HP Data Protector 6.20

インストールおよびライセンスガイド

製品番号:
初版: 2011年3月

ご注意

© Copyright 1999, 2011 Hewlett-Packard Development Company, L.P.

機密性のあるコンピュータソフトウェアです。これらを所有、使用、または複製するには、HPからの有効な使用許諾が必要です。商用コンピュータソフトウェア、コンピュータソフトウェアに関する文書類、および商用アイテムの技術データは、FAR12.211および12.212の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

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。HP製品、またはサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載で追加保証を意図するものは一切ありません。ここに含まれる技術的、編集上の誤り、または欠如について、HPはいかなる責任も負いません。

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

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

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

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

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

UNIX®は、The Open Groupの登録商標です。

目次

出版履歴 17
本書について 19
対象読者 19
ドキュメントセット 19
ガイド 19
オンラインヘルプ 22
ドキュメントマップ 23
略称 23
対応表 24
統合ソフトウェア 25
表記上の規則および記号 27
Data Protectorグラフィカルユーザーインタフェース 28
一般情報 29
HPテクニカルサポート 29
メールニュース配信サービス 30
HP Webサイト 30
ドキュメントに関する意見 30

1 インストール手順の概要 31
この章の内容 31
インストール手順の概要 31
リモートインストールの概念 34
Data ProtectorのインストールDVD-ROM 36
Cell Managerシステムの選択 38
Data Protectorユーザーインタフェースシステムの選択 39
Data Protectorグラフィカルユーザーインタフェース 40

2 ネットワークへのData Protectorのインストール 43
この章の内容 43
Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール 44
UNIX用Cell Managerのインストール 45
カーネルパラメータの設定 47

インストール手順 47
HP-UX、Solaris、およびLinuxにインストールされるディレクトリの構造 50
自動での起動とシャットダウンの構成 51
環境変数の設定 53
Cell Managerのインストール用に割り当てるディスクスペースを増やす 54
この次に行う作業 54
Windows用Cell Managerのインストール 55
インストール手順 56
インストール後の状態 60
トラブルシューティング 62
この次に行う作業 62
インストールサーバーのインストール 63
UNIX用のインストールサーバーのインストール 63
Windows用のインストールサーバーのインストール 68
Data Protectorクライアントのインストール 72
Data Protectorコンポーネント 76
Data Protectorクライアントのリモートインストール 82
セキュアシェルを使用したリモートインストール 83
クライアントのセルへの追加 87
クライアントへのコンポーネントの追加 90
Windows用クライアントのインストール 92
ローカルインストール 94
Windowsシステムへのバックアップデバイスの接続 97
HP-UXクライアントのインストール 99
HP-UXのカーネル構成のチェック 100
HP-UXシステムへのバックアップデバイスの接続 102
Solaris用クライアントのインストール 102
インストール後の構成 104
Solarisシステムへのバックアップデバイスの接続 108
Linuxクライアントのインストール 109
Linuxシステムへのバックアップデバイスの接続 113
ESX Serverクライアントのインストール 114
Mac OS Xクライアントのインストール 114
AIXクライアントのインストール 115
AIXクライアントへのバックアップデバイスの接続 117
Tru64クライアントのインストール 117
Tru64クライアントへのバックアップデバイスの接続 119
SCOクライアントのインストール 119
SCOシステムへのバックアップデバイスの接続 120
ADIC/GRAUライブラリ用またはStorageTekライブラリ用のMedia Agentのインストール 122
ライブラリドライブの接続 123
ADIC/GRAUライブラリを使用するData Protectorクライアントの準備作業 123

ADIC/GRAUライブラリ用のMedia Agentのインストール 124
StorageTekライブラリを使用するData Protectorクライアントの準備作業 128
StorageTekライブラリ用のMedia Agentのインストール 129
Novell NetWareクライアントのローカルインストール 131
HP OpenVMSクライアントのローカルインストール 139
UNIXおよびMac OS Xクライアントのローカルインストール 146
Data Protector統合クライアントのインストール 151
ローカルインストール 153
リモートインストール 154
クラスター対応統合ソフトウェアのインストール 154
Microsoft Exchange Serverクライアント 155
Data ProtectorMicrosoft Exchange Server 2003/2007用統合ソフトウェア 155
Data Protector Microsoft Exchange Server 2010用統合ソフトウェア 155
Data Protector Microsoft Exchange Server Single Mailbox用統合ソフトウェア 156
Data Protector Microsoftボリュームシャドウコピーサービス用統合ソフトウェア 157
Microsoft SQL Serverクライアント 157
Microsoft SharePoint Serverクライアント 157
Data Protector Microsoft SharePoint Server 2003用統合ソフトウェア 157
Data Protector Microsoft SharePoint Server 2007/2010用統合ソフトウェア 158
Data Protector Microsoft SharePoint Server 2007/2010 VSSを使用するソリューション 158
Data Protector Microsoftボリュームシャドウコピーサービス用統合ソフトウェア 158
Microsoft SharePoint Server向けData Protector Granular Recovery Extension 159
Sybaseクライアント 159
Informix Serverクライアント 159
IBM HACMP Cluster 160
SAP R/3クライアント 160
SAP MaxDBクライアント 161
Oracle Serverクライアント 161
VMwareクライアント 162
Data Protector仮想環境統合ソフトウェア 162
Data ProtectorVMware(レガシー)用統合ソフトウェア 162
VMware vSphere向けData Protector Granular Recovery Extension 163
Microsoft Hyper-Vクライアント 164
Data Protector仮想環境統合ソフトウェア 164
Data Protector Microsoftボリュームシャドウコピーサービス用統合ソフトウェア 164
DB2クライアント 165
NNMクライアント 165

NDMP Serverクライアント 165
Microsoftボリュームシャドウコピーサービスクライアント 166
Lotus Notes/Domino Serverクライアント 166
Lotus Domino Cluster 167
HP StorageWorks P6000 EVAディスクアレイファミリ用統合ソフトウェア 167
HP StorageWorks P6000 EVAディスクアレイファミリとOracle Serverの統合 168
HP StorageWorks P6000 EVAディスクアレイファミリとSAP R/3の統合 170
HP StorageWorks P6000 EVAディスクアレイファミリとMicrosoft Exchange Serverの統合 173
HP StorageWorks P6000 EVAディスクアレイファミリとMS SQLの統合 173
HP StorageWorks P9000 XPディスクアレイファミリ用統合ソフトウェア 174
HP StorageWorks P9000 XPディスクアレイファミリとOracle Serverの統合 175
HP StorageWorks P9000 XPディスクアレイファミリとSAP R/3の統合 176
HP StorageWorks P9000 XPディスクアレイファミリとMicrosoft Exchange Serverの統合 180
HP StorageWorks P9000 XPディスクアレイファミリとMicrosoft SQL Serverの統合 181
HP StorageWorks P4000 SANソリューション用統合ソフトウェア 181
EMC Symmetrix用統合ソフトウェア 181
EMC Symmetrix用統合ソフトウェアとOracleの組み合わせ 182
EMC Symmetrix用統合ソフトウェアとSAP R/3との組み合わせ 183
EMC Symmetrix用統合ソフトウェアとMicrosoft SQL Serverとの組み合わせ 186
VLS自動移行クライアント 186
各国語版Data Protectorユーザーインタフェースのインストール 187
トラブルシューティング 187
各国語版Data Protectorマニュアルのインストール 189
Windowsシステムへの各国語版Data Protectorマニュアルのインストール 189
UNIXシステムへの各国語版Data Protectorマニュアルのインストール 190
Data Protectorシングルサーバー版のインストール 191
Windows用SSEの制限 191
HP-UXおよびSolaris用のSSEの制限事項 192
Data Protector Web Reportingのインストール 192
MC/ServiceGuardへのData Protectorのインストール 193
クラスター対応Cell Managerのインストール 194
インストールサーバーのクラスターノードへのインストール 194
クラスター対応クライアントのインストール 194
Microsoft Cluster ServerへのData Protectorのインストール 195
クラスター対応Cell Managerのインストール 195
クラスター対応クライアントのインストール 204
Veritas ClusterへのData Protectorクライアントのインストール 207
クラスター対応クライアントのインストール 207
Novell NetWare ClusterへのData Protectorクライアントのインストール 208
クラスター対応クライアントのインストール 208

Data ProtectorのIBM HACMP Clusterへのインストール 210
クラスター対応クライアントのインストール 210

3 インストールの保守 213
この章の内容 213
セルへのクライアントのインポート 213
セルへのインストールサーバーのインポート 216
セルへのクラスター対応クライアントのインポート 217
Microsoft Cluster Server 217
その他のクラスター 218
セルからのクライアントのエクスポート 220
保護について 223
セキュリティ層 223
クライアントの保護 224
Data Protectorユーザー 224
Cell Managerの保護 226
その他のセキュリティ保護について 226
クライアントの保護設定 227
allow_hostsファイルとdeny_hostsファイル 232
inet.logファイルに大量のログが記録される 233
ホスト名厳密チェック 233
機能を使用可能にする 235
セキュアな通信の有効化 235
[バックアップ仕様を開始]ユーザー権限 238
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 238
ホストの信頼 239
保護イベントのモニター 240
どのData Protectorパッチがインストールされているかを確認する 240
GUIを使用したData Protectorパッチの確認 241
CLIを使用したData Protectorパッチの確認 242
Data Protectorソフトウェアのアンインストール 242
Data Protectorクライアントのアンインストール 243
Cell Managerとインストールサーバーのアンインストール 245
Windowsシステムからのアンインストール 245
HP-UXシステムからのアンインストール 247
MC/ServiceGuard上に構成されているCell Managerおよびインストールサーバーのアンインストール 247
Solarisシステムからのアンインストール 250
Linuxシステムからのアンインストール 253
UNIXでのData Protectorソフトウェアの手動による削除 255
Data Protectorソフトウェアコンポーネントの変更 257

4 Data Protector 6.20へのアップグレード 263
この章の内容 263
アップグレードの概要 263
アップグレードの手順 264
暗号化キーの自動移行 265
Data Protector A.06.00、A.06.10、およびA.06.11からのアップグレード 266
UNIX用Cell Managerとインストールサーバーのアップグレード 266
Cell Managerのアップグレード 266
インストールサーバーのアップグレード 270
Windows Cell Managerとインストールサーバーのアップグレード 272
構成の変更のチェック 276
クライアントのアップグレード 279
Oracle用統合ソフトウェアのアップグレード 282
SAP R/3用統合ソフトウェアのアップグレード 283
Microsoftボリュームシャドウコピーサービス用統合ソフトウェアのアップグレード 284
HP StorageWorks P6000 EVAディスクアレイファミリ用統合ソフトウェアのアップグレード 285
自動ディザスタリカバリモジュールのアップグレード 285
他の統合ソフトウェアのアップグレード 286
MoM環境でのアップグレード 286
シングルサーバー版からのアップグレード 287
旧バージョンのSSEからData Protector 6.20 SSEへのアップグレード 287
Data Protector 6.20 SSEからData Protector 6.20へのアップグレード 288
Cell Managerのアップグレード 288
複数のシステムからのアップグレード 288
HP StorageWorks Application Recovery Manager A.06.00からのアップグレード 289
アップグレード後の内部データベースのバックアップ 290
バックアップ仕様のアップグレード 290
omnib使用方法の変更点 290
Solaris 8からSolaris 9へのアップグレード 291
HP-UX 11.x (PA-RISC)からHP-UX 11.23/11.31 (IA-64)への移行 291
MoM 固有の手順 295
インストールサーバー 固有の手順 296
32ビット/64ビットWindowsから64ビットWindows/Windows Server 2008への移行 296
MoM 固有の手順 300
インストールサーバー 固有の手順 301
MC/ServiceGuard上で構成されているCell Managerのアップグレード 301
Microsoft Cluster Server上で構成されているCell Managerのアップグレード 305

5 Data Protectorライセンス 309
この章の内容 309

概要 309
ライセンスチェック機能とレポート機能 310
Cell Manager関連ライセンス 310
エンティティーベースのライセンス 310
容量ベースのライセンス 311
使用容量の計算 312
アドバンストバックアップ使用権 313
容量ベースのライセンスの例 315
必要に応じたライセンスレポートの作成 318
Data Protector 6.20以前のライセンスのチェックとレポート 319
マルチドライブサーバー使用権のレポート 319
以前のオンラインライセンスのレポート 322
NDMPダイレクトバックアップ使用権のレポート 323
スロットライブラリ使用権のレポート 324
以前のZDBおよびIRのライセンスのレポート 324
Data Protectorパスワード 327
HP AutoPassユーティリティを使用した恒久パスワードの取得とインストール 328
恒久パスワードの取得とインストールのためのその他の方法 330
パスワードの検証 333
インストール済みライセンスの数を調べる 334
他のCell Managerシステムへのライセンスの移動 334
集中型ライセンス 335
Data Protector 6.20の製品構成とライセンス 336
パスワードについて 338
Data Protector 6.20へのライセンス移行 339
Data Protector Order Tool 339
Data Protectorライセンスフォーム 340

6 インストール時のトラブルシューティング 343
この章の内容 343
Windows用Cell Managerインストール時の名前解決に関する問題 343
Data Protectorセル内のDNS接続の確認 344
omnicheckコマンドの使用 345
インストールのトラブルシューティングとData Protectorのアップグレード 347
Windowsクライアントのリモートインストールに関する問題 348
Solaris上でのData Protector Cell Managerのインストールに関する問題のトラブルシューティング 349
UNIXクライアントのインストールに関する問題のトラブルシューティング 349
Windows XPクライアントのインストールに関する問題のトラブルシューティング 351
Windows VistaおよびWindows Server 2008クライアントのインストールに関する問題のトラブルシューティング 352
Data Protectorクライアントのインストール結果の確認 352

アップグレードのトラブルシューティング 353
手動でのアップグレード手順 356
ログファイルの使用 357
ローカルインストール 357
リモートインストール 358
Data Protectorログファイル 358
インストール実行トレースの作成 359

A UNIXネイティブツールを使用したData Protectorのインストールとアップグレード 361
この付録の内容 361
ネイティブツールを使用した、HP-UX、Solaris、およびLinuxシステムへのインストール 361
swinstallを使用したHP-UXシステムへのCell Managerのインストール 362
pkgaddを使用したSolarisシステムへのCell Managerのインストール 364
rpmを使用したLinuxシステムへのCell Managerのインストール 366
swinstallを使用したHP-UXシステムへのインストールサーバーのインストール 368
pkgaddを使用したSolarisシステムへのインストールサーバーのインストール 369
rpmを使用したLinuxシステムへのインストールサーバーのインストール 375
クライアントのインストール 379
ネイティブツールを使用したHP-UX、Solaris、およびLinuxシステムでのアップグレード 380
swinstallを使用したHP-UXシステムでのData Protectorのアップグレード 380
pkgaddを使用したSolarisシステムでのData Protectorのアップグレード 381
rpmを使用したLinuxシステムでのData Protectorのアップグレード 382

B システムの準備と保守作業 385
この付録の内容 385
UNIXシステムでのネットワーク構成 385
TCP/IP設定をチェックする 386
デフォルトのポート番号の変更 388
Data Protectorのデフォルトのポート番号の変更 388
Java GUIのデフォルトのポート番号の変更 390
Data ProtectorインストールのためのWindows Server 2008上で実行するMicrosoftサーバークラスターの準備 390
Veritas Volume ManagerがインストールされたMicrosoft Cluster ServerへのData Protectorのインストール 393
NISサーバーの準備 394
Cell Manager名の変更 395

C デバイスとメディア関連タスク 397
この付録の内容 397
Windowsでのテープドライバおよびロボティクスドライバの使用 397

Windows上でのデバイスファイル(SCSIアドレス)の作成 400
HP-UX上のSCSIロボティクス構成 401
HP-UX上のデバイスファイルの作成 406
SCSIコントローラのパラメータの設定 408
HP-UX上の未使用のSCSIアドレスの取得 408
Solarisシステム上の未使用のSCSIターゲットIDの取得 410
Solarisシステム上でのデバイスおよびドライバ構成の更新 411
構成ファイルの更新 411
デバイスファイルの作成とチェック 414
Windowsシステム上の未使用のSCSIターゲットIDの取得 415
HP StorageWorks 330fxライブラリ上のSCSI IDの設定 416
バックアップデバイスの接続 417
StorageWorks 24スタンドアロンデバイスの接続 421
HP StorageWorks DATオートローダーの接続 423
HP StorageWorks DLTライブラリ28/48 スロットの接続 425
Seagate Viper 200 LTO Ultriumテープドライブの接続 429
Novell NetWare上にインストールしたGeneral Media Agentのチェック 431
記憶デバイスの識別 432
General Media Agentの起動テスト 432
HPUMA.NLMおよびHPDEVBRA.NLMの起動テスト 435

D Data Protector 6.20へのアップグレード後のコマンドラインの変更 437

用語集 467

索引 527

図一覧

1 Data Protectorグラフィカルユーザーインタフェース 29
2 Data Protectorセル 34
3 Data Protectorのインストールの概念 36
4 Data Protectorグラフィカルユーザーインタフェース 41
5 インストール手順 44
6 インストールの種類の選択 57
7 ソフトウェアコンポーネントの選択 58
8 コンポーネントのサマリーリスト 59
9 [Installation Status]ページ 59
10 AutoPassをインストール対象として選択する場合 60
11 インストールの種類の選択 70
12 コンポーネント選択サマリーページ 71
13 [Installation Status]ページ 71
14 クライアントの選択 88
15 コンポーネントの選択 89
16 クライアントの選択 91
17 コンポーネントの選択 92
18 Cell Managerの選択 95
19 コンポーネント選択サマリーページ 96
20 インストールサマリーページ 97
21 [Kernel Configuration]ウィンドウ 101
22 デバイスファイル名の形式 122
23 セットアップ時の各国語版マニュアルの選択 189
24 各国語版マニュアルのリモートでのインストール 190

