッションは終了しましたが、障害が発生しました。 • 青:セッションが待機中か、マウント要求が発行されています。
必須の選択項目:	時間枠
省略可能な選択項目:	セッション仕様、バックアップ仕様グループ
サポートされている形式:	HTML
omnirptコマンドのオプション:	`session_flow`

セッション統計

説明:	選択した時間枠内のバックアップ、オブジェクトコピー、またはオブジェクト集約のステータスの統計を示します。
必須の選択項目:	時間枠
省略可能な選択項目:	セッション仕様、バックアップ仕様グループ
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`session_statistics`

単一セッションレポート

単一セッションのレポートは、特定のセッションに関する詳細情報を提供します。

セッションデバイス

説明:	選択したセッションで使われた、すべてのあて先デバイスに関する情報を示します。
必須の選択項目:	セッションID
省略可能な選択項目:	なし
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`session_devices`

セッションメディア

説明:	選択したセッションで使われた、すべてのあて先メディアに関する情報を示します。
必須の選択項目:	セッションID
省略可能な選択項目:	なし
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`session_media`

セッションオブジェクトコピー

説明:	選択したバックアップ、オブジェクトコピー、またはオブジェクト集約のセッションの有効なコピー数を示します。 Data Protector 8.14に導入されたVADP機能は、仮想マシン用の拡張レポートを提供します。VMware仮想マシンは、VADPクライアントと呼ばれるData Protectorクライアントとして表されます。VADPクライアントの新規オブジェクト名形式は以下のとおりです。 `<hostname>:/<vCenter>/<path>/<vmname> [<UUID>]` ここで、`<hostname>`はゲスト仮想マシンのDNS名です。DNS名が不明の場合、IPアドレスまたはVM名が使用されます。
必須の選択項目:	セッションID

省略可能な選択項目:	なし
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`session_objcopies`

セッションオブジェクト

説明:	選択したセッションの要素であるすべてのバックアップ、オブジェクトコピー、またはオブジェクト集約のオブジェクトを統計情報と共に示します。 Data Protector 8.14に導入されたVADP機能は、仮想マシン用の拡張レポートを提供します。VMware仮想マシンは、VADPクライアントと呼ばれるData Protectorクライアントとして表されます。セッションオブジェクトレポートはVM名とVMパスを表示します。
必須の選択項目:	セッションID
省略可能な選択項目:	なし
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`session_objects`

クライアントごとのセッション

説明:	選択したバックアップセッションの要素である各クライアントに関する情報を示します。**[複数のレポートを作成]**オプションをオンにすると、このレポートをクライアントごとの小さなレポートに分割できます。 VMware仮想マシンは、VADPクライアントと呼ばれるData Protectorクライアントとして表されます。VADPクライアントの新規オブジェクト名形式は以下のとおりです。 `<hostname>:/<vCenter>/<path>/<vmname> [<UUID>]` ここで、`<hostname>`はゲスト仮想マシンのDNS名です。DNS名が不明の場合、IPアドレスまたはVM名が使用されます。
必須の選択項目:	セッションID
省略可能な選択項目:	メッセージレベル
サポートされている形	すべての形式

式:	
omnirptコマンドのオプション:	`session_hosts`

単一セッション

説明:	単一のData Protector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のセッションに関するすべての情報を示します。
必須の選択項目:	セッションID
省略可能な選択項目:	メッセージレベル
サポートされている形式:	すべての形式
omnirptコマンドのオプション:	`single_session`

レポートの送信方法

レポートまたはレポートグループを構成または開始するときには、さまざまな送信方法を選択できます。

ブロードキャストメッセージによる送信

ブロードキャストメッセージによる送信では、レポート先のシステムを指定して、それらのシステムにブロードキャストメッセージを送信することができます。

ブロードキャストメッセージの送信先のシステムを指定して、ブロードキャストメッセージを送信できます(Windowsシステムへのみ送信可能)。ブロードキャストメッセージは、1000文字以内に制限されるため、ショート形式をお勧めします。

電子メールによる送信

電子メールによる送信では、レポートの受信者を指定して電子メールを送信できます。受信者の電子メールアドレスを正確に指定してください。

> **重要:**
> Microsoft Outlookのセキュリティ機能によって、電子メールを送信方法として使用すると、CRSサービスが応答を停止する場合があります。詳細と解決方法については、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。電子メール(SMTP)を電子メール送信方法として使うこともできます。

> **注:**
> Microsoft Exchange Server 2007がData Protector Cell Managerにインストールされている場合

> は、電子メールレポートによる送信は機能しません。電子メール(SMTP)を送信方法として使ってください。

Windowsシステムの場合

Windowsシステムから電子メールレポートを送信するには、メールプロファイルが必要です。既存のメールプロファイルを使うことも、「`OmniBack`」という名前の新しいプロファイルを作成することもできます。

既存のメールプロファイルを使うには、Data Protector `omnirc`ファイルに次の行を追加します。

`OB2_MAPIPROFILE=`*`existing_MAPI_profile_name`*

Windows上のHTML電子メールレポートの表示は、電子メールクライアントの設定によって異なります。多くの電子メールクライアントでは、ASCIIテキスト形式でレポートが表示されます。レポートがHTMLとして正しく表示されるようにするには、Webブラウザーでレポートを開きます。

UNIXシステムの場合

UNIXシステム上に電子メールサブシステムを構成し、稼動させておく必要があります。追加の構成は必要ありません。

オペレーティングシステム側の制限により、UNIXシステムでは、ローカライズされた電子メールレポートに使われている各国語文字がロケールの異なるシステム間で送受信された場合、これらの文字が正しく表示されないことがあります。

電子メール(SMTP)による送信

電子メールによる送信では、SMTPプロトコルを使って、レポートの受信者を指定して電子メールを送信できます。受信者の電子メールアドレスを正確に指定してください。

電子メールによる送信方法としては、この方法をお勧めします。

デフォルトでは、レポートの送信に使われるSMTPサーバーのアドレスとしてCell ManagerのIPアドレスが設定されます。このアドレスを変更するには、`SMTPServer`グローバルオプションを編集します。SMTPサーバーはCell Managerシステムからアクセスできることが必要ですが、Data Protectorセルの一部でなくてもかまいません。

Windowsシステムの場合

SMTPをサポートするよう既存のMicrosoft Exchange Serverを構成する方法については、Microsoft Exchange Serverのドキュメントを参照してください。

Windows上のHTML電子メールレポートの表示は、電子メールクライアントの設定によって異なります。多くの電子メールクライアントでは、ASCIIテキスト形式でレポートが表示されます。レポートが正しく表示されるかどうかは、Webブラウザーでレポートを開いて確認してください。

UNIXシステムの場合

オペレーティングシステム側の制限により、UNIXでは、ローカライズされた電子メールレポートに使われている各国語文字がロケールの異なるシステム間で送受信された場合、これらの文字が正しく表示されないことがあります。

外部スクリプトによる送信

外部スクリプトによる送信では、独自のスクリプトでレポートの出力を処理できます。レポートの出力は、標準入力(STDIN)としてスクリプトに渡されます。スクリプト処理の形式には、タブ形式を使うことをお勧めします。

スクリプトがCell Managerシステムにある場合は、`/opt/omni/lbin`ディレクトリ(HP-UXシステムの場合)または*`Data_Protector_home`*`\bin`ディレクトリ(Windowsシステムの場合)に格納する必要があります。スクリプト名のみを指定します。絶対パスを指定する必要はありません。