25 インストールの種類の選択 198
26 SWindows Server 2008でのクラスターリソースの選択 199
27 Windowsシステムでのクラスターリソースの選択 200
28 アカウント情報の入力 200
29 コンポーネント選択ページ 201
30 [Installation Status]ページ 202
31 Data Protectorユーザーアカウント 203
32 クラスター対応インストールモードの選択 205
33 Data Protectorユーザーアカウント 206
34 セルへのクライアントのインポート 215
35 セルへのMicrosoft Cluster Serverクライアントのインポート 218
36 MC/ServiceGuardクライアント、Veritasクライアント、またはNovell NetWare Cluster Servicesクライアントのセルへのインポート 220
37 クライアントシステムのエクスポート 222
38 クライアントの保護設定 229
39 選択したクライアントの保護を使用可能にする 230
40 セル内のすべてのクライアントに対する保護の設定 231
41 インストール済みパッチの確認 241
42 コンポーネント選択サマリーページ 274
43 [Installation status]ページ 274
44 AutoPassをインストール対象として選択する場合 275
45 コンポーネントの選択 306
46 コンポーネント選択サマリーページ 306
47 [Installation status]ページ 307
48 使用容量の計算シナリオ 313
49 ディスクへのZDBセッション 316
50 テープへのZDBセッション 317
51 ディスク+テープへのZDBセッション 318
52 HP AutoPassウィザード 330

53 HP Data Protector製品構成 337
54 Data Protector Order Toolの例 340
55 [SD install - software selection]ウィンドウ 364
56 ClusterフォルダおよびAdministratorsローカルユーザーグループのアクセス許可エントリの修正 392
57 メディアチェンジャのプロパティ 399
58 ロボティクスドライバの無効化 399
59 テープドライブプロパティ 401
60 SCSI 制御デバイス 402
61 デバイスの管理 402
62 SCSIパススルードライバ(sctl)のステータス 403
63 SCSIパススルードライバsptのステータス 404
64 接続済みデバイスのリスト 406
65 HP-UXシステム上で実行したioscan -fコマンドの出力 409
66 デバイスの設定 416

表一覧

1 出版履歴 17
2 表記上の規則 27
3 Data Protector DVD-ROMの一覧 37
4 Data Protectorクライアントシステムのインストール 73
5 統合ソフトウェアソフトウェアのインストール 74
6 他のインストール 75
7 Data Protectorコンポーネントコード 148
8 HP-UX上のData Protectorソフトウェアコンポーネントの依存関係 258
9 Solaris上のData Protectorソフトウェアコンポーネントの依存関係 259
10 Linux上のData Protectorソフトウェアコンポーネントの依存関係 260
11 アップグレード後のEADRおよびOBDRの互換性 286
12 出力メッセージ 346
13 Data Protector A.06.00からのアップグレード 437
14 Data Protector A.06.10からのアップグレード 448
15 Data Protector A.06.11からのアップグレード 455
16 Application Recovery Manager A.06.00からのアップグレード 458

出版履歴

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

表 1 出版履歴

製品番号	ガイド版	製品
B6960-96002	2006年7月	Data Protector リリース A.06.00
B6960-96036	2008年11月	Data Protector リリース A.06.10
B6960-90152	2009年9月	Data Protector リリース A.06.11
	2011年3月	Data Protector リリースA.06.20

本書について

本書では、以下について説明します。

- Data Protectorネットワーク製品のインストール
- Install手順の開始前に満たす必要がある前提条件
- アップグレードとライセンス

対象読者

本書は、環境のインストールおよび保守を担当する管理者と、バックアップ環境の計画、インストール、および管理を担当するバックアップ管理者を対象としています。

概念的な情報は、『 HP Data Protectorコンセプトガイド』を参照してください。 Data Protectorに関する基礎知識とモデルについてよく理解するためにも、一読することをお勧めします。

ドキュメントセット

その他のドキュメントおよびオンラインヘルプには、関連情報が記載されています。

ガイド

Data Protectorのガイドは、電子的なPDF形式で利用できます。 PDFファイルは、Data Protectorのセットアップ時に、Windowsの場合は英語のドキュメント(ガイド、ヘルプ)コンポーネントを、UNIXの場合はOB2-DOCSコンポーネントを、それぞれ選択してインストールします。 インストールしたガイドは、Windowsの場合はData_Protector_home¥docsディレクトリに、UNIXの場合は/opt/omni/doc/Cディレクトリにあります。

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

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

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

- 『*HP Data Protectorコンセプトガイド*』

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

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

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

- 『*HP Data Protectorトラブルシューティングガイド*』

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

- 『*HP Data Protectorディザスタリカバリガイド*』

  このガイドでは、ディザスタリカバリの計画、準備、テスト、および実行の方法について説明します。

- 『*HP Data Protectorインテグレーションガイド*』

  このガイドでは、さまざまなデータベースやアプリケーションをバックアップおよび復元するための、Data Protectorの構成方法および使用法を説明します。このガイドは、バックアップ管理者やオペレータを対象としています。6種類のガイドがあります。

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

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

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

    このガイドでは、Oracle Server、SAP R/3、SAP MaxDBに対応するData Protectorの統合ソフトウェアについて説明します。

  - 『*HP Data Protector Integration Guide for IBMアプリケーション: Informix, DB2, and Lotus Notes/Domino*』

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

  - 『*HP Data Protector Integration Guide for Sybase, Network Node Manager, and Network Data Management Protocol Server*』

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

- 『*HP Data Protector Integration Guide for Virtualization Environments*』

  このガイドでは、Data Protectorと仮想環境(VMware仮想インフラストラクチャおよびVMware vSphere、Microsoft Hyper-V、およびCitrix XEN Server)との統合について説明します。

- 『*HP Data Protector 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の統合について説明します。また、ドキュメントアプリケーションライターの詳細についても説明します。

- 『*HP Data Protector Integration Guide for HP Operations Manager for UNIX*』

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

- 『*HP Data Protector Integration Guide for HP Operations Manager for Windows*』

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

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

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

- 『*HP Data Protector Zero Downtime Backup Administrator's Guide*』

  このガイドでは、HP StorageWorks P6000 EVAディスクアレイファミリ、HP StorageWorks P9000 XPディスクアレイファミリ、HP StorageWorks P4000 SANソリューション、EMC Symmetrix Remote Data FacilityおよびTimeFinderに対応するData Protector統合ソフトウェアの構成方法および使用方法を説明します。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。

- 『*HP Data Protector Zero Downtime backup Integration guide*』

  このガイドでは、Oracle Server、SAP R/3、Microsoft Exchange Server、Microsoft SQL Serverの各データベースに対して、そ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、標準復元を実行するためのData Protectorの構成方法および使用方法について説明します。

- 『*HP Data Protector Granular Recovery Extension for Microsoft SharePoint Serverユーザーガイド*』

このガイドでは、Microsoft SharePoint Server用にData Protector Granular Recovery Extensionを構成し使用する方法について説明します。Data Protector Granular Recovery ExtensionはMicrosoft SharePoint ServerのCentral Administrationに組み込まれ、個々のアイテムをリカバリできるようになります。このガイドは、Microsoft SharePoint Server管理者およびData Protectorバックアップ管理者を対象としています。

- 『*HP Data Protector Granular Recovery Extension User Guide for VMware vSphere*』

  このガイドでは、VMware vSphere用Data Protector Granular Recovery Extensionの構成方法および使用方法について説明します。Data Protector Granular Recovery ExtensionはVMware vCenter Serverに組み込まれ、個々のアイテムをリカバリできるようになります。このガイドは、VMware vCenter Serverユーザーおよび Data Protectorバックアップ管理者を対象としています。

- 『*HP Data Protector Media Operations User Guide*』

  このガイドは、システムの保守とバックアップを担当するネットワーク管理者を対象に、オフラインストレージメディアの追跡と管理に関する情報を提供します。アプリケーションのインストールと構成、日常のメディア操作、およびレポート作成のタスクについて説明します。

- 『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』

  このガイドでは、HP Data Protector 6.20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されています。

- 『*HP Data Protector Product Announcements, Software Notes, and References for Integrations to HP Operations Manager*』

  このガイドは、HP Operations Manager統合ソフトウェアに対して同様の機能を果たします。

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

  このマニュアルは、Media Operationsに対して同様の機能を果たします。

- 『*HP Data Protector Command Line Interface Reference*』

  このガイドでは、Data Protectorコマンドラインインタフェース、コマンドオプション、使用方法を、コマンドラインの基本例とともに説明しています。

オンラインヘルプ

Data Protector には、WindowsおよびUNIXの各プラットフォーム用にヘルプトピックとコンテキスト依存([F1]キー)ヘルプが用意されています。

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

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

ドキュメントマップ

略称

次の表は、ドキュメントマップで使用される略称の説明です。ガイドのタイトルには、すべて先頭にHP Data Protectorが付きます。

略称	ガイド
CLI	Command Line Interface Reference
Concepts	コンセプトガイド
DR	ディザスタリカバリガイド
GS	スタートアップガイド
GRE-SPS	Granular Recovery Extension for Microsoft SharePoint Serverユーザーガイド
GRE-VMware	Granular Recovery Extension User Guide for VMware vSphere
Help	オンラインヘルプ
IG-IBM	Integration Guide for IBM Applications: Informix, DB2, and Lotus Notes/Domino
IG-MS	Microsoftアプリケーション用インテグレーションガイド－ SQL Server、SharePoint Server、およびExchange Server
IG-O/S	インテグレーションガイド - Oracle、SAP
IG-OMU	インテグレーションガイド - HP Operations Manager for UNIX
IG-OMW	Integration Guide for HP Operations Manager for Windows

略称	ガイド
IG-Var	Integration Guide for Sybase, Network Node Manager, and Network Data Management Protocol Server
IG-VirtEnv	Integration Guide for Virtualization Environments: VMware, Microsoft Hyper-V, and Citrix XEN Server
IG-VSS	Integration Guide for Microsoft Volume Shadow Copy Service
Install	インストールおよびライセンスガイド
MO GS	Media Operations Getting Started Guide
MO RN	Media Operations Product Announcements, Software Notes, and References
MO UG	Media Operations User Guide
PA	製品案内、ソフトウェアノート、リファレンス
Trouble	トラブルシューティングガイド
ZDB Admin	ZDB Administrator's Guide
ZDB Concept	ZDBコンセプトガイド
ZDB IG	ZDB Integration Guide

対応表

以下の表は、各種情報がどのドキュメントに記載されているかを示したものです。セルが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			GRE		MO			
	Help	GS	Concepts	Install	Trouble	DR	PA	MS	O/S	IBM	Var	VSS	VirtEnv	OMU	OMW	Concept	Admin	IG	SPS	VMware	GS	User	PA	CLI
バックアップ	X	X	X					X	X	X	X	X	X			X	X	X						
CLI																								X
概念/手法	X		X					X	X	X	X	X	X	X	X	X	X	X	X	X				
ディザスタリカバリ	X		X			X																		
インストール/アップグレード	X	X		X			X							X	X						X	X		
インスタントリカバリ	X		X													X	X	X						
ライセンス	X			X			X															X		
制限事項	X				X		X	X	X	X	X	X	X					X					X	
新機能	X						X																X	
プラニング方法	X		X													X								
手順/作業	X			X	X	X		X	X	X	X	X	X	X	X		X	X	X	X		X		
推奨事項			X				X									X							X	
必要条件				X			X	X	X	X	X	X	X	X	X						X	X	X	
復元	X	X	X					X	X	X	X	X	X				X	X	X	X				
サポートされる構成																X								
トラブルシューティング	X			X	X			X	X	X	X	X	X	X	X		X	X	X	X				

統合ソフトウェア

以下のソフトウェアアプリケーション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。

ソフトウェアアプリケーション	ガイド
HP Network Node Manager (NNM)	IG-Var
HP Operations Manager	IG-OMU、IG-OMW
IBM DB2 UDB	IG-IBM

ソフトウェアアプリケーション	ガイド
Informix Server	IG-IBM
Lotus Notes/Domino Server	IG-IBM
Media Operations	MO User
Microsoft Exchange Server	IG-MS、ZDB IG
Microsoft Hyper-V	IG-VirtEnv
Microsoft SharePoint Server	IG-MS、ZDB IG、GRE-SPS
Microsoft SQL Server	IG-MS、ZDB IG
Microsoftボリュームシャドウコピーサービス(VSS)	IG-VSS
ネットワークデータ管理プロトコル(NDMP)サーバー	IG-Var
Oracle Server	IG-O/S、ZDB IG
SAP MaxDB	IG-O/S
SAP R/3	IG-O/S、ZDB IG
Sybase Server	IG-Var
VMware vSphere	IG-VirtEnv、GRE-VMware

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
HP StorageWorks P4000 SANソリューション	ZDB Concept、ZDB Admin、IG-VSS
HP StorageWorks P6000 EVAディスクアレイファミリ	すべてのZDB

ディスクアレイファミリ	ガイド
HP StorageWorks P9000 XPディスクアレイファミリ	すべてのZDB

表記上の規則および記号

表 2 表記上の規則

規則	要素
青色のテキスト: 表2(27ページ)	相互参照リンクおよび電子メールアドレス
青色の下線付きテキスト: http://www.hp.com	Webサイトアドレス
*斜体*テキスト	テキストの強調
等幅テキスト	· ファイル名とディレクトリ名 · システム出力 · コード · コマンド、コマンド引数、引数の値
等幅、*斜体*テキスト	· コード変数 · コマンド変数
等幅、太字テキスト	強調された等幅テキスト

△ **注意:**

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

⓪ **重要:**

詳細情報または特定の手順を示します。

注記:

補足情報を示します。

ヒント:

役に立つ情報やショートカットを示します。

Data Protectorグラフィカルユーザーインタフェース

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

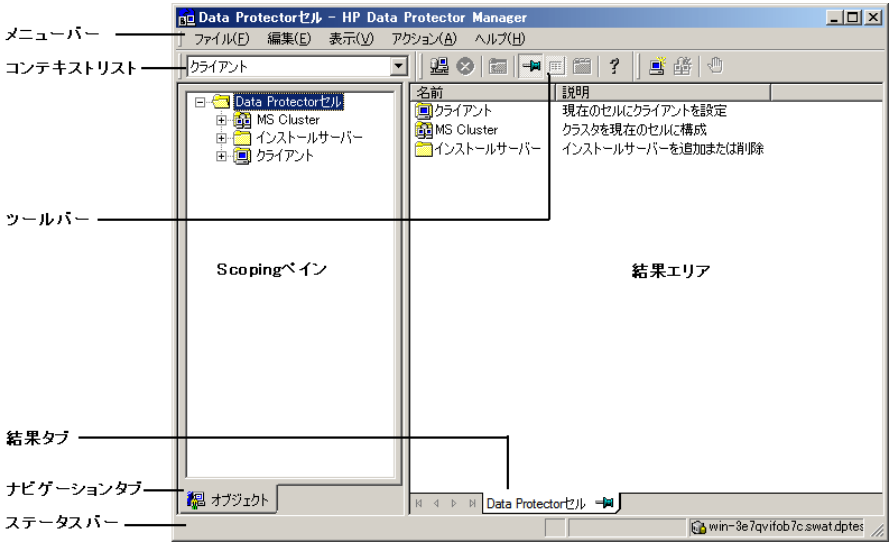


図 1 Data Protectorグラフィカルユーザーインタフェース

一般情報

Data Protectorに関する一般的な情報は、http://www.hp.com/go/dataprotectorにあります。

HPテクニカルサポート

各国のテクニカルサポート情報については、以下のアドレスのHPサポートWebサイトを参照してください。

http://www.hp.com/support

HPに問い合わせる前に、以下の情報を集めておいてください。

- 製品のモデル名とモデル番号
- 技術サポートの登録番号(ある場合)
- 製品のシリアル番号
- エラーメッセージ
- オペレーティングシステムのタイプとリビジョンレベル
- 詳細な質問内容

メールニュース配信サービス

ご使用の製品を以下のアドレスのメールニュース配信登録Webサイトで登録することをお勧めします。

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

登録すると、製品の強化機能内容、ドライバの新バージョン、ファームウェアのアップデートなどの製品リソースに関する通知が電子メールで届きます。

HP Webサイト

その他の情報については、次のHP Webサイトを参照してください。

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

ドキュメントに関する意見

HPでは、皆さまのご意見をお待ちしております。

製品ドキュメントに関するご質問やお気づきの点があれば、DP.DocFeedback@hp.comまでメッセージを送信してください。お知らせいただいた内容は、すべてHPに帰属することになります。

1 インストール手順の概要

この章の内容

この章では、Data Protectorのインストール手順の概要およびインストールに関する概念を説明します。また、この章では、Data Protector Cell ManagerおよびData Protectorについても説明します。

インストール手順の概要

Data Protectorのバックアップ環境は、同じタイムゾーンに所属し、同じLANまたはSAN上に存在する複数のシステムで構成されます。これらのシステムでは、共通のバックアップ方針が適用されます。このネットワーク環境をData Protector **セル**と呼びます。通常、セルは1つのCell Manager、複数のインストールサーバー、クライアント、およびバックアップデバイスから構成されています。

Cell Managerは、セルを集中管理するメインシステムです。Cell Managerは、Data Protector内部データベース(IDB)を含み、Data ProtectorのコアソフトウェアおよびSession Managerを実行します。

IDBには、バックアップしたファイルに関する情報と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 (IS)は、クライアントのリモートインストールに使用されるData Protectorソフトウェアレポジトリを含む、別のシステムまたはCell Managerコンポーネントです。このData Protectorの機能によって、特にリモートクライアントのソフトウェアのインストール手順が容易になります。

通常、セルは、1つのCell Managerと複数のクライアントから構成されています。Data Protectorソフトウェアコンポーネントがコンピュータシステムにインストールされると同時に、そのシステムは、Data Protector**クライアント**になります。システムにインストールされるクライアントコンポーネントは、バックアップ環境におけるシステムの役割によって異なります。Data Protectorコンポーネントは、1台のシステムにローカルに、またはインストールサーバーから複数のシステムにインストールすることができます。