Windowsシステムでサポートされている外部スクリプトの拡張子は、`.bat`、`.exe`、および`.cmd`のみです。サポートされていない拡張子(`.vbs`など)を使ったスクリプトを実行するには、そのスクリプトを起動するバッチファイルを作成します。そして、そのバッチファイルを外部スクリプトとして実行するようにData Protectorを構成します。これにより、サポートされていない拡張子のスクリプトが起動されます。

指定したメディアの取り出しをスケジュールに基づいて実行する場合にも、この通知方法を使う必要があります。

ログファイルによる送信

ログファイルによる送信では、レポートをファイルに出力することができます。

このファイルは、Cell Managerシステムに保存されます。レポートの出力先となるファイルの名前を指定する必要があります。同じ名前のファイルが存在する場合は、既存のファイルが上書きされます。

SNMPによる送信

SNMPによる送信では、レポートをSNMPトラップとして送信することができます。このSNMPトラップは、SNMPトラップをサポートしているアプリケーションで処理することができます。

> **注:**
> SNMPによる送信は、構成済みSNMPトラップの最大サイズを超えていないレポートでのみ有効です。最大サイズを超えるレポートは分割されます。

Windowsシステムの場合

SNMPトラップは、WindowsのSNMPトラップ構成で指定されているシステムに送信されます。Cell Manager上でSNMPによる送信を行うには、WindowsのSNMPトラップを構成しておく必要があります。

UNIXシステムの場合

UNIX Cell Managerでは、レポートで指定されているシステムにSNMPトラップが送信されます。

HPE Data Protector GUIを使ってレポートグループを構成する

Data Protectorのレポートは、個別に(対話形式で)実行できるだけでなく、レポートグループにまとめて、レポートグループとして開始することもできます。構成済みのレポートグループに個々のレポートを追加でき

ます。[マウント要求レポート]と[デバイスエラーレポート]は、対話型レポートとしては使用できず、レポートグループでのみ使用できます。

Data Protector GUIを使ってレポートグループを構成すると、以下のことが可能になります。

- すべてのレポートを同時に(対話形式で)開始する。
- 指定した時間にレポートを開始するように、グループのスケジュールを設定する。
- 通知をトリガーとしてグループを開始する。

レポートの出力に入力パラメーターを表示するには、「レポート」ウィザードで**[レポートに選択条件を表示]**オプションをオンにします。ただし、必須、省略可能ともに入力パラメーターをサポートしていないレポートの場合、このオプションは使用できません。また、レポートに表示されるのは、入力パラメーターのうち、デフォルト値以外の値に設定されたパラメーターのみです。

前提条件

- `admin`ユーザーグループに追加されているか、またはレポートおよび通知のユーザー権限が付与されていることが必要です。
- CRSサービスを実行しているアカウントのData Protectorユーザーは削除しないでください。このユーザーは、インストール時にデフォルトで構成されます。Windows Cell Managerの場合、このユーザーのアカウントでインストールが実行されています。UNIX Cell Managerの場合、このユーザーがCell Managerの`root`ユーザーです。

構成の段階

レポートグループを構成する

手順

1. コンテキストリストで**[レポート]**を選択します。
2. **[レポート]**を右クリックし、**[レポートグループの追加]**をクリックしてウィザードを起動します。
3. レポートグループの名前を入力し、**[次へ]**をクリックします。
4. **[完了]**をクリックしてウィザードを終了します。これで、レポートグループが追加されます。以下のタスクを任意で実行できるようになりました。
   - レポートグループをスケジュールする: レポートグループを右クリックして、**[スケジュールの編集]**をクリックします。[スケジューラー]ページが開きます。スケジューラーを使用して、Data Protectorでスケジュールを作成および編集する方法の詳細については、「*スケジューラー、ページ 103*」を参照してください。
   - レポートグループにレポートを追加する: レポートグループを右クリックして、**[レポートの追加]**をクリックします。「レポートの追加」ウィザードに従ってレポートを追加します。

> **ヒント:**
> レポートグループを通知によってトリガーするには、レポートグループを構成してから、送信方法として[レポートグループの使用]を使用するように通知を構成します。

レポートをレポートグループに追加する

手順

1. [レポート]コンテキストで**[レポート]**を展開します。レポートグループを右クリックし、**[レポートの追加]**をクリックして「レポートの追加」ウィザードを起動します。レポートグループを構成した後すぐにレポートを構成する場合は、この処理手順をスキップしてください。
2. [結果エリア]に表示されるリストから、レポートの種類を選択します。
3. [名前]テキストボックスにレポート名を入力し、[種類]ドロップダウンリストからレポートを選択します。**[次へ]**をクリックします。
4. このウィザードでは、選択したレポートの種類に応じたオプションが表示されます。たとえば、[IDBサイズのレポート]の場合に設定できるウィザードオプションの組み合わせと、[メディアのリスト]レポートの場合に設定できるウィザードオプションの組み合わせは異なります。ウィザードの最後のページが表示されるまで、**[次へ]**を繰り返しクリックします。
5. [送信方法]ドロップダウンリストでレポートの送信方法を選択し、[電子メールアドレス]テキストボックスにレポートの受信者を入力します。[形式]ドロップダウンリストで、レポートの形式を選択します。**[追加]**をクリックして、構成済み受信者のグループに受信者を追加します。

   この手順を繰り返して、必要な受信者をすべて追加します。
6. **[完了]**をクリックしてウィザードを終了します。これで、レポートグループが追加されます。

レポートグループに追加するすべてのレポートについて、この処理手順を繰り返します。

HPE Data Protector GUIを使ってレポートグループを実行する

レポートグループに所属しているレポートは、すべて一括で実行できます。

前提条件

- Adminユーザーグループに追加されているか、[レポートと通知]のユーザー権限が付与されていることが必要です。
- CRSサービスを実行しているアカウントのData Protectorユーザーは削除しないでください。このユーザーは、インストール時にデフォルトで構成されます。Windows Cell Managerの場合、このユーザーのアカウントでインストールが実行されています。UNIX Cell Managerの場合、このユーザーがCell Managerの`root`ユーザーです。

手順

1. コンテキストリストで**[レポート]**を選択します。
2. Scopingペインで、レポートグループのリストを検索し、目的のレポートグループを右クリックして、**[開始]**をクリックします。
3. **[はい]**をクリックして処理を実行します。

HPE Data Protector GUIを使って個々のレポートを実行する

個々のレポートを対話式で実行できます。また、レポートをレポートグループにまとめて、それらを一括で実行することもできます。

[マウント要求レポート]と[デバイスエラーレポート]は、対話式レポートとしては使用できず、レポートグループでのみ使用できます。

前提条件

- Adminユーザーグループに追加されているか、[レポートと通知]のユーザー権限が付与されていることが必要です。
- CRSサービスを実行しているアカウントのData Protectorユーザーは削除しないでください。このユーザーは、インストール時にデフォルトで構成されます。Windows Cell Managerの場合、このユーザーのアカウントでインストールが実行されています。UNIX Cell Managerの場合、このユーザーがCell Managerの`root`ユーザーです。

手順

1. コンテキストリストで**[レポート]**を選択します。
2. Scopingペイン下の**[タスク]**タブをクリックします。
3. Scopingペインで、実行するレポートの種類を検索し、選択してウィザードを起動します。
4. このウィザードでは、選択したレポートの種類に応じたオプションが表示されます。たとえば、[IDBサイズのレポート]の場合に設定できるウィザードオプションの組み合わせと、[メディアのリスト]レポートの場合に設定できるウィザードオプションの組み合わせは異なります。ウィザードの最後のページが表示されるまで、**[次へ]**を繰り返しクリックします。
5. ウィザードの最後のページが表示されたら、**[完了]**をクリックして、ウィザードを終了します。レポートの出力が表示されます。

HPE Data Protector CLIを使ってレポートおよびレポートグループを実行する

Data Protectorのレポートは、コマンドラインインターフェイス(CLI)を使用して生成できます。コマンドラインインターフェイスでは、使用している他のスクリプトにData Protectorレポートを取り込むことができます。個々のレポートを生成できるほか、レポートグループを開始したり、レポートの送信方法と形式を定義したりできます。

前提条件

- Adminユーザーグループに追加されているか、[レポートと通知]のユーザー権限が付与されていることが必要です。
- CRSサービスを実行しているアカウントのData Protectorユーザーは削除しないでください。このユーザーは、インストール時にデフォルトで構成されます。Windows Cell Managerの場合、このユーザーのアカウントでインストールが実行されています。UNIX Cell Managerの場合、このユーザーがCell Managerの`root`ユーザーです。

手順

1. omnirptコマンドを使用してレポートを生成します。このコマンドの詳細については、omnirpt manページまたは『*HPE Data Protector Command Line Interface Reference*』を参照してください。

新しいメールプロファイルを作成する

Windowsシステムから電子メールレポートまたは電子メール通知を送信するには、メールプロファイルが必要です。「OmniBack」という名前の新しいメールプロファイルをMicrosoft Outlook 2002がインストールされているWindowsシステムで作成する作業は、以下の手順で行います。

> **重要：**
> Microsoft Outlookのセキュリティ機能によって、電子メールを送信方法として使用すると、CRSサービスが応答を停止する場合があります。詳細と解決方法については、『*HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス*』を参照してください。e-mail (SMTP)を送信方法として使用することもできます。

手順

1. Windowsの[コントロールパネル]で、**[メール]**アイコンをダブルクリックします。
2. [メール設定]ダイアログボックスで、**[プロファイルの表示]**をクリックします。
3. [メール]ダイアログボックスで、**[追加]**をクリックします。
4. [新しいプロファイル]ダイアログボックスの[プロファイル名]テキストボックスに「OmniBack」と入力し、**[OK]**をクリックして、「電子メールアカウント」ウィザードを起動します。
5. **[新しい電子メールアカウントの追加]**を選択し、**[次へ]**をクリックします。
6. [サーバーの種類]ページで、**[Microsoft Exchange Server]**を選択し、**[次へ]**をクリックします。
7. [Exchange Server設定]ページで、ローカルのMicrosoft Exchange Serverシステムの名前とユーザー名を入力し、**[次へ]**をクリックします。
8. **[完了]**をクリックして、ウィザードを終了します。

Windows SNMPトラップを構成する

Windows Cell Managerでは、レポートで指定されているシステムにSNMPトラップが送信されます。Windowsシステム上でSNMPを使用して通知またはレポートを送信するには、WindowsのSNMPトラップを構成しておく必要があります。

UNIX Cell Managerでは、SNMPトラップは、通知またはレポートで指定されているシステムに送信されます。

手順

1. *Data_Protector_home*\binディレクトリからomnisnmpコマンドを実行します。

   このコマンドを実行すると、レジストリのSystemで、CurrentControlSet\Services\SNMP\Parameters\ExtensionAgentsの下に、適切なData Protectorエントリが作成されます。

2. **Windows XP、Windows Server 2003の場合:**
   a. [コントロールパネル]で、**[ネットワーク接続]**を選択します。
   b. [詳細設定]メニューの**[オプション ネットワーク コンポーネント]**を選択してウィザードを起動します。
   c. **[管理とモニター ツール]**をオンにし、**[次へ]**をクリックします。
   d. ウィザードの指示に従って、管理と監視ツールをインストールします。

   Windows 7、Windows 8の場合:
   a. [コントロールパネル]で、**[プログラムと機能]**を選択します。
   b. **[Windowsの機能の有効化または無効化]**を選択します。
   c. **[Simple Network Management Protocol (SNMP)]**を選択して、**[OK]**をクリックします。

   Windows Server 2008、Windows Server 2012の場合:
   a. [スタート]メニューで、**[コンピューター]**を右クリックして、**[管理]**を選択します。
   b. **[Features]**を選択して、**[Add Features]**をクリックします。
   c. [Features]ツリーで、**[SNMP Services]**→**[SNMP Service]**の順に選択します。
   d. **[次へ]**→**[Install]**の順にクリックします。
3. **[コントロール パネル]**、**[管理ツール]**、**[サービス]**の順に選択します。
4. **[SNMP サービス]**を右クリックして**[プロパティ]**を選択します。
   a. **[トラップ]**タブを選択します。[コミュニティ名]テキストボックスに「`public`」と入力し、[トラップ送信先]テキストボックスにアプリケーション管理サーバーのホスト名を入力します。
   b. **[セキュリティ]**タブを選択します。[受け付けるコミュニティ名]で、コミュニティ[`public`]を選択し、**[編集]**をクリックして、[コミュニティの権利]を[`READ CREATE`]に設定します。

      [これらのホストから SNMP パケットを受け付ける]を選択し、認証が失敗した場合、[トラップ送信先]テキストボックスにホスト名ではなくIPアドレスを入力します。
   c. 変更内容を確認します。
5. `omnisnmp`を実行します。

通知について

Data Protectorでは、特定のイベントが発生した場合に、Cell Managerから通知を送信できます。たとえば、バックアップ、オブジェクトコピー、オブジェクト集約、またはオブジェクト検証の各セッションの完了時に、セッションのステータスを電子メールで送信できます。

通知は、レポートをトリガーするように設定できます。

通知は、Data Protector GUIで構成できるほか、Javaをサポートしている任意のWebブラウザーで構成することもできます。

通知をカスタマイズするための入力パラメーターが用意されています。一部のパラメーターでは複数項目の選択が可能です。その他の入力パラメーターは、通知の種類によって異なります。送信先は、送信方法に応じて、以下のいずれかとなります。

- システム
- 電子メールアドレス
- SNMPトラップ

- スクリプト
- ファイル
- 構成済みレポートグループ
- Data Protectorイベントログ

デフォルトでは、通知はデフォルト値で構成され、Data Protectorイベントログに送信されます。他の送信方法でも通知を送信する場合や、他の入力パラメーター値を使う場合は、構成値を変更する必要があります。

Data Protectorの通知機能にアクセスする場合は、`admin`ユーザーグループに追加されているか、または**レポートおよび通知のユーザー権限**が付与されていることが必要です。

通知の種類 - 通知をトリガーするイベント

通知は、以下の2種類に大別できます。

- イベントの発生時にトリガーされる通知
- Data Protectorのチェック/保守メカニズムによりスケジュール設定および開始される通知

警告

イベント/通知名:	警告
通知をトリガーする条件:	自動メディアコピーのアップグレード、アップグレードコアパートの終了、アップグレード詳細パートの終了、削除の終了、セッションの中止、UCP中のDisk Agentのアップグレードなど、Data Protector内部の重要条件。
デフォルトのメッセージレベル:	注意域
表示されるメッセージ:	警告: *`Alarm_message`*