ユーザーインタフェースコンポーネントは、Data Protector機能にアクセスするために必要です。すべての構成作業および管理作業は、ユーザーインタフェースを使用して行わ

れます。ユーザーインタフェースコンポーネントは、バックアップ管理に使用するシステムにインストールする必要があります。Data Protectorには、グラフィカルユーザーインタフェース(GUI)とコマンドラインインタフェース(CLI)があります。

バックアップが必要なディスクがあるクライアントシステムには、適切なData Protector **Disk Agent** コンポーネントがインストールされている必要があります。Disk Agentでは、クライアントディスクからのデータのバックアップまたはその復元ができます。

バックアップデバイスに接続されているクライアントシステムには、**Media Agent** コンポーネントがインストールされている必要があります。このソフトウェアでは、バックアップデバイスおよびメディアを管理します。Data Protectorには、**General Media Agent**および**NDMP Media Agent**という2つのMedia Agentがあります。NDMP Media Agentは、NDMPサーバーのバックアップを制御するクライアントシステム(NDMP専用ドライブを制御するクライアントシステム)にのみ必要です。それ以外の場合は、これらの2つのMedia Agentは置き換え可能です。

Data Protectorをネットワークにインストールする前に、以下の項目を決定しておく必要があります。

- Cell Managerがインストールされるシステム。サポートされるオペレーティングシステムおよびバージョンについては、最新のサポート一覧(http://www.hp.com/support/manuals)を参照してください。

  セルごとに設定できるCell Managerは1つだけです。Cell Managerがインストールされていないと、Data Protectorは実行できません。

- ユーザーインタフェースを介して、Data Protectorの機能へのアクセスに使用されるシステム。これらのシステムには、ユーザーインタフェースコンポーネントがインストールされている必要があります。
- バックアップされるシステム。これらのシステムには、ファイルシステムのバックアップ用のDisk Agentコンポーネント、およびオンラインデータベース統合用の関連Application Agentコンポーネントがインストールされている必要があります。
- バックアップデバイスの接続先となるシステム。これらのシステムには、Media Agentコンポーネントをインストールする必要があります。
- Data Protector インストールサーバーがインストールされるシステム(1台または複数)。ソフトウェアのリモートインストールには、UNIXクライアントとWindowsクライアント用の2つのタイプのインストールサーバーを使用できます。

  インストールサーバーとして選択するコンピュータは、Cell Managerおよびユーザーインタフェースがインストールされているシステムとは無関係です。Cell Managerおよびインストールサーバーは、同一のシステム(同じプラットフォームで実行される場合)、または別々のシステムにインストールできます。

  1つのインストールサーバーを複数のData Protectorセル間で共有することもできます。

注記:

Windows用インストールサーバーは、Windowsシステムにインストールする必要があります。UNIX用インストールサーバーは、HP-UX、Solaris、またはLinuxシステムにインストールする必要があります。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については、最新のサポート一覧(http://www.hp.com/support/manuals)を参照してください。

重要:

Data Protector Cell Manager、インストールサーバー、またはクライアントをSolarisシステムにインストールする場合は、/usr/omniディレクトリのすべてのファイルを別のディレクトリに保存してください。Data Protectorをインストールすると、/usr/omniディレクトリのすべてのファイルは削除されます。

Data Protectorセル内における各システムの役割を決定したら、インストール作業を行います。一般的な手順は以下のとおりです。

1. Installの前提条件が満たされていることをチェックします。
2. Data Protector Cell Managerをインストールします。
3. インストールサーバーおよびユーザーインタフェースをインストールします。
4. クライアントシステムをリモートでインストールするか(推奨)、またはインストールDVD-ROMからローカルにインストールします。

注記:

インストールサーバーをすでにインストールしてあるWindowsシステムには、Data Protectorクライアントをリモートでインストールすることはできません。同一システム上にインストールサーバーとクライアントコンポーネントをインストールする場合は、クライアントをData Protector WindowsインストールDVD-ROMからローカルにインストールする必要があります。[カスタムセットアップ]ウィンドウで、必要なクライアントコンポーネントとインストールサーバーコンポーネントをすべて選択してください。

リモートインストールは、Windows XP Home Edition、Novell NetWare、HP OpenVMSクライアントでも実行できません。ローカルにインストールする必要があります。

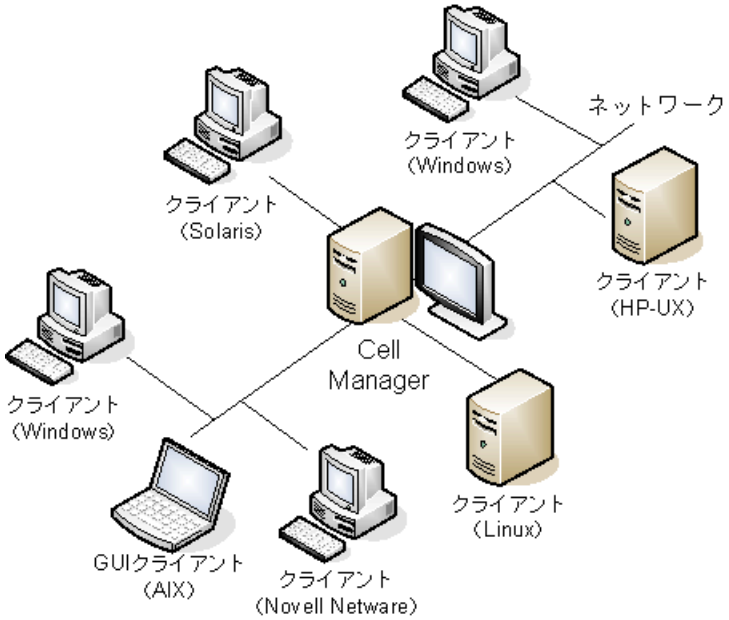


図 2 Data Protectorセル

リモートインストールの概念

Data Protector Cell Manager、ユーザーインタフェース、およびインストールサーバー(UNIX、Windowsともに少なくとも1台のインストールサーバーが必要)をインストールすると、リモートインストールがサポートされているオペレーティングシステムを使用して、Data Protectorソフトウェアをクライアントに配布できます。図3(36ページ)を参照してください。

リモートインストールを実行するたびに、GUIを介してインストールサーバーにアクセスします。ユーザーインタフェースコンポーネントはCell Managerにインストールできますが、これは前提条件ではありません。さまざまな場所からCell Managerにアクセスできるように、ユーザーインタフェースを複数のシステムにインストールすることをお勧めします。

クライアントソフトウェアは、Windows用のインストールサーバーから、Windows XP Home Edition以外のWindowsシステムに配布できます。

Windows XP Home Editionクライアントシステムは、Data ProtectorのWindowsインストールDVD-ROMからローカルにインストールする必要があります。

Data Protectorでは、Novell NetWareクライアントもサポートされていますが、クライアントのリモートインストールは使用できません。インストールは、Novellネットワークに接続されたWindowsシステムを使用して行います。

クライアントソフトウェアは、HP-UX、Solaris、Linux、AIX、およびその他のサポートされているUNIXオペレーティングシステムに、UNIX用のインストールサーバーからリモートでインストールできます。サポートされるプラットフォームの一覧は、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。

Install先のシステムがリモートインストールをサポートしていないUNIXオペレーティングシステムである場合や、UNIX用のインストールサーバーをインストールしていない場合は、Data ProtectorのUNIX用インストールDVD-ROMを使用して、UNIXクライアントをローカルにインストールできます。

ただし、一部のOS環境については、リモートインストールしか実行できない場合があります。

さまざまなData Protectorクライアントのそれぞれのインストール方法の詳細は、「Data Protectorクライアントのインストール」(72ページ)を参照してください。

UNIXクライアントのローカルアンインストールの手順は、「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)を参照してください。

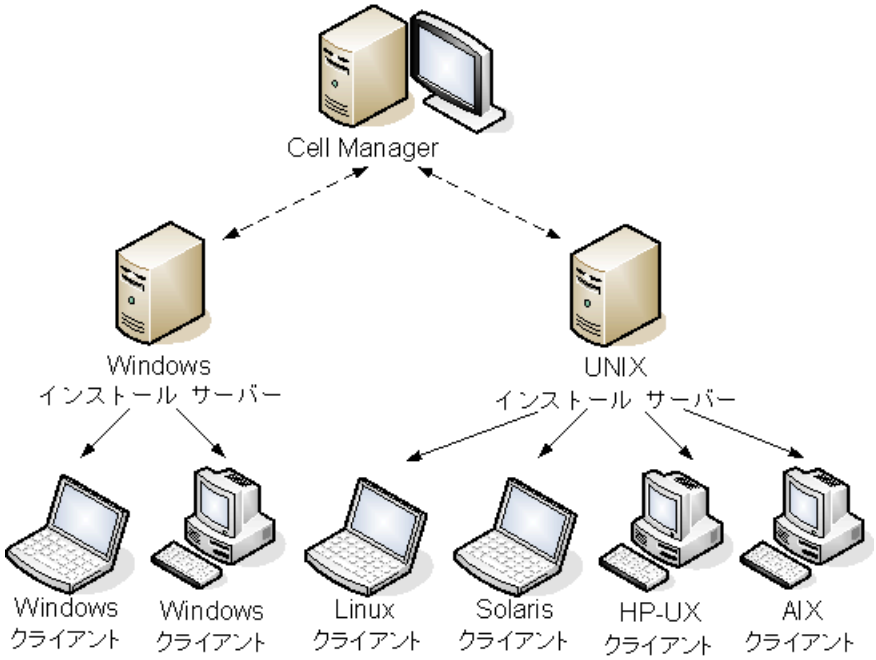


図 3 Data Protectorのインストールの概念

Data ProtectorのインストールDVD-ROM

Data Protectorでは、さまざまなオペレーティングシステムおよび複数のプロセッサアーキテクチャがサポートされています。すべてのプラットフォームに対応するために、DVD-ROMが3枚用意されています。DVD-ROMに収録されているコンポーネントの一覧は、表3（37ページ）を参照してください。

注記：

Windows Vista、Windows 7、およびWindows Server 2008オペレーティングシステム用のData Protectorインストールファイルは、Data Protectorによってデジタル署名されています。

表 3 Data Protector DVD-ROMの一覧

DVD番号	DVD-ROMのタイトル	内容
1	Data Protector Starter Pack for Windows Media Operations、Novell Netware用のエージェント、HP OpenVMSクライアントが含まれています。	・ Windows 32ビット/64ビット(AMD64/Intel EM64T)システム用のCell Managerおよびインストールサーバー ・ HP AutoPass[1] ・ PDF形式の英語版マニュアル一式(DOCSディレクトリ) ・ Windows IA-64クライアント ・ Novell NetWareクライアント ・ HP OpenVMSクライアント(AlphaおよびIA64システム) ・ Windowsプラットフォーム用の製品デモ ・ 製品情報 ・ HPソフトウェア統合パッケージ ・ HP Data Protector Media Operationsのインストールパッケージ
2	Data Protectorスターターパック(HP-UX用) HP-UX、Solaris、およびLinuxクライアント用エージェントを含みます。	・ HP-UXシステム用のCell Manager、インストールサーバー、およびクライアント ・ その他のUNIXシステムのクライアント ・ Mac OS Xシステム用のクライアント ・ HP AutoPass[2] ・ PDF形式の英語版マニュアル一式(DOCSディレクトリ) ・ HPソフトウェア統合パッケージ

DVD番号	DVD-ROMのタイトル	内容
3	Data Protectorスターターパック(HP-UX、Solaris、およびLinux用) HP-UX、Solaris、およびLinuxクライアント用エージェントを含みます。	・ SolarisおよびLinux用のCell Manager、インストールサーバー、およびクライアント ・ その他のUNIXシステムのクライアント ・ Mac OS Xシステム用のクライアント ・ HP AutoPass[2] ・ PDF形式の英語版マニュアル一式(DOCSディレクトリ) ・ HPソフトウェア統合パッケージ

[1]Windows Server 2003 x64、Windows Vista x64、Windows Server 2008 x64上ではHP AutoPassは使用できません。

[2]Linux上ではHP AutoPassは使用できません。

Cell Managerシステムの選択

Cell Managerは、Data Protectorセル内のメインシステムです。Cell Managerの機能は次のとおりです。

- セルを集中管理します。
- IDB(バックアップセッション、復元セッション、およびメディア管理セッションに関する情報を格納するファイル)を維持します。
- Data Protectorのコアソフトウェアを実行します。
- Session Managerを実行します。Session Managerは、バックアップセッションおよび復元セッションの開始と停止を制御し、セッション情報をIDBに書き込みます。

お使いの環境のどのシステムをCell Managerとして使用するかを決定する際には、以下の点に留意してください。

- サポート対象プラットフォーム

  Cell Managerは、Windows、HP-UX、SolarisまたはLinuxプラットフォームのいずれかにインストールできます。これらのプラットフォームのサポートされるバージョンまたはリリースの詳細は、最新のサポート一覧(http://www.hp.com/support/manuals)を参照してください。

- Cell Managerシステムの信頼性

  Cell Manager上ではIDBが保持されており、Cell Managerが正常に動作していないとバックアップや復元を実行できなくなるため、お使いの環境では特に信頼性の高いシステムを選択してください。

- データベースのサイズの増加および 必要なディスクスペース

Cell Managerは、Data Protector内部データベース(IDB)を保持しています。IDBには、バックアップデータとそのメディア、セッションメッセージ、およびデバイスに関する情報が含まれます。環境によっては、IDBのサイズがかなり増加する可能性があります。たとえば、バックアップの大部分がファイルシステムバックアップの場合は、標準的なIDBのサイズは、バックアップされたデータに使用されるディスクスペースの2%となります。IDB_capacity_planning.xlsの表(Data ProtectorインストールDVD-ROMに収納)を使用して、IDBのサイズを見積ることができます。

データベースのサイズおよび拡張に関する計画および管理の詳細は、オンラインヘルプの索引「IDBのサイズ増加とパフォーマンス」を参照してください。

IDBに必要な最小ディスクスペースについては、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。

注記:

Cell Managerをグラフィカルユーザーインタフェースシステムとして使用する必要はありません。たとえば、UNIX用Cell Managerを使用していても、ユーザーインタフェースコンポーネントがWindowsクライアントにインストールされている場合があります。

この次に行う作業

「Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール」(44ページ)を参照して、将来のCell Managerシステムの最小要件を決定します。

Data Protectorユーザーインタフェースシステムの選択

Data Protectorでは、GUI およびCLIを Windows、HP-UX、Solaris、およびLinuxプラットフォームに提供します。ユーザーインタフェースは、Data Protectorソフトウェアコンポーネントとしてインストールされます。

セルの制御用に選択したシステムは、ネットワーク管理者またはバックアップオペレータが使用することになります。

ただし大規模なコンピュータ環境では、複数のシステム上でユーザーインタフェースを使用できる方が便利です。また、混在環境では、プラットフォームの異なる複数のシステム上にユーザーインタフェースを配置するのが理想的です。

たとえば、混在UNIXネットワークで、少なくとも1台のSolarisまたはHP-UXシステムにユーザーインタフェースがインストールされている場合は、そのユーザーインタフェースの表示をXサーバーが実行されているその他の任意のUNIXシステムにエクスポートすることができます。ただし、パフォーマンスを保つために、Data Protectorセルを制御するために使用されるすべてのシステムにData ProtectorGUIをインストールすることをお勧めします。

多くのWindowsシステムをバックアップする必要があるオフィスでは、利便性のために、ローカルのバックアップおよび復元作業をローカルのWindowsシステムから制御する方が望ましい場合があります。この場合は、ユーザーインタフェースコンポーネントをWindowsシステムにインストールします。また、ロケールを変更する必要がないため、異機種環境ではWindowsシステムのData Protector GUIを使用した方が簡単に処理できます。

UNIX Cell Managerプラットフォームでは、Data Protector Java GUI(サポートされている場合)またはomniusersコマンドを使用して、Cell Managerのリモートユーザーアカウントを作成できます。このユーザーアカウントを使用して、Data ProtectorGUIがインストールされているその他の任意のシステムでGUIを起動し、Cell Managerに接続できます。詳細は、omniusersのマンページを参照してください。

ユーザーインタフェースについてサポート対象のオペレーティングシステムのバージョンやリリースの詳細は、http://www.hp.com/support/manualsを参照してください。ローカル言語サポート、およびファイル名に非ASCII文字を使用することについては、オンラインヘルプの索引「言語設定、カスタマイズ」を参照してください。

セル内のシステムにユーザーインタフェースをインストールすると、そのシステムからCell Managerにリモートでアクセスできます。Cell Managerでグラフィカルユーザーインタフェースシステムを使用する必要はありません。

Data Protectorグラフィカルユーザーインタフェース

Data Protector GUIは高機能ユーザーインタフェースであり、Data Protectorの機能に簡単にアクセスできます。メインウィンドウには、[**Clients**]、[**Users**]、[**Devices & Media**]、[**Backup**]、[**Restore**]、[**Object Operations**]、[**Reporting**]、[**Monitor**]、[**Instant Recovery**]、[**Internal Database**]などのビューがあり、関連するすべての作業をこれらのビューで行うことができます。

たとえば、[**Clients**]ビューでは、すべての対象システム、および指定したインストールサーバーに送られるインストールパスとオプションを指定することによって、クライアントをリモートでインストール(追加)できます。クライアントでセットアップが稼動している場合は、インストール固有のメッセージがモニターウィンドウに表示されます。