期限切れ証明書

イベント/通知名:	ExpiredCertificates
通知をトリガーする条件:	Cell Managerの証明書ディレクトリに格納されている証明書が期限切れか、まだ有効でない場合。Cell Managerの証明書ディレクトリには、セキュアな制御通信を行うためのクライアント証明書がすべて格納されています。
デフォルトのメッセージレベル:	注意域
表示されるメッセージ:	証明書*certificate_name*の有効期限が切れているか、まだ有効になっていません。

Csa Start Sessionの失敗

イベント/通知名：	CsaStartSessionFailed
通知をトリガーする条件：	バックアップセッションが次のエラーメッセージで終了した場合：`Could not start a new backup session.`
デフォルトのメッセージレベル:	重要警戒域
表示されるメッセージ:	データリスト*datalist_name*のCsaStartSessionが失敗しました。

デバイスエラー

イベント/通知名：	DeviceError
通知をトリガーする条件：	**[デバイス]**で指定されたデバイス(デフォルト：`<Any>`)上のエラー。
デフォルトのメッセージレベル:	危険域
表示されるメッセージ:	デバイス*Device*にエラーが発生しました。

セッションの完了

イベント/通知名：	EndofSession
通知をトリガーする条件：	セッション仕様**[セッション仕様]**(デフォルトでは`<Any>`)の**[セッションステータス]**で指定されたメッセージ(デフォルトでは[`Completed with errors`])で終了したバックアップ、コピー、集約、またはオブジェクト検証セッション。
デフォルトのメッセージレベル:	注意域
表示されるメッセージ:	バックアップ仕様グループ*group*に属するセッション仕様*backup_specification*,のバックアップセッション*session_ID*が、全体ステータスsession_overall_statusで終了しました。*session_overall_status;* *session_type* セッション仕様*session_spec*のセッション*session_ID*が完了しました。ステータスは*session_status*です。

ファイルライブラリのディスクの使用状況

イベント/通知名：	FileLibraryDiskUsage

通知をトリガーする条件:	**[ファイルライブラリの名前]**で指定されたファイルライブラリ(デフォルトでは`All`)の空きディスクスペースの不足。
デフォルトのメッセージレベル:	注意域
表示されるメッセージ:	ディレクトリ*`File Library Path`*内でファイルライブラリ*`File Library Device`*のディスクスペースが不足しています。

健全性チェックの失敗

イベント/通知名:	HealthCheckFailed
通知をトリガーする条件:	`omnihealthcheck`コマンドによって返されるゼロ以外の値。このコマンドは、以下の条件が真のときにゼロを返します。 • Data Protectorサービス(CRS、MMD、hpdp-idb、hpdp-idb-cp、hpdp-as、KMS、omnitrig、およびomniinet)はアクティブ。 • Data Protectorメディア管理データベースの整合性が確保されていること。 • IDBのバックアップが1つ以上存在する。 このコマンドの詳細については、`omnihealthcheck` manページまたは『*HPE Data Protector Command Line Interface Reference*』を参照してください。 デフォルトでは、Data Protectorは健全性のチェック(`omnihealthcheck`コマンドを実行)を1日1回開始します。
デフォルトのメッセージレベル:	危険域
表示されるメッセージ:	健全性チェックメッセージ: *`healthcheck_command`*が失敗しました。

IDBのバックアップ必要

イベント/通知名:	IDBBackupNeeded
通知をトリガーする条件:	連続増分IDBバックアップが多すぎるか、頻繁なIDBフルバックアップが不十分。
デフォルトのメッセージレベル:	注意域
表示されるメッセージ:	連続増分IDBバックアップが*n*個あります。Data Protector内部データベースの前回のバックアップは*`MM/DD/YY hh:mm:ss`*に実行されました。

IDBの破損

イベント/通知名:	IDBCorrupted

通知をトリガーする条件:	IDB一部分の破損。
デフォルトのメッセージレベル:	危険域
表示されるメッセージ:	Data Protector内部データベースの*IDB_part*部分で、データ破損が検出されました(*error_message*)。 エラーメッセージの値: • `Verification of datafile(s) failed.` • `KeyStore is corrupted.` • `Media and Media in position tables are not consistent.` • `Database is not in consistent state.` • `Database schema is not consistent.`

IDBの制限

イベント/通知名:	IDBLimits
通知をトリガーする条件:	MMDBまたはCDB部分のいずれかの制限に到達する。
デフォルトのメッセージレベル:	重要警戒域
表示されるメッセージ:	Data Protector内部データベースの*IDB_part*部分が制限に達しました。

IDBの再構成必要

イベント/通知名:	IDBReorganizationNeeded
通知をトリガーする条件:	断片化または無駄な領域が発生しているため、1つ以上のIDBエンティティを再構成する必要があります。
デフォルトのメッセージレベル:	注意域
表示されるメッセージ:	テーブル*name_of_table*の膨張が検出されました。 テーブル*name_of_table*の列*uuid*に断片化が検出されました。インデックス*name_of_index*の断片化が検出されました。

IDBのスペース不足

イベント/通知名:	IDBSpaceLow

通知をトリガーする条件:	以下のイベントのうちのひとつ。 • 最大空きディスクサイズが**[IDB空きディスク領域のしきい値[MB]]**(デフォルトは300 MB)以下である。 • すべてのDCディレクトリの最大サイズと現在のサイズの相違が**[DCBFのサイズ制限しきい値[MB]]**(デフォルトは500 MB)を下回っている。 • 最大空きディスクサイズが**[WAL空きディスク領域のしきい値[MB]]**(デフォルトは300 MB)以下である。 デフォルトでは、Data Protectorは1日に1回、[IDBのスペース不足]条件をチェックします。
デフォルトのメッセージレベル:	重要警戒域
表示されるメッセージ:	Data Protector内部データベースのディスクスペースがいっぱいになりました。

ライセンス警告

イベント/通知名:	LicenseWarning
通知をトリガーする条件:	ライセンス購入が必要になった場合。
デフォルトのメッセージレベル:	注意域
表示されるメッセージ:	*n* カテゴリ*name of the license*では、n個のライセンスを購入する必要があります。詳細は、omnicc -check_licenses -detailを実行してください。

ライセンス期限切れ

イベント/通知名:	LicenseWillExpire
通知をトリガーする条件:	Data Protectorライセンスの有効期限が間近に迫っている場合。ライセンスは、**[ライセンスの有効期限]**で指定された日数(デフォルトは10)で期限切れになります。
デフォルトのメッセージレベル:	注意域
表示されるメッセージ:	最初に取得したライセンスはあと*License expires in days*日で期限切れになります。

メールスロット満量

イベント/通知名:	MailSlotsFull

通知をトリガーする条件:	**[デバイス]**で指定されたデバイス(デフォルトは`<Any>`)のメールスロットがいっぱい。
デフォルトのメッセージレベル:	注意域
表示されるメッセージ:	ライブラリ*Device*のすべてのメールスロットがいっぱいです。ただちに削除してください。

マウント要求

イベント/通知名:	MountRequest
通知をトリガーする条件:	**[デバイス]**で指定されたデバイス(デフォルトは`<Any>`)に対するマウント要求。
デフォルトのメッセージレベル:	注意域
表示されるメッセージ:	デバイスに対するマウント要求がありました。*Device*.

フリーメディア不足

イベント/通知名:	NotEnoughFreeMedia
通知をトリガーする条件:	**[メディアプール]**のフリーメディアの不足。**[メディアプール]**が**[フリープール]**を使用するように構成されている場合、**[フリープール]**の**[フリーメディア数]**も考慮されることに注意してください。
デフォルトのメッセージレベル:	注意域
表示されるメッセージ:	メディアプール*Media Pool*には*number_of_media*個のメディアにしか空きがありません。

セッションエラー

イベント/通知名:	SessionError
通知をトリガーする条件:	[単一メッセージレベル](デフォルトでは[`Major`])以上のレベルのメッセージが出たバックアップ、コピー、集約、またはオブジェクト検証セッション。
デフォルトのメッセージレベル:	重要警戒域
表示されるメッセージ:	バックアップ仕様グループ*group*に属するセッション仕様*backup_specification*のバックアップセッション*session_ID*にエラーがあります:

	number_of_errors *session_type* セッション仕様 *session_spec*のセッション*session_ID*にエラーがあります: *number_of_errors*

セッションの開始

イベント/通知名:	StartofSession
通知をトリガーする条件:	セッション仕様 **[セッション仕様]**(デフォルトは<Any>)で指定されたバックアップ、コピー、集約、またはオブジェクト検証セッションの開始。
デフォルトのメッセージレベル:	正常域
表示されるメッセージ:	バックアップ仕様グループ*group*に属するセッション仕様*backup_specification*のバックアップセッション*session_ID*が開始されました。 *session_type* セッション仕様 *session_spec*のセッション*session_ID*が開始されました。

セッションが多すぎる

イベント/通知名:	TooManySessions
通知をトリガーする条件:	1000セッションを既に同時実行している場合にセッションを開始した。
デフォルトのメッセージレベル:	注意域
表示されるメッセージ:	同時に実行可能なセッションの最大数を超えたため、セッションを開始できません。

予期しないイベント

イベント/通知名:	UnexpectedEvents
通知をトリガーする条件:	最後のチェック実施以降のData Protectorイベントログ内の新規イベント数が異常に多い。新規イベント数が**[イベント数]**で指定された数(デフォルトは20)を超えている。 デフォルトでは、Data Protectorは1日に1回条件をチェックします。
デフォルトのメッセージレベル:	注意域
表示されるメッセージ:	Data Protectorイベントログが、前日の*number_of events_in_last_day*の予期しないイベントにより増加しました。

UNIX Media Agentのチェック

イベント/通知名:	UnixMediaAgentWarning
通知をトリガーする条件:	クライアントデバイスが、非巻き戻しデバイスファイルではなく巻き戻しデバイスファイルを使用しているときに`mrgcfg -check_ma`コマンドがこの通知をトリガーした。
デフォルトのメッセージレベル:	注意域
表示されるメッセージ:	Media Agentのクライアントデバイスが、非巻き戻しデバイスファイルではなく巻き戻しデバイスファイルを使用して構成されている可能性があります。これにより、SAN環境では問題が起きる可能性があります。

ユーザーチェックの失敗

イベント/通知名:	UserCheckFailed
通知をトリガーする条件:	デフォルトのData Protector管理コマンドディレクトリにある、**[コマンドパス]**で指定された名前のユーザー作成スクリプトまたはコマンドから、ゼロ以外の値が返された場合。 デフォルトでは、Data Protectorはスクリプトを実行するユーザーチェックを1日1回開始します(デフォルトは`None`)。
デフォルトのメッセージレベル:	重要警戒域
表示されるメッセージ:	ユーザーチェックが失敗しました。終了コード: *`error_code`*:*`error_description`*

通知の送信方法

通知の構成時には、さまざまな送信方法を選択できます。デフォルトの送信方法では、すべての通知がData Protectorイベントログに送信されるように構成されます。通知をほかの方法で送信する場合は、その送信方法を構成する必要があります。構成可能な通知送信方法は、以下のとおりです。

ブロードキャストメッセージによる送信

ブロードキャストメッセージによる送信では、指定イベントが発生した後、通知先のシステムを指定して、それらのシステムにブロードキャストメッセージを送信することができます。

ブロードキャストメッセージをWindowsシステムに送信するには、ターゲットシステムを指定する必要があります。ブロードキャストメッセージは、1000文字以内に制限されるため、ショート形式をお勧めします。

電子メールによる送信

電子メールによる送信では、通知の受信者を指定して電子メールを送信できます。受信者の電子メールアドレスを正確に指定してください。

> **重要:**
> Microsoft Outlookのセキュリティ機能によって、電子メールを送信方法として使用すると、CRSサービスが応答を停止する場合があります。詳細と解決方法については、『HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照してください。このため、電子メールによる通知を送信する方法としては、SMTPをお勧めします。

> **注:**
> Microsoft Exchange Server 2007がData Protector Cell Managerにインストールされている場合は、電子メール通知による送信は機能しません。電子メール(SMTP)を送信方法として使ってください。

Windowsシステムの場合

Windowsシステムから電子メール通知を送信するには、メールプロファイルが必要です。既存のメールプロファイルを使うことも、「`OmniBack`」という名前の新しいプロファイルを作成することもできます。

既存のメールプロファイルを使うには、Data Protector `omnirc`ファイルに次の行を追加します。

```
OB2_MAPIPROFILE=existing_MAPI_profile_name
```

UNIXシステムの場合

UNIXシステム上に電子メールサブシステムを構成して稼動させておく必要があります。

オペレーティングシステム側の制限により、UNIXシステムでは、ローカライズされた電子メール通知に使われている各国語文字がロケールの異なるシステム間で送受信された場合、これらの文字が正しく表示されないことがあります。

電子メール(SMTP)による送信

電子メールによる送信では、通知の受信者を指定して電子メールを送信できます。受信者の電子メールアドレスを正確に指定してください。

電子メールによる送信方法としては、この方法をお勧めします。

デフォルトでは、通知の送信に使われるSMTPサーバーのアドレスとしてCell ManagerのIPアドレスが設定されます。このアドレスを変更するには、`SMTPServer` グローバルオプションを編集します。SMTPサーバーはCell Managerシステムからアクセスできることが必要ですが、Data Protectorセルの一部でなくてもかまいません。

外部スクリプトによる送信

外部スクリプトによる送信では、独自のスクリプトで通知の出力を処理できます。レポートの出力は、標準入力(STDIN)としてスクリプトに渡されます。スクリプト処理の形式には、タブ形式を使うことをお勧めし

ます。

Cell Managerシステム上にあるスクリプトは、デフォルトのData Protector管理コマンドディレクトリに置く必要があります。スクリプト名のみを指定します。

Windowsシステムでサポートされている外部スクリプトの拡張子は、.bat、.exe、および.cmdのみです。サポートされていない拡張子(.vbsなど)を使ったスクリプトを実行するには、そのスクリプトを起動するバッチファイルを作成します。そして、そのバッチファイルを外部スクリプトとして実行するようにData Protectorを構成します。これにより、サポートされていない拡張子のスクリプトが起動されます。

指定したメディアの取り出しをスケジュールに基づいて実行する場合にも、この通知方法を使う必要があります。

ログファイルによる送信

ログファイルによる送信では、指定イベントが発生したときに通知をファイルに出力することができます。

このファイルは、Cell Managerシステムに保存されます。通知の出力先となるファイルの名前を指定する必要があります。同じ名前のファイルが存在する場合は、既存のファイルが上書きされます。

Data Protectorイベントログによる送信

デフォルトの送信方法では、すべての通知がData Protectorイベントログに送信されます。Data Protectorイベントログへアクセスできるのは、adminユーザーグループのData Protectorユーザーと、[レポートと通知]のユーザー権限を持つData Protectorユーザーのみです。Data Protectorイベントログに書き込まれているイベントは、いずれも表示と削除が可能です。