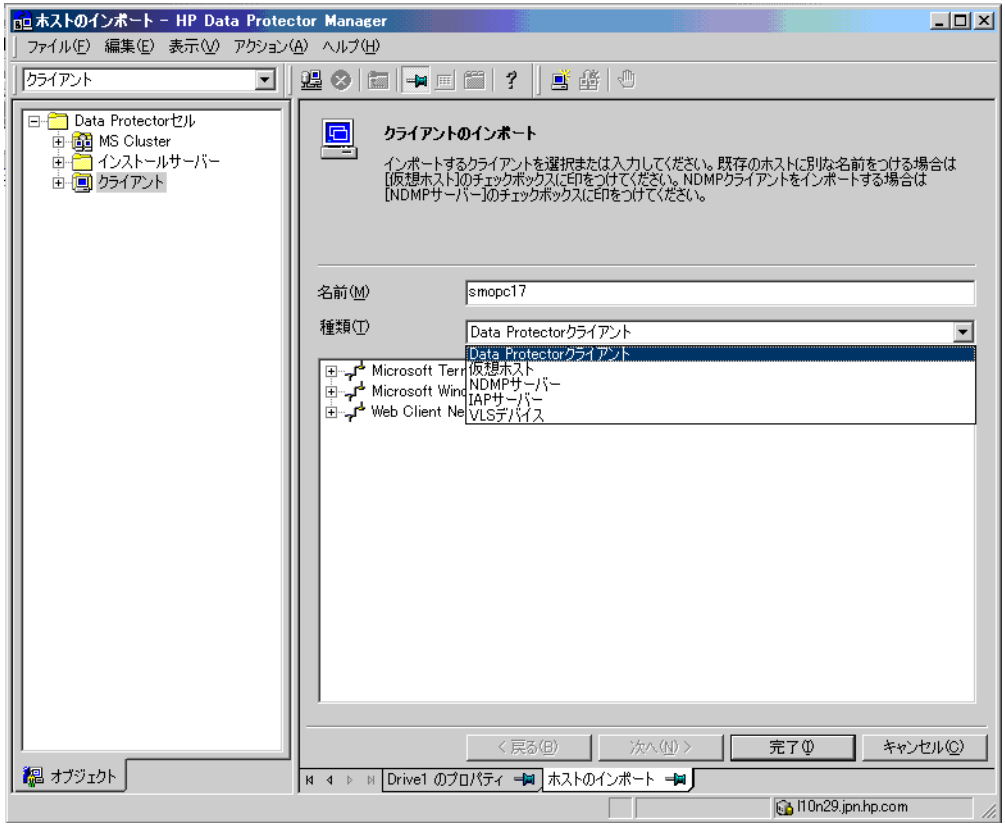


図 4 Data Protectorグラフィカルユーザーインタフェース

本書の前書きにある図1(29ページ)も参照してください。この図にはData Protector GUIの主な領域が示されています。

注記:

UNIXでは、Data Protector GUIを起動する前に、GUIが稼動しているシステムのローカル設定を調整する必要があります。これによって、GUIの文字エンコードを切り換えられ、ファイル名およびセッションメッセージに含まれる非ASCII文字を表示するための正しいエンコードを選択できるようになります。詳細は、オンラインヘルプの索引「設定、UNIXのGUIのロケール」を参照してください。

2 ネットワークへのData Protectorのインストール

この章の内容

この章では、以下の各作業について詳細な手順を示します。

- Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール詳細については、「Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール」(44ページ)を参照してください。
- Data Protectorクライアントのインストール。詳細については、「Data Protectorクライアントのインストール」(72ページ)を参照してください。
- Data Protector統合クライアントのインストール。詳細については、「Data Protector統合クライアントのインストール」(151ページ) を参照してください。
- 各国語版Data Protectorユーザーインタフェースのインストール。詳細については、「各国語版Data Protectorユーザーインタフェースのインストール」(187ページ)を参照してください。
- Data Protectorシングルサーバー版のインストール詳細については、「Data Protectorシングルサーバー版のインストール」(191ページ)を参照してください。
- Data Protector Web Reportingのインストール。詳細については、「Data Protector Web Reportingのインストール」(192ページ)を参照してください。
- MC/ServiceGuardへのData Protectorのインストール。詳細については、「MC/ServiceGuardへのData Protectorのインストール」(193ページ)を参照してください。
- Microsoft Cluster ServerへのData Protectorのインストール詳細については、「Microsoft Cluster ServerへのData Protectorのインストール」(195ページ)を参照してください。
- Veritas ClusterへのData Protectorクライアントのインストール。詳細については、「Veritas ClusterへのData Protectorクライアントのインストール」(207ページ)を参照してください。
- Novell NetWare ClusterへのData Protectorクライアントのインストール。詳細については、「Novell NetWare ClusterへのData Protectorクライアントのインストール」(208ページ)を参照してください。

Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール

Install手順は、図5（44ページ）およびを参照してください。

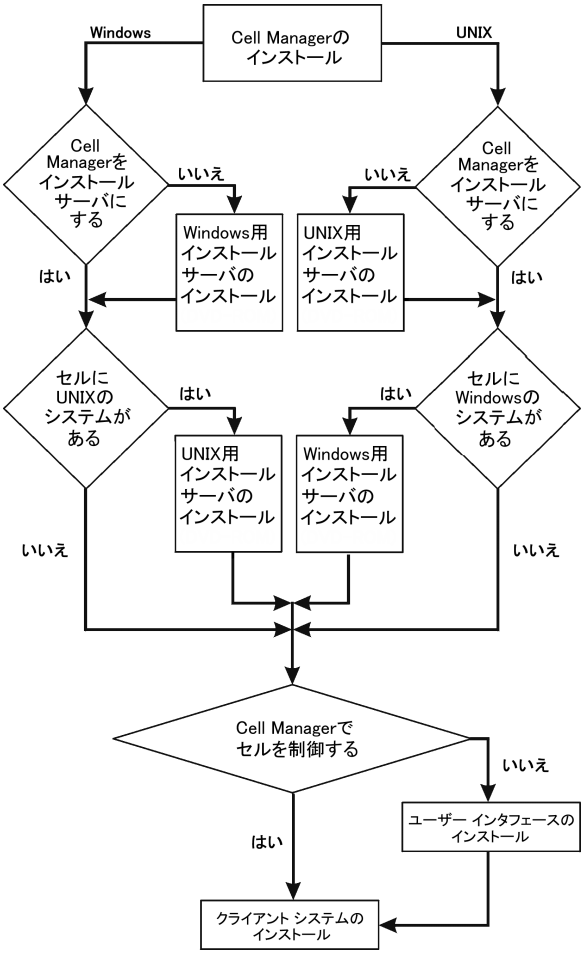


図 5 インストール手順

Cell Managerとインストールサーバーを同一システム上にインストールする場合は、この作業を1つにまとめて実施できます。

重要:

Data Protectorセル内の構成情報やセッション情報に関するファイルはすべて、Cell Manager上に保存されます。これらの情報を後から別のシステムに移動するのは困難です。そのため、適正に管理されている安定した環境内の信頼性の高いシステムを、Cell Managerとして選択してください。

UNIX用Cell Managerのインストール

この項では、UNIX用Cell Managerのインストール手順について、順を追って詳しく説明します。Windows用Cell Managerのみをインストールする場合は、「Windows用Cell Managerのインストール」(55ページ)を参照してください。

前提条件

- Cell Managerとして機能させるHP-UX、Solaris、またはLinuxシステムは、以下の条件を満たしていなければなりません。
  - Data Protectorソフトウェアをインストールするのに十分な大きさの空きディスクスペースがあること。詳細については、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。ディスク容量の不足については、リンクディレクトリにインストールすることで解決できますが、最初に「HP-UX、Solaris、およびLinuxにインストールされるディレクトリの構造」(50ページ)および「Cell Managerのインストール用に割り当てるディスクスペースを増やす」(54ページ)を必ずお読みください。
  - IDBを作成するのに十分な大きさの空きディスクスペース(バックアップ対象データの約2%)があること。詳細は『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。現在のIDBの仕様では、データベースのサイズが大きくなった場合に、必要に応じてデータベースのバイナリファイルを再配置できます。オンラインヘルプの索引「IDB、サイズの計算」を参照してください。
  - ロングファイル名がサポートされていること。使用しているファイルシステムでロングファイル名がサポートされているかどうかを調べる場合は、`getconf NAME_MAX directory`コマンドを使用します。
  - `inetd`または`xinetd`デーモンが正常に稼働していること。
  - ポート番号5555(デフォルト)が利用可能であること。このポート番号がすでに使用されている場合は、「Data Protectorのデフォルトのポート番号の変更」(388ページ)を参照してください。
  - TCP/IPプロトコルがインストールされており、実行されていること。このプロトコルを使って、ホスト名を解決できること。
  - DVD-ROMドライブにアクセスできること。

- NISサーバーを使用する場合は、Cell Managerを認識するように構成されていること。詳細については、「NISサーバーの準備」(394ページ)を参照してください。
- Java GUIサーバーまたはJava GUIクライアントをインストールする場合は、ポート番号5556を利用可能にします。
- Java GUIクライアントの場合、Java実行時環境のサポート対象バージョンが必要です。*HP Data Protector製品案内*、*ソフトウェアノート*、*リファレンス*、または最新のサポート一覧(http://www.hp.com/support/manuals)を参照してください。

- ターゲットシステムに対するrootパーミッションが必要です。

注記:

Cell Managerでは元のData Protector GUIがサポートされません。Data Protector Java GUIを使用するか、Data Protector GUIがサポートされているシステムに元のData Protector GUIをインストールしてください。新しいCell Manager上にリモートユーザーアカウントを作成するには、omniusersコマンドを使用します。これにより、Data Protector GUIをインストールした任意のシステム上でこのユーザーアカウントを使ってGUIを起動し、新しいCell Managerに接続できます。詳細はomniusersのマンページを参照してください。

クラスター対応Cell Manager

クラスター対応Cell Managerをインストールする場合は、前述の説明以外にも必要となる前提条件および手順があります。詳細については、「クラスター対応Cell Managerのインストール」(194ページ)を参照してください。

注記:

マルチセル環境(MoM)では、すべてのCell Managerに同じバージョンのData Protectorをインストールする必要があります。

推奨事項

- *UNIX*プラットフォームでは、ラージファイルサポート(LFS)の使用をお勧めします。推奨事項は、2 GBを超える可能性があるDCバイナリファイルが格納された内部データベースを保持するファイルシステムに適用されます。

カーネルパラメータの設定

HP-UXの場合、カーネルパラメータmaxdsiz(最大データセグメントサイズ)またはmaxdsiz_64 (64ビットシステムの場合)を134217728バイト(128MB)以上に、また、カーネルパラメータsemmnu (セマフォ取り消し構造体の数)を256以上に、それぞれ設定することをお勧めします。パラメータを変更したときは、カーネルを再コンパイルし、マシンを再起動してください。

Solarisの場合、/etc/system内のカーネルパラメータshmsys:shminfo_shmmax(最大共有メモリーセグメントサイズ(SHMMAX))を67108864バイト(64MB)以上に設定することをお勧めします。パラメータを変更したときは、この変更を確定し、マシンを再起動してください。

インストール手順

ヒント:

Cell Managerとインストールサーバーを同じシステム上にインストールする場合は、omnisetup.sh -CM -ISコマンドを使用して、この作業をワンステップで実行できます。

omnisetup.shコマンドの説明については、DVD-ROMのMount_point/LOCAL_INSTALLディレクトリにあるREADMEファイル、またはDVD-ROMのMount_point/DOCS/C/MANディレクトリにある『*HP Data Protector Command Line Interface Reference*』を参照してください。

HP-UXシステム、Solarisシステム、またはLinuxシステムにCell Managerをインストールするには、以下の手順に従ってください。

1. HP-UX用またはSolarisおよびLinux用のインストールDVD-ROMをドライブに挿入し、マウントポイントにマウントします。

   たとえば、次のように入力してください。

   ```
   mkdir /dvdrom
   mount /dev/dsk/c0t0d0 /dvdrom
   ```

   必要であれば、Data Protectorをディスク上のデポからインストールすることもできます。その場合は、以下の手順に従ってください。

   - Installファイルが格納されているディレクトリをローカルディスクにコピーする場合は、以下のコマンドを実行します。

     ```
     mkdir directory
     cp -r /dvdrom/platform_dir/DP_DEPOT directory
     cp -r /dvdrom/LOCAL_INSTALL directory
     ```

     ここで、*platform_dir*には、以下のいずれかの値を指定します。

hpux	HP-UXシステム
linux_x86_64	AMD64/Intel EM64T上のLinuxシステム
Solaris	Solarisシステム

   - DVD-ROM全体をローカルディスクにコピーするには、以下のコマンドを実行します。

     ```
     cp -r /dvdrom dvd_image_dir
     ```

2. omnisetup.shコマンドを実行します。

   このコマンドをDVD-ROMから実行するには、以下のコマンドを実行します。

   ```
   cd /dvdrom/LOCAL_INSTALL
   ./omnisetup.sh -CM
   ```

   ディスクからインストールを開始するには、以下の手順に従ってください。

   - Installディレクトリをローカルディスクの*directory*にコピーした場合は、以下のコマンドを実行します。

     ```
     cd directory/LOCAL_INSTALL
     ./omnisetup.sh -CM
     ```

   - DVD-ROM全体を*dvd_image_dir*にコピーした場合は、-CMパラメータを指定してomnisetup.shコマンドを実行します。

     ```
     cd dvd_image_dir/LOCAL_INSTALL
     ./omnisetup.sh -CM
     ```

3. ***HP-UXおよびSolarisの場合***、omnisetup.shコマンドを実行するとプロンプトが表示され、購入済みライセンスのパスワードをHP Password Delivery CenterのWebサーバーからインターネットを介して直接ダウンロードしてインストールする場合は、HP AutoPassユーティリティをインストールまたはアップグレードするよう指示されます。AutoPassユーティリティの詳細は、「HP AutoPassユーティリティを使用した恒久パスワードの取得とインストール」(328ページ)およびHP AutoPassのオンラインヘルプを参照してください。AutoPassはできるだけインストールすることをお勧めします。

   AutoPassをMC/ServiceGuardにインストールする場合は、すべてのノードにインストールする必要があります。

   確認が表示されたら、[Return]キーを押して、AutoPassをインストールまたはアップグレードします。AutoPassをインストールまたはアップグレードしたくない場合は、nを入力します。

   Linuxシステムでは、HP AutoPassはインストールされません。

注記:

Solaris 9またはSolaris 10上でCell Managerをインストールした場合は、インストールの完了後にインストールサーバーを使用してCell Manager上にDisk Agentをリモートインストールすることができます。これにより、汎用のSolaris Disk AgentがSolaris 9 Disk AgentまたはSolaris 10 Disk Agentに置き換えられます。Solaris 10では、Cell Manager上でのMedia Agentのリモートインストールも必要です。詳細は、「Data Protectorクライアントのリモートインストール」(82ページ)を参照するか、または`ob2install`のマンページを参照してください。

UNIX用のインストールサーバーをCell Manager上にインストールする場合は、この段階でインストールしてください。必要な手順の詳細は、「UNIX用のインストールサーバーのインストール」(63ページ)を参照してください。

HP-UX、Solaris、およびLinuxにインストールされるディレクトリの構造

Data Protectorのコアソフトウェアは/opt/omni/binディレクトリにインストールされ、UNIX用のインストールサーバーは/opt/omni/databases/vendorディレクトリにインストールされます。以下の一覧はData Protectorのサブディレクトリとその内容を示したものです。

重要:

Data Protectorは、たとえば次のようなリンクディレクトリにインストールすることができます。

```
/opt/omni/ -> /prefix/opt/omni/
/var/opt/omni/ -> /prefix/var/opt/omni/
/etc/opt/omni/ -> /prefix/etc/opt/omni/
```

このようにする場合は、インストール前にリンクを作成しておき、インストール先ディレクトリが存在することを確認しておかなければなりません。

詳細は、「Cell Managerのインストール用に割り当てるディスクスペースを増やす」(54ページ)を参照してください。

/opt/omni/bin	すべてのコマンド
/opt/omni/help/C	オンラインヘルプファイル
/opt/omni/lbin	Data Protector内部コマンド

/opt/omni/sbin	スーパーユーザー用コマンド
/opt/omni/sbin/install	Install用スクリプト
/etc/opt/omni	構成情報
/opt/omni/lib	圧縮、データ暗号化、デバイス処理のための共有ライブラリ
/opt/omni/doc/C	電子的なPDF形式のガイド(省略可能)
/var/opt/omni/log and /var/opt/omni/server/log	ログファイル
/opt/omni/lib/nls/C	メッセージカタログファイル
/opt/omni/lib/man	マンページ
/var/opt/omni/tmp	一時ファイル
/var/opt/omni/server/db40	IDBファイル。オンラインヘルプの索引「IDB、ディレクトリの場所」を参照してください。
/opt/omni/java/server	Java GUIサーバーの実行可能ファイルが格納されているディレクトリ
/opt/omni/java/client	Java GUIクライアントの実行可能ファイルが格納されているディレクトリ

自動での起動とシャットダウンの構成

Data Protectorのインストール時には、システムの再起動時にすべてのData Protectorプロセスが自動的にシャットダウンおよび起動されるように構成されます。この構成の一部は、オペレーティングシステムによって異なります。

以下のファイルが自動的に構成されます。

HP-UX:

/sbin/init.d/omni

起動処理およびシャットダウン処理を実行するスクリプト。

/sbin/rc1.d/K162omni

Data Protectorをシャットダウンする/sbin/init.d/omniスクリプトへのリンク。

/sbin/rc2.d/S838omni

Data Protectorを起動する/sbin/init.d/omniスクリプトへのリンク。

/etc/rc.config.d/omni

omni変数が格納されます。この変数は、以下のいずれかの値をとります。

omni=1　システムの再ブート時にData Protectorの自動停止および自動起動を行います。デフォルトでは、この値が適用されます。

omni=0　システムの再ブート時にData Protectorの自動停止および自動起動を行いません。

Solarisの場合:

/etc/init.d/omni

起動処理およびシャットダウン処理を実行するスクリプト。

/etc/rc1.d/K09omni

Data Protectorをシャットダウンする/etc/init.d/omniスクリプトへのリンク。

/etc/rc2.d/S97omni

Data Protectorを起動する/etc/init.d/omniスクリプトへのリンク。

Linuxの場合:

/etc/init.d/omni

起動処理およびシャットダウン処理を実行するスクリプト。

/etc/rcinit_level.d/K10omni

Data Protectorをシャットダウンする/etc/init.d/omniスクリプトへのリンク。

*init_level*は1および6です。

/etc/rcinit_level.d/S90omni

Data Protectorを起動する/etc/init.d/omniスクリプトへのリンク。

*init_level*は2、3、4、および5です。

Install中には、Cell Managerシステムのシステムファイルのうち、以下のファイルが修正されます。

HP-UX:

/etc/services

Data Protectorのサービス用ポート番号がファイルに追加されます。

/opt/omni/lbin/crs

Data Protector CRSサービスが追加されます。

Installが完了すると、以下のプロセスがCell Manager上で動作するようになります。

/opt/omni/lbin/crs

Data Protector Cell Request Server (CRS)サービス Cell Managerシステム上で実行され、Cell Managerソフトウェアがシステムにインストールされると起動されます。CRSは、セル内のバックアップセッションおよび復元セッションの開始および制御に使用されます。

/opt/omni/lbin/rds

Data Protector Raima Database Server (RDS)サービス Cell Managerシステム上で実行され、Cell Managerソフトウェアがシステムにインストールされると起動されます。RDSは、IDBの管理に使用されます。

/opt/omni/lbin/mmd

Data Protector Media Management Daemon (MMD)サービス Cell Manager上で実行され、Cell Managerソフトウェアがシステムにインストールされると起動されます。MMDは、デバイスおよびメディアの管理操作に使用されます。

/opt/omni/lbin/inetd

Data Protector 常駐サービス ネットワーク上の他のシステムでData Protectorサービスと通信できます。Inetサービスは、Data Protectorセル内のすべてのシステム上で実行することが必要です。

/opt/omni/lbin/kms

Data Protector Key Management Server (KMS)サービス Cell Manager上で実行され、Cell Managerソフトウェアがシステムにインストールされると起動されます。KMSは、Data Protector暗号化機能のキーを管理します。

/opt/omni/java/server/bin/uiproxyd

システムにCell Managerソフトウェアをインストールすると、Cell Managerシステム上でData Protector Java GUIサーバー(UIProxyサービス)が実行されます。UIProxyサービスは、Java GUIクライアントとCell Manager間の通信を行います。

環境変数の設定

先に説明したUNIX用Cell Managerのインストール時には、Data Protectorのユーザーインタフェースもインストールされます。

ユーザーインタフェース(グラフィカルユーザーインタフェースまたはコマンドラインインタフェース)を使用する場合は、事前に次の内容を環境変数に追加してください。

/opt/omni/bin、/opt/omni/lbin、および、/opt/omni/sbinを、PATH変数に追加します。

/opt/omni/lib/manをMANPATH変数に追加します。

/opt/omni/libおよび/opt/omni/lib/armをLD_LIBRARY_PATH変数に追加します。

さらに、グラフィカルユーザーインタフェースを使用する前に、DISPLAY変数とロケール設定が正しく設定されていることも確認してください。

注記:

Data Protectorユーザーインタフェースを使用して複数のプラットフォームでバックアップまたは復元を行う場合は、その際の制限事項については*HP Data Protector製品案内、ソフトウェアノート、リファレンス*を、Data Protector GUIでの言語設定のカスタマイズ方法についてはオンラインヘルプの索引「言語設定のカスタマイズ」をそれぞれ参照してください。

Cell Managerのインストール用に割り当てるディスクスペースを増やす

UNIX用Cell Managerをインストールする場合は、特に、/optディレクトリと、データベースの保存先となる/varディレクトリに、十分な空きディスクスペース(バックアップ対象データの約2%)が必要です。必要となるディスクスペースの詳細は、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。ディスクスペースが足りない場合はリンクディレクトリを使用することも可能ですが、その場合はインストール前にリンクを作成しておき、インストール先ディレクトリが存在することを確認しておかなければなりません。

この次に行う作業

この段階で、Cell Manager(および選択した場合はUNIX用のインストールサーバー)がインストールされています。準備が整ったら、以下の作業を実施します。

1. UNIX用のインストールサーバーを同一システム上にインストールしなかった場合は、「UNIX用のインストールサーバーのインストール」(63ページ)を参照してください。
2. ソフトウェアをWindowsクライアントにリモートインストールしたい場合は、Windows用のインストールサーバーをインストールします。詳細については、「Windows用のインストールサーバーのインストール」(68ページ)を参照してください。
3. ソフトウェアをクライアントに配布します。詳細については、「Data Protectorクライアントのインストール」(72ページ)を参照してください。

Windows用Cell Managerのインストール

前提条件

Windows Cell Managerをインストールするには、Administrator権限が必要です。Cell Managerシステムとして使用するWindowsシステムは、以下の条件を満たしている必要があります。

- サポート対象のWindowsオペレーティングシステムがインストールされていること。Cell Managerで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、http://www.hp.com/support/manualsを参照してください。
- Microsoft Internet Explorer 5.0以上がインストールされていること。
- Data Protector Cell Managerソフトウェアをインストールするのに十分な容量の空きディスクスペースがあること。詳細については、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- IDBを作成するのに十分な容量の空きディスクスペース(バックアップ対象データの約2%)があること。詳細は、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- ポート番号5555 (デフォルト)が利用可能であること。このポート番号がすでに使用されている場合は、「Data Protectorのデフォルトのポート番号の変更」(388ページ)を参照してください。
- Cell Managerのインストール先のシステムには、静的なIPアドレスが必要です。DHCPクライアントとして構成されているシステムの場合は、そのIPアドレスが変更されます。そのため、システムに恒久DNSを割り当てる(再構成する)か、DHCPサーバーでシステムの静的IPアドレス(IPアドレスはシステムのMACアドレスにバインドされる)を構成する必要があります。
- Microsoft社のTCP/IPプロトコルがインストールされており、実行されていること。このプロトコルを使って、ホスト名を解決できること。コンピュータの名前とホスト名は同じでなければなりません。
- DVD-ROMドライブにアクセスできること。
- Java GUIサーバーまたはJava GUIクライアントをインストールする場合は、ポート番号5556を利用可能にします。
- Java GUIクライアントの場合、Java実行時環境のサポート対象バージョンが必要です。『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』、または最新のサポート一覧(http://www.hp.com/support/manuals)を参照してください。
- ネットワークアクセスユーザー権限が、インストールを実行するアカウントのWindowsローカルセキュリティポリシーの下に設定されていることを確認します。

Microsoftターミナルサービスクライアント

- Microsoftターミナルサービスクライントを介してWindows上にData Protectorをインストールする場合は、Data Protectorのインストール先システムで、**[ターミナルサーバーモード]**が**[リモート管理]**に設定されていることを確認してください。
  1. Windowsの[コントロールパネル]で**[管理ツール]**をクリックし、次に**[ターミナルサービス構成]**をクリックします。
  2. [ターミナルサービス構成]ダイアログボックスで、**[サーバー設定]**をクリックします。ターミナルサービスサーバーがリモート管理モードで実行中であることを確認してください。

推奨事項

- Data Protector 6.20のインストール前に Microsoft Installer (MSI) 2.0があることを確認します。MSIのバージョンが古い場合は、Data Protectorセットアッププログラムにより、自動的にバージョン2.0にアップグレードされます。この場合、Data Protectorによって、アップグレードの最後の段階でMSIがアップグレードされたことが通知されます。MSIがアップグレードされた場合は、システムを再起動することを強く推奨します。

  Data Protector 6.20をインストールする前に、MSIをバージョン2.0にアップグレードすることをお勧めします。
- DCバイナリファイルが2GBを超える可能性がある場合(ファイルシステムの設定によってのみ制限される)、NTFSファイルシステムの使用をお勧めします。

クラスター対応Cell Manager

クラスター対応Cell Managerをインストールする場合は、前述の説明以外にも必要となる前提条件および手順があります。詳細については、「クラスター対応Cell Managerのインストール」(195ページ)を参照してください。

インストール手順

Windowsシステムに新規でインストールするには、以下の手順に従ってください。

1. WindowsインストールDVD-ROM

   Windows Server 2008の場合は、[ユーザーアカウント制御]ダイアログボックスが表示されます。**[続行]**をクリックしてインストールを続けます。
2. HP Data Protectorウィンドウで**[インストールData Protector]**を選択し、Data Protectorのセットアップ用ウィザードを開始します。
3. セットアップ用ウィザードの指示に従って操作を行い、ライセンス契約を十分にお読みください。記載内容に同意する場合は、**[Next]**をクリックして次に進みます。

4. [Installation Type]ページで、[Cell Manager]を選択します。[Next]をクリックすると、選択したData Protector Cell Managerソフトウェアがインストールされます。

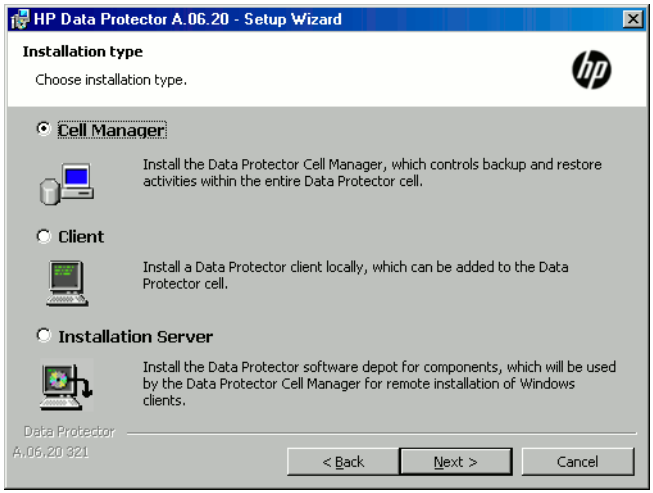


図 6 インストールの種類の選択

5. Data Protectorサービスを実行するアカウントの、ユーザー名とパスワードを入力します。[Next]をクリックし、次に進みます。

6. Data Protectorをデフォルトフォルダにインストールする場合には、[Next]をクリックします。

   それ以外の場合は、[Change]をクリックして[Change Current Destination Folder]ウィンドウを開き、別のパスを入力します。

7. [Component Selection]ページで、インストールするコンポーネントを選択します。Data Protectorコンポーネントのリストと説明は、「Data Protectorコンポーネント」(76ページ)を参照してください。

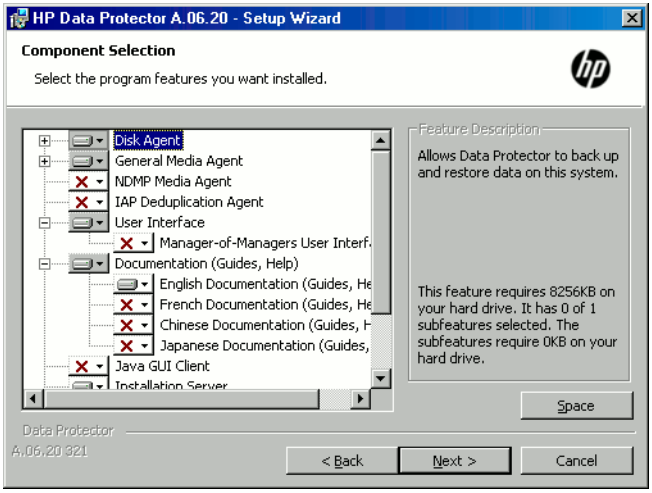


図 7 ソフトウェアコンポーネントの選択

[Disk Agent]、[General Media Agent]、[User Interface]、および[**インストールサーバー**]はデフォルトで選択されています。[Next]をクリックします。

8. *Data Protectorによってシステムに*Windows*ファイアウォールが検出されると、*[Windows Firewall configuration]ページが表示されます。Data Protectorのセットアッププログラムによって、必要なすべてのData Protector実行可能ファイルが登録されます。デフォルトでは、[Initially, enable newly registered Data Protector binaries to open ports as needed]オプションが選択されています。この時点で、Data Protectorによってポートがオープンされないようにするには、オプションを選択解除します。ただし、Data Protectorを適切に機能させるには、実行可能ファイルを有効にする必要があります。

[Next]をクリックします。

9. コンポーネントのサマリーリストが表示されます。[Install]をクリックして、選択したコンポーネントのインストールを開始します。この処理には、数分かかる場合があります。

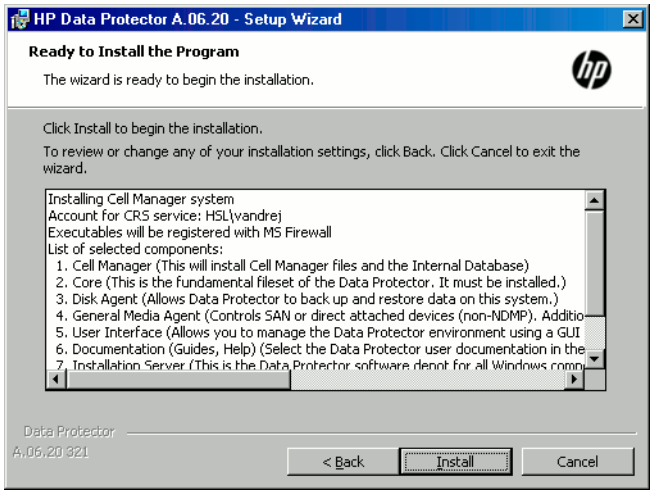


図 8 コンポーネントのサマリーリスト

10. [Installation status]ページが表示されます。[Next]をクリックします。

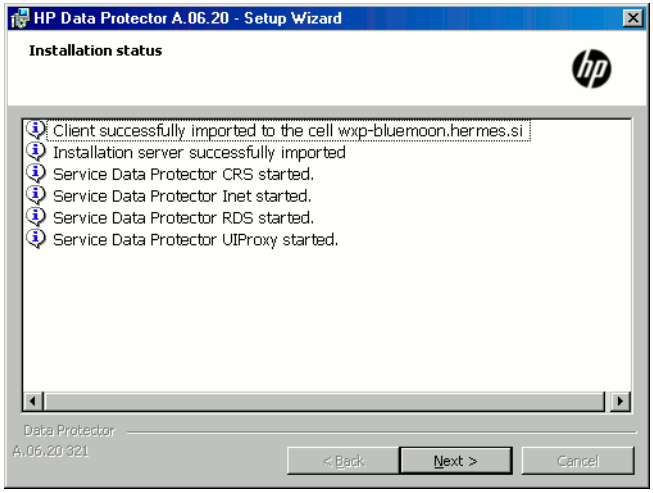


図 9 [Installation Status]ページ

11. HPパスワードセンタのWebサーバーからインターネットを介して直接購入したライセンスのパスワードをダウンロードしてインストールする場合は、セットアップ用ウィザードでHP AutoPassユーティリティをインストールまたはアップグレードできます。AutoPassユーティリティの詳細は、「HP AutoPassユーティリティを使用した恒久パスワードの取得とインストール」(328ページ)およびHP AutoPassのオンラインヘルプを参照してください。

    デフォルトでは、[Start AutoPass installation]オプションまたは[Upgrade AutoPass installation]オプションが選択されています。HP AutoPassユーティリティをインストールすることをお勧めします。AutoPassをインストールまたはアップグレードしない場合は、オプションを選択解除します。

    Windows Server 2003 x64、Windows Vista x64、およびWindows Server 2008 x64システムでは、HP AutoPassはインストールされません。

    セットアップ後すぐにData Protectorを使用するには、[Start the Data Protector Manager]を選択します。

    『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を表示するには、[Open the Product Announcements]を選択します。

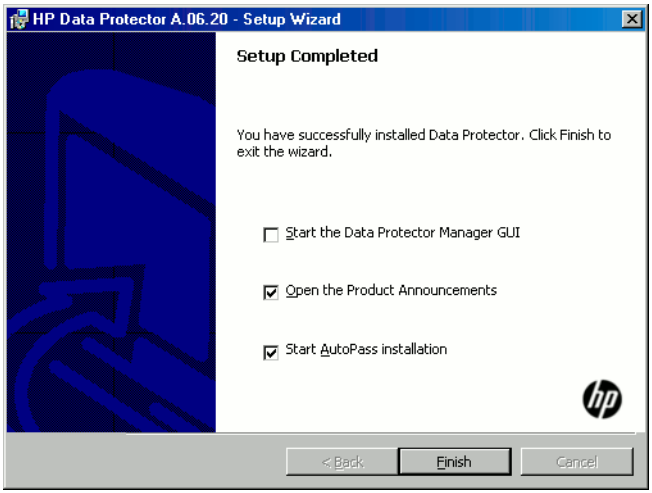


図 10 AutoPassをインストール対象として選択する場合

    [Finish]をクリックします。

インストール後の状態

*Windows Server 2008:*セットアップが完了するとすぐに、Cell Managerプログラムとデータファイルは`Data_Protector_home`および`Data_Protector_program_data`のディレクトリ

にそれぞれ配置されますが、ソフトウェアデポはData_Protector_program_data¥Depotディレクトリに配置されます。

他のWindowsシステムの場合: セットアップが完了するとすぐに、Cell ManagerファイルはData_Protector_homeディレクトリに配置され、ソフトウェアデポはData_Protector_home¥Depotディレクトリに配置されます。

Installが完了すると、以下のプロセスがCell Managerシステム上で動作するようになります。

crs.exe	Data Protector Cell Request Server (CRS)サービス Cell Managerシステム上で実行され、Cell Managerソフトウェアがシステムにインストールされると起動されます。CRSは、セル内のバックアップセッションおよび復元セッションの開始および制御に使用されます。Data_Protector_home¥binディレクトリで実行されます。
rds.exe	Data Protector Raima Database Server (RDS)サービス Cell Managerシステム上で実行され、Cell Managerソフトウェアがシステムにインストールされると起動されます。RDSは、IDBの管理に使用されます。Data_Protector_home¥binディレクトリで実行されます。
mmd.exe	Data Protector Media Management Daemon (MMD)サービス Cell Managerシステム上で実行され、Cell Managerソフトウェアがシステムにインストールされると起動されます。MMDは、デバイスおよびメディアの管理操作に使用されます。Data_Protector_home¥binディレクトリで実行されます。
OmniInet.exe	Cell Managerが他のシステムでエージェントを起動できるようにするData Protectorクライアントサービス Data Protector Inetサービス は、Data Protectorセルのすべてのシステムで実行する必要があります。Data_Protector_home¥binディレクトリで実行されます。
kms.exe	Data Protector Key Management Server (KMS)サービス Cell Managerシステム上で実行され、Cell Managerソフトウェアがシステムにインストールされると起動されます。KMSは、Data Protector暗号化機