SNMPによる送信

SNMPによる送信では、指定したイベントの発生時に通知出力をSNMPトラップとして送信することができます。このSNMPトラップは、SNMPトラップをサポートしているアプリケーションで処理できます。

Windowsシステムの場合

Windows Cell Managerでは、レポートで指定されているシステムにSNMPトラップが送信されます。Windowsシステム上でSNMPによる送信を行うには、WindowsのSNMPトラップを構成しておく必要があります。

UNIXシステムの場合

UNIX Cell Managerでは、通知で指定されているシステムにSNMPトラップが送信されます。

レポートグループによる送信

レポートグループによる送信では、指定したイベントの発生時にレポートグループを実行できます。

通知を構成する

通知を構成するには、通知の名前、通知の種類、メッセージレベル、送信方法、および受信者を指定する必要があります。その他の入力パラメーターは、通知の種類によって異なります。

前提条件

`admin`ユーザーグループに追加されているか、またはレポートおよび通知のユーザー権限が付与されていることが必要です。

手順

1. コンテキストリストで**[レポート]**を選択します。
2. **[通知]**を右クリックし、**[通知の追加]**をクリックしてウィザードを起動します。
3. ウィザードのオプションは、選択する通知によって異なります。たとえば、[IDBのスペース不足]通知にはすべてのオプションが使えますが、[IDBの制限]通知の場合には一部しか使用できません。ウィザードの最後のページが表示されるまで、**[次へ]**を繰り返しクリックします。
4. **[完了]**をクリックしてウィザードを終了します。

指定したイベントが発生すると、指定した送信方法で通知が送信されます。

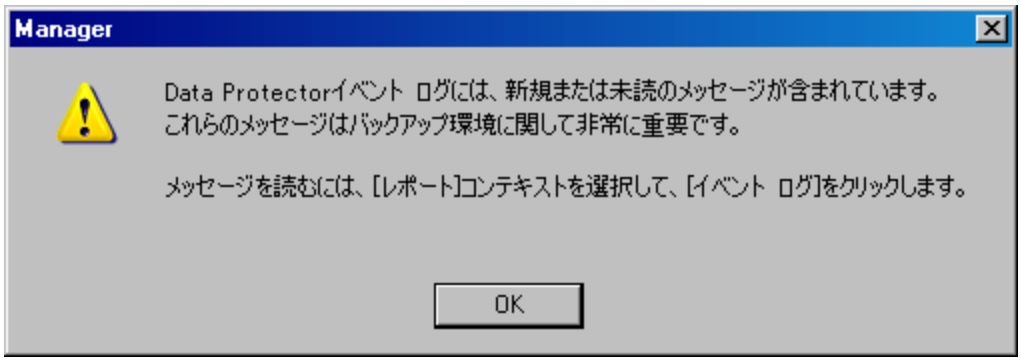
> **ヒント:**
> レポートグループを通知によってトリガーするには、レポートグループを構成してから、送信方法として[レポートグループの使用]を使用するように通知を構成します。

HPE Data Protectorイベントログについて

Data Protectorイベントログは、Data Protectorの操作中に発生した特定のイベントを一元管理するためのメカニズムです。Data Protectorのイベントロギングメカニズムでは、処理によって発生するイベントとユーザーが発生させるイベントの2種類のイベントがログに記録されます。イベントは、Cell Manager上のデフォルトのData Protectorログファイルディレクトリに存在する`Ob2EventLog.txt`ファイルに記録されます。

Data Protectorイベントログは、イベントログビューアーを使って表示でき、トラブルシューティングに役立てることができます。

ユーザーがData Protectorのグラフィカルユーザーインターフェイスを起動したとき、このユーザーが確認していない新しい通知がData Protectorのイベントログにある場合は、次のメッセージが表示されます。



この場合、Data Protector GUIは、自動的に[レポート]コンテキストに切り替わります。

以下に追加情報を示します。

- ユーザーは、adminユーザーグループのメンバーであるか、[レポートと通知]のユーザー権限が付与されている必要があります。
- Data Protectorのイベントログは自動更新されません。新しいメッセージを表示するためには、**[F5]**キーを押して手動でイベントログを更新する必要があります。

処理によって発生するイベント

イベントは通知機能によってログに記録されます。

ユーザーが発生させるイベント

イベントは、ユーザーが特定のGUI操作または一連のGUI操作を行ったときにログに記録されます。この一連の操作には、バックアップ仕様、オブジェクトコピー仕様、集約仕様の変更のほか、ユーザーやユーザーグループの操作、デバイスやメディアに関連する構成の作成と変更、リモートインストールなどの操作があります。

デフォルトでは、ユーザーが発生させるイベントのログ記録は無効になっています。このログ記録を有効にするためには、グローバルオプションEventLogAuditを1に設定する必要があります。

MoM環境では、このグローバルオプションが1に設定されていると、イベントはローカルのCell Managerシステムでのみ記録されます。

イベントログビューアーにアクセスする

Data Protectorイベントログビューアーを使用して、記録されているイベントを検索できます。

前提条件

ユーザーは、adminユーザーグループのメンバーであるか、[レポートと通知]のユーザー権限が付与されている必要があります。

手順

1. コンテキストリストで**[レポート]**を選択します。
2. Scopingペインで**[レポート]**を展開します。
3. **[イベントログ]**を選択して表示します。

イベントログビューアーの表示内容を削除する

> **注：**
> イベントログビューアーの内容を削除しても、`Ob2EventLog.txt`ファイルの内容は削除されません。

前提条件

Adminユーザーグループのメンバーになっているか、[レポートと通知]のユーザー権限が付与されていることが必要です。

手順

1. コンテキストリストで**[レポート]**を選択します。
2. Scopingペインで**[レポート]**を展開します。
3. **[イベントログ]**を右クリックし、**[イベントログを空にする]**を選択すると、イベントログビューアー内のすべてのエントリが削除されます。

監査について

Data Protectorには、バックアップセッション監査が用意されています。この監査には、Data Protectorセル全体のユーザー定義期間に実行されたすべてのバックアップタスクに関する変更不可および上書き不可の情報が格納されます。監査情報は、監査および管理のために一体的かつ印刷可能な方式でオンデマンドで取得できます。

監査情報ログを有効にして、監査ログファイルの保持期間を設定できます。これを行うには、グローバルオプション`AuditLogEnable`および`AuditLogRetention`を変更します。

監査レポートを生成する

監査レポートを生成するには、以下の手順に従います。

> **注：**
> MoM環境では、Cell Managerごとに個別に監査レポートを実行する必要があります。

手順

1. コンテキストリストで**[内部データベース]**をクリックします。
2. Scopingペインで、**[監査]**項目をクリックし、[監査]ページを開きます。
3. [検索インターバル]ドロップダウンリストから、いずれかの値を選択します(たとえば、`Last week`など)。
4. **[更新]**ボタンをクリックすると、選択した期間中に実行されたすべてのバックアップセッションのリストが表示されます。
5. セッションリストから特定のセッションを選択して、[監査]プロパティページの中央部および下部に、使用メディア、およびオブジェクトについての詳細情報を表示します。

Data Protectorが正常に機能していることのチェック

Data Protectorが実行するチェック

Data Protectorには自己診断および保守機能があり、保守タスクとチェックを毎日実行します。日常の保守作業では、Data Protectorの内部データベースの多くのセクションから古いデータを削除する一連のコマンドを実行します。

デフォルトでは、日常の保守作業は毎日正午に行われます。この作業では、IDBのすべての構成要素が削除されるわけではなく、IDBへの排他アクセスなしに削除できる構成要素だけが削除されます。

保守タスク

Data Protectorは、デフォルトでは毎日午後12:00に、以下を実行します。

- 以下の`omnidbutil -purge`コマンドを実行して、古いDCバイナリファイル、セッション、および関連メッセージを削除します。
  - `-dcbf`
  - `-sessions`
  - `-messages`

  日常の保守作業の`-sessions`オプションは`KeepObsoleteSessions`グローバルオプション、`-messages`オプションは`KeepMessages`グローバルオプションの設定によって異なります。
- **[フリープールを使用]**オプションと**[フリーメディアをフリープールに移動]**オプションが設定されているメディアプールからフリー(保護されていない)メディアを探し、`omnidbutil -free_pool_update`コマンドを実行して、そのフリーメディアの割り当てを解除し、フリープールに移動します。
- メディアの保護を確認し、メディアおよび対応するメディアの位置を削除します。メディアがIDBからエクスポートされると、メディアの位置がIDBで認識されなくなるため、Data Protectorでメディアのストレージを解放できなくなります。このようなメディアは、ストレージから手動で削除し、メディアの位置(スロット)もデバイスコンテキストから手動で削除する必要があります。

詳細については、omnidbutilのmanページまたは『*HPE Data Protector Command Line Interface Reference*』を参照してください。

チェック

Data Protectorは、デフォルトでは毎日午後12:30に、以下の通知のチェックを開始します。

- IDBのスペース不足
- IDBの制限
- IDBのバックアップ必要
- フリーメディア不足
- 健全性チェックの失敗
- [ユーザーチェックの失敗](設定されている場合)
- 予期しないイベント
- ライセンス警告
- ライセンス期限切れ

Data Protectorは、デフォルトでは毎週月曜日午後12:30に、以下の通知のチェックを開始します。

- IDBの再構成必要

デフォルトでは、トリガーされた通知はData Protectorのイベントログに送られます。

> **ヒント：**
> 保守タスクおよびチェック用のデフォルトスケジュール値は、変更が可能です。
> DailyMaintenanceTimeおよびDailyCheckTimeグローバルオプションをそれぞれ、24時間制を使って変更します。

ユーザーが実行するチェックについて

Data Protectorがデフォルトで実行するチェック以外に、定期的にチェックを実行することをお勧めします。これにより、Data Protectorが正常に機能していることを確認し、障害が発生する前に問題点を特定できます。

> **ヒント：**
> スクリプトを作成し、[ユーザーチェックの失敗]通知を使用してチェックを自動化できます。

いくつかのチェック(たとえば、omnihealthcheckやomnitrig -run_checks)は、Data Protectorのチェックおよび保守管理機能の一部としてすでに実行されています。

使用するコマンドの詳細については、各コマンドのマンページまたは*HPE Data Protector Command Line Interface Reference*を参照してください。

実行するチェック	チェックの内容および方法
Data Protector Cell Managerのチェック	コマンドの終了コードが0 (OK)であれば、以下のチェックが正常に終了したことを示しています。コマンドの終了コードが0以外の場合は、チェックに失敗したことを示します。 1. omnihealthcheckコマンドを実行して、以下を確認します。

	• Data Protectorサービス(CRS、MMD、hpdb-idb、hpdp-idb-cp、hpdp-as、omnitrig、KMS、およびinet)がアクティブであること • Data Protectorメディア管理データベースの整合性が確保されていること • 少なくとも1つのIDBバックアップイメージが存在すること このコマンドの終了コードが0 (OK)になるのは、上の3つの条件がすべて成立している場合(つまり、すべてのチェックの終了コードが0になった場合)だけです。 2. `omnidbcheck -quick`コマンドを実行してIDBをチェックします。
バックアップが正しく構成されているかどうかのチェック	1. 重要なバックアップ仕様のバックアッププレビューを実行します。プレビューにより、以下を確認します。 • バックアップ仕様で指定したすべてのクライアントがCell Managerからアクセス可能であること • すべてのファイルがアクセス可能であること • バックアップするデータ容量が決定していること • すべてのバックアップデバイスが正しく設定されていること プレビューは、一部の統合およびZDBではサポートされていません。 2. バックアップ仕様がバックアップポリシーに応じてスケジュール設定されているかどうかをチェックするには、`omnirpt -report dl_sched`コマンドを実行します。このコマンドは、すべてのバックアップ仕様およびそのスケジュールを表示します。
Data Protectorインストールの検証	Data ProtectorのGUI ([クライアント]コンテキスト)を使用してインストールを検証し、Cell ManagerまたはクライアントシステムでData Protectorソフトウェアコンポーネントが正常に稼動しているかどうかをチェックします。
Data Protectorログファイルのチェック	以下のData Protectorログファイルを調べ、問題が発生しているかどうかを特定します。 • `event.log` • `debug.log` • `purge.log`
通知チェックの実行	デフォルトでは、Data Protectorは以下の通知のチェックを1日1回開始します。トリガーされた通知はData Protectorイベントログに送信されます。 `omnitrig -run_checks`コマンドを実行して、以下の通知のチェックを開始することもできます。 • IDBのスペース不足 • フリーメディア不足 • 予期しないイベント

	• 健全性チェックの失敗 • IDBの制限 • IDBのバックアップ必要 • IDBの再構成必要 • ライセンス期限切れ • ライセンス警告 • [ユーザーチェックの失敗](設定されている場合)
他のシステムリソースのチェック	以下のログファイルを調べ、問題が発生しているかどうかを特定します。 **Windowsシステムの場合:** Windowsのイベントビューアーのセキュリティログ、システムログ、アプリケーションログ **UNIXシステムの場合:** `/var/adm/syslog/syslog.log`
IDB復旧ファイルのチェック	IDB復旧ファイル(`obrindex.dat`)をチェックし、Cell Managerシステムの正常な復旧に必要なIDBおよび構成ファイルが定期的に作成されることを確認します。

チェックを自動化する方法

スクリプトを使用し、[ユーザーチェックの失敗]通知を構成することで、チェックを自動化することができます。

[ユーザーチェックの失敗]通知は、この通知に入力パラメーターとして指定されたコマンドまたはスクリプトを実行し、そのスクリプト内で実行されたコマンドのいずれかの戻り値が`0`でない場合に通知をトリガーします。通知は、選択した送信方法で行われます。

コマンド/スクリプトは、アプリケーションシステム上のデフォルトのData Protector管理コマンドディレクトリに置く必要があります。

構成された[ユーザーチェックの失敗]通知は、Data Protectorの日常チェックの際に毎日開始され、トリガーされると、Data Protectorイベントログに送信されます。

HPE Data Protectorのドキュメント

> **注：**
> このドキュメントセットはHPEサポートWebサイト(https://softwaresupport.hpe.com/)で利用できます。このドキュメントセットには最新の更新情報および修正情報が記載されています。

HPE Data Protectorドキュメントセットには、次の場所からアクセスできます。

- HPE Data Protectorインストールディレクトリ

  Windowsシステムの場合：`Data_Protector_home\docs`

  UNIXシステムの場合：`/opt/omni/doc/C`
- HPE Data ProtectorGUIの**[ヘルプ]**メニュー
- HPEサポートWebサイト(https://softwaresupport.hpe.com/)

ドキュメントマップ

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。セルが灰色に塗りつぶされているドキュメントを最初に参照してください。