	能のキーを管理します。Data_Protector_home¥binディレクトリで実行されます。
uiproxy.exe	Data Protector Java GUIサーバー（UIProxyサービス）Data_Protector_home¥java¥server¥binディレクトリのCell Managerシステム上で実行されます。UIProxyサービスは、Java GUIクライアントとCell Manager間の通信を行います。

注記：

複数プラットフォームにわたるバックアップや復元をData Protectorユーザーインタフェースを使用して実行するよう計画している場合は、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照して制限事項を確認してください。

ヒント：

Data Protector GUIで適切なエンコーディングが使用できない場合は、ファイル名を正しく表示するために、コードページ変換テーブルを追加でインストールすることが可能です。手順の詳細は、オペレーティングシステムのマニュアルを参照してください。

トラブルシューティング

セットアップを正常に完了できない場合は、セットアップ自体がチェックする前提条件を検証し、その条件が満たされていなかった場合にエラーの原因となる項目を調べてください。前提条件（55ページ）を参照してください。

セットアップがチェックする前提条件を以下に示します。

- サービスパックのバージョン
- NSLookupを実行して、Data Protectorがホスト名を解決できることが確認されていること。
- ディスク容量
- 管理者権限

この次に行う作業

この段階で、Cell Managerがインストールされます。また、選択した場合はWindows用のインストールサーバーもインストールされます。準備が整ったら、以下の作業を実施します。

1. オペレーティングシステムが混在するバックアップ環境の場合は、UNIX用のインストールサーバーをインストールします。詳細については、「インストールサーバーのインストール」(63ページ)を参照してください。なお、UNIX用のインストールサーバーが不要な場合は、この作業は省略できます。
2. ソフトウェアをクライアントに配布します。詳細については、「Data Protectorクライアントのインストール」(72ページ)を参照してください。

インストールサーバーのインストール

インストールサーバーは、Cell Managerシステム上にインストールすることも、LANを介してCell Managerと接続されているサポート対象システム上にインストールすることも可能です。インストールサーバーで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、http://www.hp.com/support/manualsを参照してください。

Cell Managerとは別のシステム上にインストールサーバーを配置する場合は、該当するソフトウェアデポをローカルにインストールしてください。この項では、手順の詳細を説明します。

UNIX用のインストールサーバーのインストール

前提条件

インストールサーバーシステムとして使用するシステムは、以下の条件を満たしている必要があります。

- HP-UX、Solaris、Linuxのいずれかのオペレーティングシステムがインストールされていること。インストールサーバーで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、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- inetdまたはxinetdデーモンが稼働していること。
- ポート番号5555 (デフォルト)が利用可能であること。このポート番号がすでに使用されている場合は、「Data Protectorのデフォルトのポート番号の変更」(388ページ)を参照してください。
- TCP/IPプロトコルがインストールされており、実行されていること。このプロトコルを使って、ホスト名を解決できること。
- 完全なData Protectorソフトウェアデポを作成するのに十分な空きディスクスペースがあること。詳細は『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- DVD-ROMドライブがあること。
- Data Protectorセル内のCell Managerは、バージョン6.20であること。

重要:

Data Protectorをリンクディレクトリにインストールするには、たとえば次のような手順を実行します。

```
/opt/omni/ -> /prefix/opt/omni/
/etc/opt/omni/ -> /prefix/etc/opt/omni/
/var/opt/omni/ -> /prefix/var/opt/omni/
```

Install前にリンクを作成しておき、インストール先ディレクトリが存在することを確認します。

注記:

ネットワーク上のデバイスからソフトウェアをインストールする場合は、まず、インストール対象のコンピュータにソースディレクトリをマウントします。

インストール手順

UNIX用のインストールサーバーをHP-UXシステム、Solarisシステム、またはLinuxシステムにインストールするには、以下の手順に従ってください。

1. HP-UX用またはSolarisおよびLinux用のインストールDVD-ROMをドライブに挿入し、マウントポイントにマウントします。

   たとえば、次のように入力します。

   ```
   mkdir /dvdrom
   mount /dev/dsk/c0t0d0 /dvdrom
   ```

   必要であれば、Data Protectorをディスク上のデポからインストールすることもできます。その場合は、以下の手順に従ってください。

   - Installファイルが格納されているディレクトリをローカルディスクにコピーする場合は、以下のコマンドを実行します。

     ```
     mkdir directory
     cp -r /dvdrom/platform_dir/DP_DEPOT directory
     cp -r /dvdrom/LOCAL_INSTALL directory
     ```

     ここで、*platform_dir*には、以下のいずれかの値を指定します。

hpux	HP-UXシステム
linux_x86_64	AMD64/Intel EM64T上のLinuxシステム
solaris	Solarisシステム

   - DVD-ROM全体をローカルディスクにコピーするには、以下のコマンドを実行します。

     cp -r /dvdrom *dvd_image_dir*

2. omnisetup.shコマンドを実行します。

   このコマンドをDVD-ROMから実行するには、以下のコマンドを実行します。

   ```
   cd /dvdrom/LOCAL_INSTALL
   ./omnisetup.sh -IS
   ```

   ディスクからインストールを開始するには、以下の手順に従ってください。

   - Installディレクトリをローカルディスクの*directory*にコピーした場合は、以下のコマンドを実行します。

     ```
     cd directory/LOCAL_INSTALL
     ./omnisetup.sh -IS
     ```

   - DVD-ROM全体を*dvd_image_dir*にコピーした場合は、-CMパラメータを指定してomnisetup.shコマンドを実行します。

     ```
     cd dvd_image_dir/LOCAL_INSTALL
     ./omnisetup.sh -IS
     ```

   omnisetup.shコマンドの説明については、DVD-ROMのMount_point/ディレクトリにあるREADMEファイルか、DVD-ROMのMount_point/DOCS/C/MANディレクトリにある『*HP Data Protector Command Line Interface Reference*』を参照してください。

Installが終了すると、UNIX用のソフトウェアデポは、/opt/omni/databases/vendorディレクトリにインストールされます。

omnisetup.shコマンドを実行すると、インストールサーバーのすべてのパッケージがインストールされます。パッケージの一部のみをインストールする場合は、swinstallコマンド(HP-UXの場合)、pkgaddコマンド(Solarisの場合)、またはrpmコマンド(Linuxの場合)を使用する必要があります。詳細については、「ネイティブツールを使用した、HP-UX、Solaris、およびLinuxシステムへのインストール」(361ページ)を参照してください。

重要:

ネットワーク上にUNIX用のインストールサーバーをインストールしない場合は、HP-UX用またはSolarisおよびLinux用のインストールDVD-ROMを使用して、すべてのUNIXクライアントをローカルにインストールする必要があります。

注記：

ユーザーインタフェースコンポーネント(グラフィカルユーザーインタフェースまたはコマンドラインインタフェース)を使用する場合は、事前に環境変数を更新してください。詳細は、「環境変数の設定」(53ページ)を参照してください。

複数プラットフォームにわたるバックアップや復元をData Protectorユーザーインタフェースを使用して実行するよう計画している場合は、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照して制限事項を確認してください。

この次に行う作業

この時点で、UNIX用のインストールサーバーがネットワーク上にすでにインストールされていなければなりません。準備が整ったら、以下の作業を実施します。

1. インストールサーバーをCell Managerとは別のシステムにインストールした場合は、そのシステムをData Protectorセルに追加(インポート)する必要があります。詳細については、「セルへのインストールサーバーのインポート」(216ページ)を参照してください。

   注記：

   インストールサーバーをインポートすると、Cell Manager上の`/etc/opt/omni/server/cell/installation_servers`が更新されて、インストールしたリモートインストールパケットが更新されます。CLIからこのファイルを使用して、使用可能なリモートインストールパケットを確認できます。このファイルを最新状態に保つために、リモートインストールパケットをインストールまたは削除したときは、インストールサーバーのエクスポートと再インポートを必ず実行してください。これは、インストールサーバーをCell Managerと同じシステムにインストールしてある場合も同様です。

2. Data ProtectorセルにWindowsシステムがある場合は、Windows用のインストールサーバーをインストールします。詳細については、「Windows用のインストールサーバーのインストール」(68ページ)を参照してください。
3. ソフトウェアをクライアントに配布します。詳細については、「Data Protectorクライアントのインストール」(72ページ)を参照してください。

Windows用のインストールサーバーのインストール

前提条件

インストールサーバーシステムとして使用するWindowsシステムは、以下の条件を満たしている必要があります。

- サポート対象のWindowsオペレーティングシステムがインストールされていること。インストールサーバーで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、http://www.hp.com/support/manualsを参照してください。
- Microsoft Internet Explorer 5.0以上がインストールされていること。
- 完全なData Protectorソフトウェアデポを作成するのに十分な空きディスクスペースがあること。詳細については、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- DVD-ROMドライブにアクセスできること。
- Microsoft社のTCP/IPプロトコルがインストールされており、実行されていること。このプロトコルを使って、ホスト名を解決できること。コンピュータの名前とホスト名は同じでなければなりません。

制限事項

Windowsオペレーティングシステムのセキュリティ規制により、インストールサーバーを使用してクライアントをリモートにインストールできるのは、同一ドメイン内に限られます。

推奨事項

Data Protector 6.20のインストールを開始するにあたって、Microsoft Installer (MSI) 2.0がインストールされていることを確認してください。MSIのバージョンが古い場合は、Data Protectorセットアッププログラムにより、自動的にバージョン2.0にアップグレードされます。この場合、Data Protectorによって、アップグレードの最後の段階でMSIがアップグレードされたことが通知されます。MSIがアップグレードされた場合は、システムを再起動することを強く推奨します。個々のWindowsオペレーティングシステムに対するMSI 2.0の前提条件については、Microsoft Supportにお問い合わせください。

Data Protector 6.20をインストールする前に、MSIをバージョン2.0にアップグレードすることをお勧めします。

重要：

ネットワーク上にWindows用のインストールサーバーをインストールしない場合は、DVD-ROMを使用して、すべてのWindowsクライアントをローカルにインストールしなければなりません。

注記：

インストールサーバーをすでにインストールしてあるWindowsシステムには、Data Protectorクライアントをリモートでインストールすることはできません。同一システム上にインストールサーバーとクライアントコンポーネントをインストールする場合は、クライアントをローカルにインストールする必要があります。この場合はインストール手順の中で、必要なクライアントコンポーネントとインストールサーバーコンポーネントをすべて選択してください。詳細については、「Windows用クライアントのインストール」（92ページ）を参照してください。

インストール手順

Windows用のインストールサーバーをインストールするには、以下の手順に従ってください。

1. WindowsインストールDVD-ROM

   Windows Server 2008の場合は、[ユーザーアカウント制御]ダイアログボックスが表示されます。[**続行**]をクリックしてインストールを続けます。

2. HP Data Protectorウィンドウで[**インストールData Protector**]を選択し、Data Protectorのセットアップ用ウィザードを開始します。

3. セットアップ用ウィザードの指示に従って操作を行い、ライセンス契約を十分にお読みください。記載内容に同意する場合は、[**Next**]をクリックして次に進みます。

4. [Installation Type]ページで、[**インストールサーバー**]を選択します。[Next]をクリックすると、選択したData Protectorソフトウェアデポがインストールされます。

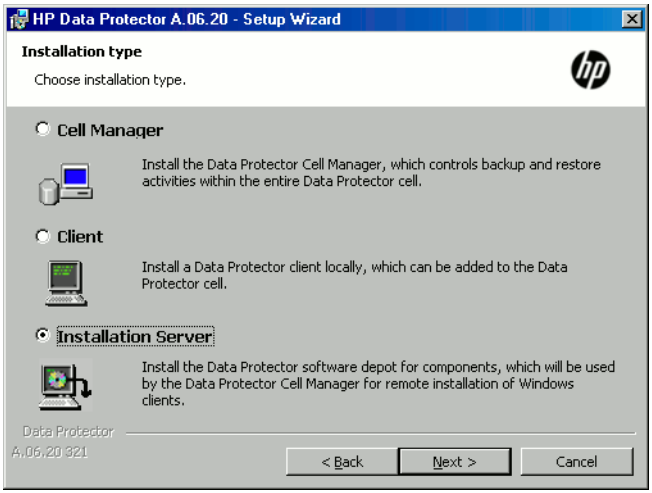


図 11 インストールの種類の選択

5. Data Protectorをデフォルトフォルダにインストールする場合には、[Next]をクリックします。

   それ以外の場合は、[Change]をクリックして[Change Current Destination Folder]ウィンドウを開き、別のパスを入力します。

6. *Data Protectorによってシステムに*Windows*ファイアウォールが検出されると*、[Windows Firewall configuration]ページが表示されます。Data Protectorのセットアッププログラムによって、必要なすべてのData Protector実行可能ファイルが登録されます。デフォルトでは、[**Initially, enable newly registered Data Protector binaries to open ports as needed**]オプションが選択されています。この時点で、Data Protectorによってポートがオープンされないようにするには、オプションを選択解除します。ただし、Data Protectorを適切に機能させるには、実行可能ファイルを有効にする必要があります。

   [Next]をクリックします。

7. コンポーネントのサマリーリストが表示されます。[Install]をクリックして、選択したコンポーネントのインストールを開始します。この処理には、数分かかる場合があります。

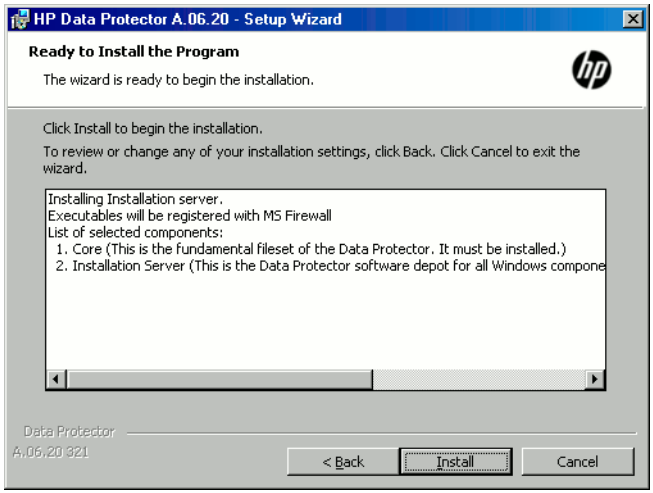


図 12 コンポーネント選択サマリーページ

8. Installステータスのページが表示されます。[Next]をクリックします。

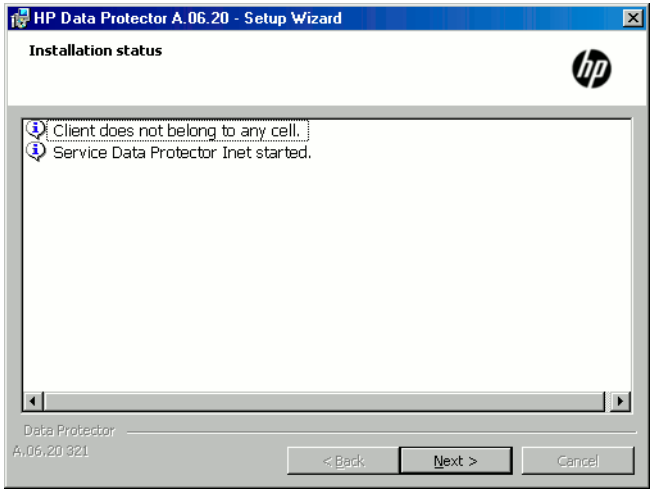


図 13 [Installation Status]ページ

9. 『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を表示するには、[Open the Product Announcements]を選択します。

   [Finish]をクリックします。

Installが終了すると、ソフトウェアはデフォルトでData_Protector_program_data¥Depotディレクトリ(Windows Server 2008の場合)、またはData_Protector_home¥Depotディレクトリ(その他のWindowsシステム)にインストールされます。ソフトウェアは共有されるため、ネットワークからアクセスできます。

この次に行う作業

この時点で、Windows用のインストールサーバーがネットワーク上にインストールされていなければなりません。準備が整ったら、以下の作業を実施します。

1. 独立した形で(たとえば、Cell Managerとは別のシステムに)インストールサーバーをセットアップした場合は、このシステムをData Protectorセルに手作業で追加(インポート)する必要があります。詳細については、「セルへのインストールサーバーのインポート」(216ページ)を参照してください。
2. オペレーティングシステムが混在するバックアップ環境の場合は、HP-UXシステム、Solarisシステム、またはLinuxシステム上に、UNIX用のインストールサーバーをインストールします。詳細については、「UNIX用のインストールサーバーのインストール」(63ページ)を参照してください。
3. ソフトウェアをクライアントに配布します。詳細については、「Data Protectorクライアントのインストール」(72ページ)を参照してください。

Data Protectorクライアントのインストール

Data Protectorクライアントは、インストールサーバーを使って配布することによりリモートでインストールでき、また、該当するインストールDVD-ROMからローカルにインストールすることもできます。

Data ProtectorインストールDVD-ROMのリストについては、「Data ProtectorのインストールDVD-ROM」(36ページ)を参照してください。

Data Protectorクライアントをインストールして Data Protectorセル内にインポートした後には、インストール結果を確認し、不正アクセスからクライアントを保護することを強くお勧めします。クライアントのインストール結果を確認する手順は、「Data Protectorクライアントのインストール結果の確認」(352ページ)を参照してください。セキュリティ保護の詳細は、「保護について」(223ページ)を参照してください。

「Data Protectorクライアントのインストール」(72ページ)は、Data Protectorクライアントシステムの一覧と詳細説明の参照先を示したものです。