											インテグレーションガイド					ZDBガイド		GREガイド		
	管理者	ヘルプ	スタートアップ	コンセプト	インストール	トラブルシューティング	DR	CLI	PA	インテグレーションVSS	MSFT	Oracle/SAP	IBM	Sybase/NDMP	仮想環境	ZDB管理者	ZDB IG	Exchange	SharePoint	VMware
管理タスク	X	X																		
バックアップ		X	X	X						X	X	X	X	X	X	X	X			
CLI								X												
コンセプト、テクニック		X		X						X	X	X	X	X	X	X	X	X	X	X
ディザスタリカバリ				X			X													
インストール、アップグレード			X		X				X											
インスタントリカバリ				X	X											X	X			
ライセンス					X				X											
制限事項		X			X	X			X	X	X	X	X	X	X		X			
新機能		X							X											
計画戦略		X		X																
手順、タスク	X	X			X	X	X			X	X	X	X	X	X	X	X	X	X	X
推奨事項				X					X											
要件					X				X	X	X	X	X	X	X					
復元	X	X	X	X						X	X	X	X	X	X	X	X	X	X	X
サポートされている構成				X																
トラブルシューティング		X			X	X				X	X	X	X	X	X	X	X	X	X	X

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。ドキュメント項目のタイトルには、すべて先頭に"HPE Data Protector"が付きます。

略称	ドキュメント	
Admin	管理者ガイド	このガイドはData Protectorの管理タスクを説明しています。
CLI	Command Line Interface Reference	このガイドでは、Data Protectorのコマンドラインインターフェイス、コマンドオプション、およびそれらの使用方法を説明し、基本コマンドラインの例を示します。
Concepts	コンセプトガイド	このガイドでは、Data Protectorのコンセプトとゼロダウンタイムバックアップ(ZDB)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。これは、タスク指向のヘルプとともに使用するように、作成されています。
DR	ディザスタリカバリガイド	このガイドでは、ディザスタリカバリのプランニング、準備、テスト、および実行の方法について説明します。
Getting Started	スタートアップガイド	このガイドでは、Data Protectorでの操作をすぐに開始するための情報を記載しています。インストールの前提条件を一覧し、基本的なバックアップ環境のインストールと構成の手順、およびバックアップと復元の実行手順を記載しています。また、詳細な情報を記載しているリソースについても一覧しています。
GRE Guide	Granular Recovery Extensionユーザーガイド - Microsoft SharePoint Server、ExchangeおよびVMware	このガイドでは、次の製品用のData Protector Granular Recovery Extensionの構成方法と使用方法について説明します。 • Microsoft SharePoint Server • Exchange Server • VMware vSphere
ヘルプ	ヘルプ	
Install	インストールガイド	このガイドでは、実際の環境のオペレーティングシステムとアーキテクチャーに応じたData Protectorソフトウェアのインストール方法を説明します。また、Data Protectorのアップグレード方法と、環境に応じた適切なライセンスの取得方法も説明します。

略称	ドキュメント	
インテグレーションガイド	インテグレーションガイド	このガイドでは、Data Protectorを次のプリケーションと統合する方法を説明します。 • **MSFT:**Microsoft SQL Server、Microsoft SharePoint Server、およびMicrosoft Exchange Server。 • **IBM:**Informix Server、IBM DB2 UDB、およびLotus Notes/Domino Server。 • **Oracle/SAP:**Oracle Server、MySQL、SAP R3、SAP MaxDB、およびSAP HANA Appliance。 • **Sybase/NDMP:**SybaseおよびNetwork Data Management Protocol Server。 • **仮想環境:**VMware vSphere、VMware vCloud Director、Microsoft Hyper-V、およびCitrix XenServerとの仮想環境統合
Integration VSS	Integration Guide for Microsoft Volume Shadow Copy Service	このガイドでは、Data ProtectorとMicrosoftボリュームシャドウコピーサービスとの統合について説明します。
PA	製品案内、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、最新リリースの新機能について説明しています。また、インストール要件、必要なパッチ、制限事項、報告されている問題とその回避方法などの情報も記載しています。
トラブルシューティング	トラブルシューティングガイド	このガイドでは、Data Protectorの使用時に発生する可能性がある問題をトラブルシューティングする方法について説明します。
ZDB Admin	ZDB管理者ガイド	このガイドでは、ディスクアレイを持つData Protectorの統合の構成方法と使用方法について説明します。このガイドは、バックアップ管理者やオペレーターを対象としています。ファイルシステムと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。
ZDB IG	ZDBインテグレーションガイド	このガイドでは、Oracle Server、SAP R/3、Microsoft Exchange Server、および

略称	ドキュメント	
		Microsoft SQL Serverの各データベース、およびVMwareの仮想環境についてゼロダウンタイムバックアップ、インスタントリカバリ、標準的な復元を実行するためのData Protectorの構成方法と使用方法について説明します。

統合

ソフトウェアアプリケーション統合

ソフトウェアアプリケーション	ガイド
IBM DB2 UDB	インテグレーションガイド
Informix Server	インテグレーションガイド
Lotus Notes/Domino Server	インテグレーションガイド
Microsoft Exchange Server	インテグレーションガイド、ZDB IG、GRE Guide
Microsoft Hyper-V	インテグレーションガイド
Microsoft SharePoint Server	インテグレーションガイド、ZDB IG、GRE Guide
Microsoft SQL Server	インテグレーションガイド、ZDB IG
Microsoftボリュームシャドウコピーサービス(VSS)	Integration VSS
Network Data Management Protocol (NDMP) Server	インテグレーションガイド
Oracle Server	インテグレーションガイド、ZDB IG
MySQLサーバー	インテグレーションガイド
SAP HANA Appliance	インテグレーションガイド
SAP MaxDB	インテグレーションガイド
SAP R/3	インテグレーションガイド、ZDB IG

ソフトウェアアプリケーション	ガイド
Sybase Server	インテグレーションガイド
VMware vCloud Director	インテグレーションガイド
VMware vSphere	インテグレーションガイド、ZDB IG、GRE Guide

ディスクアレイシステム統合

以下のディスクアレイシステムファミリと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。

ディスクアレイファミリ	ガイド
EMC Symmetrix	すべてのZDB
HPE P4000 SANソリューション	コンセプト、ZDB Admin、インテグレーションガイド
HPE P6000 EVAディスクアレイファミリ	すべてのZDB、インテグレーションガイド
HPE P9000 XPディスクアレイファミリ	すべてのZDB、インテグレーションガイド
HPE 3PAR StoreServ Storage	コンセプト、ZDB Admin、インテグレーションガイド
NetApp Storage	コンセプト、ZDB Admin、ZDB IG
EMC VNX	コンセプト、ZDB Admin、ZDB IG
EMC VMAX	コンセプト、ZDB Admin、ZDB IG

フィードバックを送信

このドキュメントに関するご意見は、ドキュメンテーションチームまで電子メールでお送りください。お使いのシステムに電子メールクライアントが設定されている場合は、上のリンクをクリックすると、電子メールウィンドウが開き、件名行に次の情報が入力されます。

管理者ガイド (HPE Data Protector 10.00)に関するフィードバック

本文にご意見、ご感想を記入の上、**[送信]**をクリックしてください。

電子メールクライアントが利用できない場合は、上記の情報をコピーしてWebメールクライアントの新規メッセージに貼り付け、AutonomyTPFeedback@hpe.com宛にお送りください。

お客様からのご意見、ご感想をお待ちしています。