表 4 Data Protectorクライアントシステムのインストール

クライアントシステム	インストールの種類とリファレンス
Windows	リモートおよびローカルインストール。「Windows用クライアントのインストール」(92ページ)を参照してください。
HP-UX	リモートおよびローカルインストール。「HP-UXクライアントのインストール」(99ページ)を参照してください。
Solaris	リモートおよびローカルインストール。「Solaris用クライアントのインストール」(102ページ)を参照してください。
Linux	リモートおよびローカルインストール。「Linuxクライアントのインストール」(109ページ)を参照してください。
ESX Server	リモートおよびローカルインストール。「ESX Serverクライアントのインストール」(114ページ)を参照してください。
Mac OS X	リモートおよびローカルインストール。「Mac OS Xクライアントのインストール」(114ページ)を参照してください。
AIX	リモートおよびローカルインストール。「AIXクライアントのインストール」(115ページ)を参照してください。
Tru64	リモートおよびローカルインストール。「Tru64クライアントのインストール」(117ページ)を参照してください。
SCO	リモートおよびローカルインストール。「SCOクライアントのインストール」(119ページ)を参照してください。
DASクライアント	リモートおよびローカルインストール。「ADIC/GRAUライブラリ用またはStorageTekライブラリ用のMedia Agentのインストール」(122ページ)を参照してください。
ACSクライアント	リモートおよびローカルインストール。「ADIC/GRAUライブラリ用またはStorageTekライブラリ用のMedia Agentのインストール」(122ページ)を参照してください。
Novell NetWare	ローカルインストール。「Novell NetWareクライアントのローカルインストール」(131ページ)を参照してください。

クライアントシステム	インストールの種類とリファレンス
HP OpenVMS	ローカルインストール。「HP OpenVMSクライアントのローカルインストール」(139ページ)を参照してください。
その他のUNIXクライアント	ローカルインストール。「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)を参照してください。

統合

Data Protector統合ソフトウェアは、Data Protectorを使用してデータベースアプリケーションのバックアップを可能にするソフトウェアコンポーネントです。MS Exchange Serverデータベースのバックアップには MS Exchange Integrationコンポーネントを使用し、Oracleデータベースのバックアップには Oracle Integrationコンポーネントを使用するというように、適切な統合ソフトウェアを選択すれば、データベースアプリケーションを実行するシステムをWindowsクライアントシステムおよびUNIXクライアントシステムと同じ方法でインストールできます。詳細は本章の表5(74ページ)を参照してください。

表 5 統合ソフトウェアソフトウェアのインストール

ソフトウェアアプリケーションまたはディスクアレイファミリ	リファレンス
Microsoft Exchange Server	「Microsoft Exchange Serverクライアント」(155ページ)を参照してください。
Microsoft SQL Server	「Microsoft SQL Serverクライアント」(157ページ)を参照してください。
Microsoft SharePoint Server	「Microsoft SharePoint Serverクライアント」(157ページ)を参照してください。
Microsoft Hyper-V	「Microsoft Hyper-Vクライアント」(164ページ)を参照してください。
Sybase Server	「Sybaseクライアント」(159ページ)を参照してください。
Informix Server	「Informix Serverクライアント」(159ページ)を参照してください。
SAP R/3	「SAP R/3クライアント」(ページ)を参照してください。
SAP MaxDB	「SAP MaxDBクライアント」(161ページ)を参照してください。

ソフトウェアアプリケーションまたはディスクアレイファミリ	リファレンス
Oracle Server	「Oracle Serverクライアント」(161ページ)を参照してください。
VMware	「VMwareクライアント」(162ページ)を参照してください。
IBM DB2 UDB	「DB2クライアント」(165ページ)を参照してください。
HP Network Node Manager (NNM)	「NNMクライアント」(165ページ)を参照してください。
Network Data Management Protocol (NDMP) Server	「NDMP Serverクライアント」(165ページ)を参照してください。
Microsoftボリュームシャドウコピーサービス(VSS)	「Microsoftボリュームシャドウコピーサービスクライアント」(166ページ)を参照してください。
Lotus Notes/Domino Server	「Lotus Notes/Domino Serverクライアント」(166ページ)を参照してください。
EMC Symmetrix	「EMC Symmetrix用統合ソフトウェア」(181ページ)を参照してください。
HP StorageWorks P9000 XPディスクアレイファミリ	「HP StorageWorks P9000 XPディスクアレイファミリ用統合ソフトウェア」(174ページ)を参照してください。
HP StorageWorks P6000 EVAディスクアレイファミリ	「HP StorageWorks P6000 EVAディスクアレイファミリ用統合ソフトウェア」(167ページ)を参照してください。

表 6 他のインストール

設置	リファレンス
仮想ライブラリシステム(VLS)自動移行	(「VLS自動移行クライアント」(186ページ)を参照)。

設置	リファレンス
各国語版ユーザーインタフェース	「各国語版Data Protectorユーザーインタフェースのインストール」(187ページ)を参照してください。
Webレポート	「Data Protector Web Reportingのインストール」(192ページ)を参照してください。
MC/ServiceGuard	「MC/ServiceGuardへのData Protectorのインストール」(193ページ)を参照してください。
Microsoft Cluster Server	「Microsoft Cluster ServerへのData Protectorのインストール」(195ページ)を参照してください。
Veritas Cluster Server	「Veritas ClusterへのData Protectorクライアントのインストール」(207ページ)を参照してください。
Novell NetWare Cluster	「Novell NetWare ClusterへのData Protectorクライアントのインストール」(208ページ)を参照してください。
IBM HACMP Cluster	詳細は、「Data ProtectorのIBM HACMP Clusterへのインストール」(210ページ)を参照してください。

Data Protectorコンポーネント

サポートされるプラットフォームの最新情報については、http://www.hp.com/support/manualsのHP Data Protectorホームページを参照してください。

選択可能なData Protectorコンポーネントとその説明を以下に示します。

ユーザーインタフェース

ユーザーインタフェースコンポーネントには、Data Protectorのグラフィカルユーザーインタフェース(Windowsシステム)とコマンドラインインタフェースの一部(WindowsシステムおよびUnixシステム)が含まれます。Data Protector Cell Managerにアクセスするには、このコンポーネントが必要です。セルの管理用システムには、このコンポーネントを必ずインストールする必要があります。

注記：

Data Protectorコマンドラインインタフェースの特定のコマンドは、他のData Protectorコンポーネントに含まれています。詳細は、『*HP Data Protector Command Line Interface Reference*』を参照してください。

異種混合環境でData Protectorのユーザーインタフェースを使用する前に、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照して制限事項を確認してください。

Java GUIクライアント	Data Protector Java GUI クライアントサーバーアーキテクチャを持つJavaベースのグラフィカルユーザーインタフェースです。これには、Cell Managerのグラフィカルユーザーインタフェースおよび Manager-of-Managers(MoM)のグラフィカルユーザーインタフェースが含まれます。デフォルトでは、Java GUIクライアントはインストールするよう選択されていません。Java GUIクライアントは手動で選択する必要があります。Java GUIがインストールされているクライアントにコマンドラインインタフェースをインストールするには、システムにユーザーインタフェースまたは他の適切なData Protectorコンポーネントもインストールしてください。
英語版マニュアル(ガイド、ヘルプ)	これは、Data Protectorの英語のマニュアルおよびオンラインヘルプ(OLH)ファイルセットです。
フランス語版マニュアル(ガイド、ヘルプ)	これは、Data Protectorのフランス語のマニュアルおよびオンラインヘルプ(OLH)ファイルセットです。
日本語版マニュアル(ガイド、ヘルプ)	これは、Data Protectorの日本語のマニュアルおよびオンラインヘルプ(OLH)ファイルセットです。
簡体字中国語版マニュアル(ガイド、ヘルプ)	これは、Data Protectorの簡体字中国語のマニュアルおよびオンラインヘルプ(OLH)ファイルセットです。

Manager-of-Managersユーザーインタフェース	Manager-of-Managersユーザーインタフェースには、Data Protectorのグラフィカルユーザーインタフェースが含まれます。Data ProtectorのManager-of-Managers機能にアクセスしてマルチセル環境を管理するには、このコンポーネントが必要です。Manager-of-Managersユーザーインタフェースと Managerユーザーインタフェースは、共通アプリケーションとして使用できます。
Disk Agent	Disk Agentコンポーネントは、Data Protectorによるバックアップの対象となるディスクを持つシステムにインストールする必要があります。
General Media Agent	General Media Agentは、Data Protectorで管理するバックアップデバイスに接続されているシステムか、Data Protectorで管理するライブラリロボティクスにアクセス可能なシステムにインストールする必要があります。
VLS自動移行	VLS自動移行コンポーネントは、Data Protectorを使用してVirtual Library System (VLS)のスマートメディアをコピーするクライアントにインストールする必要があります。
自動ディザスタリカバリモジュール	自動ディザスタリカバリコンポーネントは、自動ディザスタリカバリ方法を使用した復旧を可能にするシステムと、拡張ディザスタリカバリのDR CD ISOイメージを作成してディザスタリカバリを自動的に準備するシステムにインストールする必要があります。
SAP R/3用統合ソフトウェア	SAP R/3用統合コンポーネントは、Data Protectorによるバックアップの対象となるSAP R/3データベースがあるシステムにインストールする必要があります。
SAP DB用統合ソフトウェア	SAP DB用統合ソフトウェアコンポーネントは、Data Protectorによるバックアップの対象となるSAP MaxDBデータベースがあるシステムにインストールする必要があります。
Oracle用統合ソフトウェア	Oracle用統合ソフトウェアコンポーネントは、Data Protectorによるバックアップの対象となるOracleデー

タベースがあるシステムにインストールする必要があります。

VMware用統合ソフトウェア(レガシー)	VMware用統合ソフトウェア(レガシー)コンポーネントは、VirtualCenterシステム(存在する場合)、およびData Protectorでバックアップを行うすべてのESX Serverシステムにインストールする必要があります。また、VCBfileまたはVCBimageのバックアップ方法を採用する場合は、統合ソフトウェアコンポーネントをバックアッププロキシーシステムにもインストールする必要があります。
仮想環境統合ソフトウェア	仮想環境統合ソフトウェアのコンポーネントは、Data Protectorの仮想環境統合ソフトウェアを使って仮想マシンのバックアップおよび復元を制御する際にバックアップホストとして使用するシステムにインストールする必要があります。Microsoft Hyper-Vシステムをバックアップおよび復元する場合は、この統合ソフトウェアコンポーネントを、MSボリュームシャドウコピー用統合ソフトウェアコンポーネントとともに、バックアップ対象となるすべてのMicrosoft Hyper-Vシステムにもインストールする必要があります。
DB2用統合ソフトウェア	DB2用統合ソフトウェアコンポーネントは、Data Protectorによるバックアップの対象となるDB2 Serverがあるシステムすべてにインストールする必要があります。
Sybase用統合ソフトウェア	Sybase用統合ソフトウェアコンポーネントは、Data Protectorによるバックアップの対象となるSybaseデータベースがあるシステムにインストールする必要があります。
Informix用統合ソフトウェア	Informix用統合ソフトウェアコンポーネントは、Data Protectorによるバックアップの対象となるInformix Serverデータベースがあるシステムにインストールする必要があります。
MS Exchange用統合ソフトウェア	MS Exchange Server用統合ソフトウェアコンポーネントは、Data Protector Microsoft Exchange Server 2003/2007用統合ソフトウェアまたはData Protector Microsoft Exchange Single Mailbox用統合ソフトウェ

	アを使用してバックアップを行うMicrosoft Exchange Server 2003/2007システムにインストールする必要があります。 また、Data Protector Microsoft Exchange Single Mailbox用統合ソフトウェアを使用してバックアップを行うMicrosoft Exchange Server 2010システムにもインストールする必要があります。
MS Exchange Server 2010統合ソフトウェア	MS Exchange Server用統合ソフトウェアコンポーネントは、Data Protector Microsoft Exchange Server 2010用統合ソフトウェアを使用してバックアップを行うMicrosoft Exchange Server 2010システムにインストールする必要があります。
MS SQL用統合ソフトウェア	SQL用統合ソフトウェアコンポーネントは、Data Protectorによるバックアップの対象となるMicrosoft SQL Serverデータベースがあるシステムにインストールする必要があります。
MS SharePoint Portal Server用統合ソフトウェア	MS SharePoint Portal Server用統合ソフトウェアコンポーネントは、Data Protectorによるバックアップの対象となるMicrosoft SharePoint Portal Serverシステムにインストールする必要があります。
MS SharePoint Server 2007/2010用統合ソフトウェア	MS SharePoint 2007/2010用統合ソフトウェアコンポーネントは、Data Protectorによるバックアップの対象となるMicrosoft SharePoint Server 2007/2010システムにインストールする必要があります。
MS ボリュームシャドウコピー用統合ソフトウェア	MSボリュームシャドウコピー用統合ソフトウェアコンポーネントは、ボリュームシャドウコピーサービスによるバックアップを実行するWindows Server 2003システムにインストールする必要があります。
HP StorageWorks P6000 EVA SMI-S Agent	HP StorageWorks P6000 EVA SMI-S Agentコンポーネントは、HP StorageWorks P6000 EVAディスクアレイファミリをData Protectorと統合する場合に、アプリケーションシステムとバックアップシステムにインストールする必要があります。

HP StorageWorks P9000 XP Agent	HP StorageWorks P9000 XP Agentコンポーネントは、HP StorageWorks P9000 XPディスクアレイファミリをData Protectorと統合する場合に、アプリケーションシステムとバックアップシステムにインストールする必要があります。
HP StorageWorks P4000 Agent	HP StorageWorks P4000 Agentコンポーネントは、HP StorageWorks P4000 SANソリューションをData Protectorと統合する場合に、アプリケーションシステムとバックアップシステムにインストールする必要があります。
EMC Symmetrix Agent	EMC Symmetrix Agentコンポーネントは、EMC SymmetrixをData Protectorと統合する場合に、アプリケーションシステムとバックアップシステムにインストールする必要があります。
HP Network Node Manager用統合ソフトウェア	NNM用統合ソフトウェアコンポーネントは、セル内でData Protectorによるバックアップの対象となるNNMデータベースがあるすべてのシステムにインストールする必要があります。
NDMP Media Agent	NDMP Media Agentコンポーネントは、NDMPサーバーを介してNDMP専用ドライブにデータをバックアップしているすべてのシステムにインストールする必要があります。
Lotus用統合ソフトウェア	Lotus用統合ソフトウェアコンポーネントは、セル内でData Protectorによるバックアップを実行するLotus Notes/Domino Serverデータベースがあるすべてのシステムにインストールする必要があります。
MS SharePoint Granular Recovery Extension	Microsoft SharePoint Server向けData Protector Granular Recovery Extensionは、Microsoft SharePoint Serverサーバーの全体管理システムにインストールする必要があります。
VMware Granular Recovery Extension Web Plug-In	VMware仮想マシンを細かな単位で復旧するには、Data Protector VMware Granular Recovery Extension Web Plug-InコンポーネントをVMware Virtual Serverシステムにインストールする必要があ

	ります。リモートインストールのみがサポートされています。
VMware Granular Recovery Extension Agent	VMware仮想マシンの復元と、細かな単位での復旧を行うには、Data Protector VMware Granular Recovery Extension Agentコンポーネントをマウントプロキシシステムにインストールする必要があります。リモートインストールのみがサポートされています。

注記:

General Media AgentとNDMP Media Agentを同じシステムにインストールすることはできません。

Data Protectorクライアントのリモートインストール

この項では、インストールサーバーを使ってData Protectorソフトウェアをクライアントに配布する手順(リモートインストールまたはアップグレード手順)を説明します。

Data Protectorユーザーインタフェースを使って、ソフトウェアコンポーネントをクライアントに配布します。プラットフォームが異なるクライアントへのインストールも可能です。

前提条件

- Installの前提条件および推奨事項については、対象となるクライアントシステムに応じたインストール手順の説明をお読みください。説明は、表4(73ページ)および表5(74ページ)に示すとおりです。
- サポートされるプラットフォーム、Data Protectorコンポーネント、およびディスクスペース要件については、http://www.hp.com/support/manualsおよび『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- この手順を開始する前に、Cell Managerおよびインストールサーバーをネットワークにインストールしておく必要があります。
- Windows用のインストールサーバーは、ネットワーク上の他のコンピュータからアクセスできるように、共有ディレクトリに格納する必要があります。

推奨事項

- ***UNIXシステムの場合:*** セキュリティ上の理由から、Data Protectorリモートインストールにはセキュアシェルを使用することをお勧めします。セキュアシェルを使用できない

場合は、従来のUNIXツールであるrshおよびrexecがData Protectorのリモートインストールで自動的に使用されます。

セキュアシェルを使用するには、クライアントおよびインストールサーバーの両方にOpenSSHをインストールしてセットアップします。秘密キーが暗号化されている場合は、インストールサーバー上にkeychainをインストールしてセットアップします。(「セキュアシェルを使用したリモートインストール」(83ページ)を参照)。

注記:

別のData Protectorセル内のクライアントにソフトウェアを配布することはできません。ただし独立したインストールサーバーがある場合は、それを複数のセルにインポートすることも可能です。こうすることで、各セルのCell Managerに接続されたGUIを順番に使用することにより、それぞれのセル内にソフトウェアを配布できます。

セキュアシェルを使用したリモートインストール

セキュアシェルインストールでは、安全な方法でData Protectorコンポーネントがインストールされるため、クライアントとインストールサーバーのセキュリティ保護に役立ちます。以下の処理により、高度な保護が実現されます。

- 公開-秘密キーペアメカニズムによって保護された方法で、クライアントにアクセスするインストールサーバーのユーザーを認証します。
- Installパッケージを暗号化してからネットワーク上で転送します。

注記:

セキュアシェルインストールは、UNIXシステムでのみサポートされています。

OpenSSHのセットアップ

クライアントおよびインストールサーバーの両方にOpenSSHをインストールしてセットアップします。

1. OpenSSHがシステムにインストールされていることを確認します。詳細は、お使いのオペレーティングシステムまたはディストリビューションのマニュアルを参照してください。

   OpenSSHパッケージがお使いのOSディストリビューションに含まれていない場合は、OpenSSHをhttp://www.openssh.orgからダウンロードして、Data Protectorクライアントとインストールサーバーの両方にインストールします。

   HP-UXでは、代わりにHP-UX Secure Shellを使用できます。

注記:

セキュアシェルインストールのデフォルトの場所は/opt/ssh**です。**

2. インストールサーバー上で、ssh-keygenを実行して公開キーペアを生成します。公開キーはクライアントに転送しますが、秘密キーはインストールサーバー上に維持します。暗号化された(パスフレーズで保護された)秘密キーを使用する場合は、インストールサーバー上にkeychainをセットアップする必要がある点に注意してください。詳細はkeychainのセットアップ(86ページ)を参照してください。

   ssh-keygenの詳細については、http://www.openbsd.org/cgi-bin/man.cgi?query=ssh-keygen&sektion=1を参照してください。

3. クライアント上では、$HOME/.sshディレクトリにauthorized_keysという名前で公開キーを保存します。

注記:

通常、$HOME/.sshは、rootユーザーのホームディレクトリです。

SSHプロトコルのバージョン(SSH1またはSSH2)を設定するには、以下のファイルを開いて、protocolパラメータの設定を変更します。

1. ***インストールサーバーの場合:***

   ssh_install_directory/ssh/etc/ssh_config

   このファイルは、sshコマンドにより使用されます。

2. ***クライアントの場合:***

   ssh_install_directory/ssh/etc/sshd_config

   このコマンドはsshデーモン(sshd)によって使用されます。

なお、上記の2つのファイルは同期させる必要があります。

注記:

SSHプロトコルのデフォルトバージョンは、SSH2です。

4. クライアント上で、以下のコマンドを実行してsshデーモンを起動します。

   ssh_install_directory/ssh/sbin/sshd

5. 次のコマンドを実行して、インストールサーバー上の$HOME/.ssh/known_hostsにある既知のホストのリストにクライアントを追加します。

   ssh root@client_host

   なお、client_hostは、次の例のような完全修飾DNS名でなければなりません。

   ssh root@client1.company.com

6. インストールサーバー上で、omnirc変数OB2_SSH_ENABLEDを1に設定します。omnirc変数の詳細は、『*HP Data Protectorトラブルシューティングガイド*』を参照してください。

keychainのセットアップ

keychainは、パスフレーズを手動で入力しなくても秘密キーを復号化できるようにするツールです。このツールは、秘密キーが暗号化されている場合にのみ必要です。keychainをセットアップするには以下の手順に従ってください。

1. http://www.gentoo.org/proj/en/keychain/index.htmlからインストールサーバーにkeychainをダウンロードします。
2. $HOME/.profileファイルに以下の2行を追加します。

   HP-UX、Solarisの場合:

   keychain_install_directory/keychain-keychain_version/keychain $HOME/.ssh/private_key

   . $HOME/.keychain/'hostname'-sh

   Linuxの場合:

   /usr/bin/keychain $HOME/.ssh/private_key

   . $HOME/.keychain/'hostname'-sh
3. インストールサーバー上で、omnirc変数OB2_ENCRYPT_PVT_KEYを1に設定します。omnirc変数の詳細は、『*HP Data Protectorトラブルシューティングガイド*』を参照してください。

この次に行う作業

OpenSSHとkeychainのセットアップが終了したら、GUIを使用するか(クライアントのセルへの追加(87ページ)の手順を参照)、CLIからob2installコマンドを実行することにより、クライアントをセルに追加します。CLIコマンドとそのパラメータについては、『*HP Data Protector Command Line Interface Reference*』を参照してください。

注記:

コマンドの実行に失敗するためセキュアシェルインストールを実行できない場合は、警告メッセージが表示されます。ただし、Data Protectorの標準リモートインストール方法によりインストールは続行されます。

クライアントのセルへの追加

クライアントのセルへの追加

Data Protectorセルにまだ含まれていないクライアントに Data Protectorソフトウェアを配布するには、以下の手順に従ってください。

1. Data Protector GUIの起動:
   - オリジナルのData Protector GUI (Windowsの場合のみ):
     - **[スタート]** > **[プログラム]** > **[HP Data Protector]** > **[Data Protector][Manager]** を選択します。
   - Data Protector Java GUI:
     - Windowsの場合: **[スタート]** > **[プログラム]** > **[HP Data Protector]** > **[Data Protector][Java GUI Manager]**を選択します。

       [Connect to a Cell Manager]ダイアログで、Cell Managerの名前を選択するか入力して[Connect]をクリックします。
     - UNIXの場合、次のコマンドを実行します。

       /opt/omni/java/client/bin/javadpgui.sh

   Data Protectorグラフィカルユーザーインタフェースの詳細は、「Data Protectorグラフィカルユーザーインタフェース」(40ページ)およびオンラインヘルプを参照してください。
2. Data Protector Managerで、**[クライアント]**コンテキストを選択します。
3. Scopingペインで**[クライアント]**を右クリックし、**[クライアントの追加]**をクリックします。
4. 複数のインストールサーバーが構成されている場合は、インストールするクライアントのプラットフォーム(UNIXまたはWindows)と、クライアントのインストールに使用するインストールサーバーを選択します。**[次へ]**をクリックします。

5. クライアントの名前を直接入力できるほか、Windows GUIを使用している場合は図14(88ページ)およびで説明されているようにインストールするクライアントを検索することもできます。[**次へ**]をクリックします。

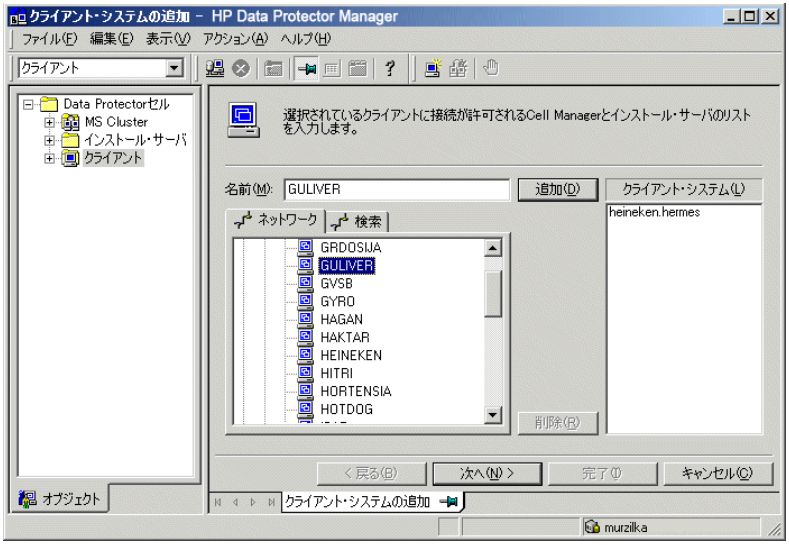


図 14 クライアントの選択

6. 図15(89ページ)に示すように、インストールするData Protectorコンポーネントを選択します。なお、Media Agentは1種類しか選択できません。「Data Protectorコンポーネント」(76ページ)を参照してください。

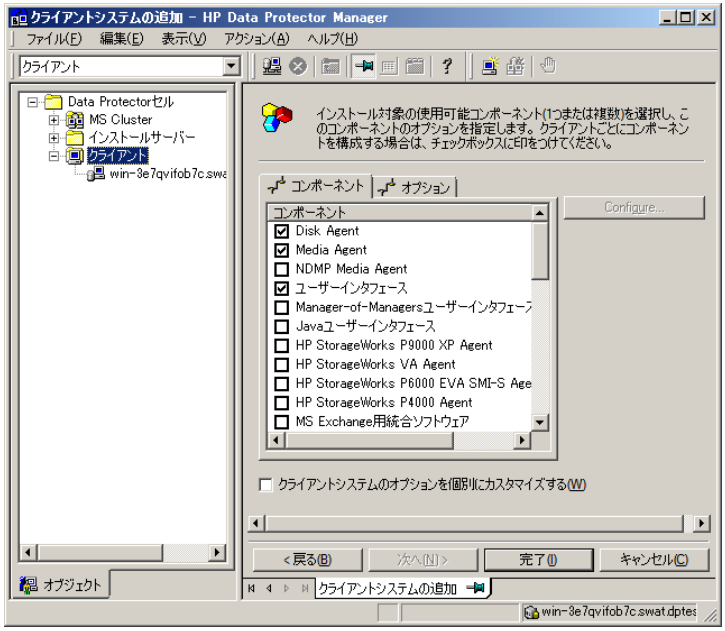


図 15 コンポーネントの選択

デフォルトのユーザーアカウントとインストール先ディレクトリ(Windowsのみ)を変更する場合は、**[オプション]**をクリックします。

複数のクライアントを選択した後、クライアントごとに異なるコンポーネントをインストールするには、**[クライアントシステムのオプションを個別にカスタマイズする]**をクリックし、**[次へ]**をクリックします。その後、インストール対象のコンポーネントをクライアントごとに個別に選択します。

[完了]をクリックしてインストールを開始します。

7. Install中にメッセージが表示されたら、目的のクライアントシステムにアクセスするために必要なデータ(ユーザー名、パスワード、およびWindowsの場合はドメイン)を入力し、[OK]をクリックします。

システムにData Protectorソフトウェアがインストールされ、Data Protectorセルに追加されるとすぐに、Data Protectorクライアントとなります。

注記：

クライアントシステム上でData Protector GUIを起動する前に、そのシステムを使用するユーザーを適切なData Protectorユーザーグループに追加しておいてください。ユーザーグループへの追加手順と選択可能なユーザー権限の詳細は、オンラインヘルプを参照してください。

トラブルシューティング

リモートインストールが完了すると、GUIを使用して[Actions]および[Restart Failed Clients]をクリックすることにより、失敗したインストール手順を再開できます。インストールが再度失敗する場合は、第6章（343ページ）を参照してください。

クライアントへのコンポーネントの追加

既存のクライアントとCell Managerには、追加のData Protectorソフトウェアコンポーネントをインストールできます。コンポーネントは、リモートまたはローカルに追加できます。ローカルインストールについては、「Data Protectorソフトウェアコンポーネントの変更」（257ページ）を参照してください。

MC/ServiceGuardクライアント

MC/ServiceGuardクラスター環境では、コンポーネントの追加先のノードがアクティブになっていることを確認してください。

前提条件

対応するインストールサーバーが利用可能であること。

Data Protectorセル内のクライアントにData Protectorソフトウェアを配布するには、以下の手順に従ってください。

1. Data Protector Managerで、[**クライアント**]コンテキストを選択します。
2. Scopingペインで[クライアント]を展開し、クライアントを右クリックし、[**クライアントの追加**]をクリックします。
3. 複数のインストールサーバーが構成されている場合は、コンポーネントをインストールするクライアントのプラットフォーム(UNIXまたはWindows)と、コンポーネントのインストールに使用するインストールサーバーを選択します。[**次へ**]をクリックします。

4. 図16(91ページ)に示すように、コンポーネントをインストールするクライアントを選択します。[**次へ**]をクリックします。

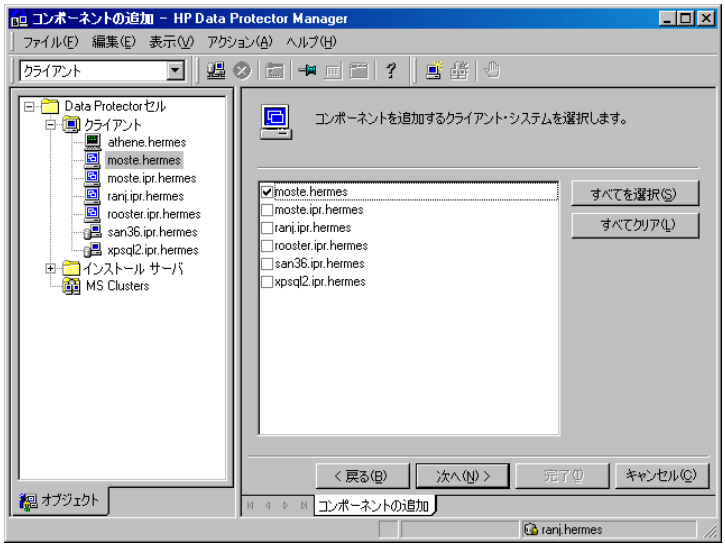


図 16 クライアントの選択

5. 図17(92ページ)に示すように、インストールするData Protectorコンポーネントを選択します。なお、Media Agentは1種類しか選択できません。「Data Protectorコンポーネント」(76ページ)を参照してください。

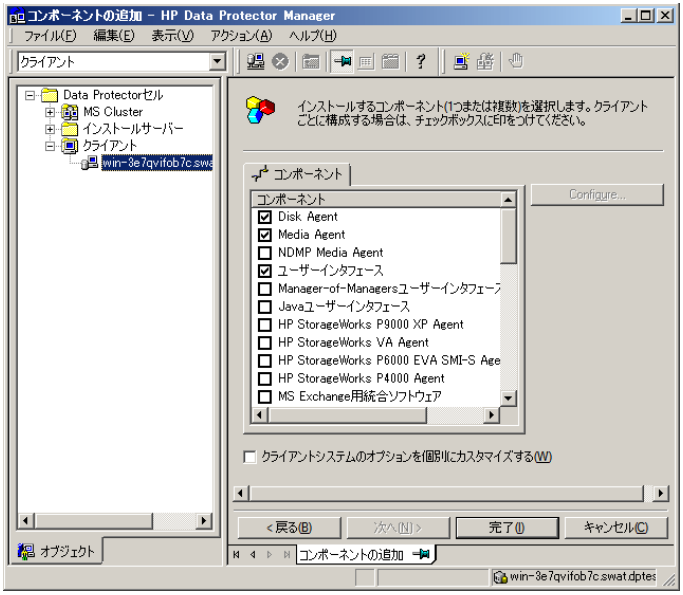


図 17 コンポーネントの選択

複数のクライアントを選択した後、クライアントごとに異なるコンポーネントをインストールするには、[**クライアントシステムのオプションを個別にカスタマイズする**]をクリックし、[**次へ**]をクリックします。その後、コンポーネントをクライアントごとに個別に選択します。

[**完了**]をクリックしてインストールを開始します。

Windows用クライアントのインストール

特定のWindowsオペレーティングシステムでサポートされるプラットフォームとコンポーネントの詳細は、http://www.hp.com/support/manualsを参照してください。

前提条件

Windowsクライアントをインストールするには、Administrator権限が必要です。Data Protectorクライアントシステムとして使用するWindowsシステムは、以下の条件を満たしている必要があります。

- Microsoft Internet Explorer 5.0以上がインストールされていること。

- Data Protectorクライアントソフトウェアをインストールするのに十分な容量の空きディスクスペースがあること。詳細は、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- ポート番号5555 (デフォルト)が利用可能であること。
- Microsoft社のTCP/IPプロトコルがインストールされており、実行されていること。このプロトコルを使って、ホスト名を解決できること。コンピュータの名前とホスト名は同じでなければなりません。
- Java GUIクライアントの場合、Java実行時環境のサポート対象バージョンが必要です。『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』、または最新のサポート一覧(http://www.hp.com/support/manuals)を参照してください。
- ネットワークアクセスユーザー権限が、インストールを実行するアカウントのWindowsローカルセキュリティポリシーの下に設定されていることを確認します。

制限事項

- Windowsオペレーティングシステムのセキュリティ規制により、インストールサーバーを使用してクライアントをリモートにインストールできるのは、同一ドメイン内に限られます。
- Windows XP Home Editionでは、Data Protectorクライアントはローカルにのみインストールできます。
- Windows Vista、Windows 7、またはWindows Server 2008システムにクライアントをリモートでインストールするときは、次のいずれかのアカウントを使用する必要があります。
  - リモートシステム上の組み込み管理者アカウント。このアカウントは、*管理者承認モード*を無効にした状態で有効にしておく必要があります。
  - ドメインユーザーアカウント。このアカウントは、リモートシステムのローカル管理者ユーザーグループのメンバーです。

推奨事項

Data Protector 6.20のインストールを開始するにあたって、各Windowsクライアント上にMicrosoft Installer (MSI) 2.0がインストールされていることを確認してください。MSIのバージョンが古い場合は、Data Protectorセットアッププログラムにより、自動的にバージョン2.0にアップグレードされます。この場合、Data Protectorによって、アップグレードの最後の段階でMSIがアップグレードされたことが通知されます。MSIがアップグレードされた場合は、システムを再起動することを強く推奨します。個々のWindowsオペレーティングシステムに対するMicrosoft Installer 2.0の前提条件については、Microsoft Supportにお問い合わせください。

MSIの古いバージョンでData Protectorのインストールを開始した場合は、Data Protectorセットアッププログラムにより、自動的にバージョン2.0にアップグレードされます。ただし、

アップグレードを有効にするには、システムを再ブートする必要があります。システムの再ブートが完了したら、インストールを初めからやり直してください。

自動ディザスタリカバリモジュール

ディザスタリカバリの準備を自動実行するには、自動ディザスタリカバリで復旧したいクライアント、および拡張ディザスタリカバリ用のDR CD ISOイメージを準備するシステムに、自動ディザスタリカバリコンポーネントをインストールする必要があります。

クラスター対応クライアント

クラスター対応クライアントをインストールする場合は、上記以外にも必要となる前提条件があります。詳細は、「クラスター対応クライアントのインストール」(204ページ)を参照してください。

Install手順を開始する前に、どのコンポーネントをクライアントシステムにインストールするかを決定しておいてください。Data Protectorソフトウェアコンポーネントのリストと説明は、「Data Protectorコンポーネント」(76ページ)を参照してください。

ローカルインストール

Windowsクライアントは、WindowsインストールDVD-ROMからローカルにインストールすることができます。以下の手順に従ってください。

1. WindowsインストールDVD-ROM

   Windows Vista、Windows 7、およびWindows Server 2008システムの場合は、[ユーザーアカウント制御]ダイアログボックスが表示されます。**[続行]**をクリックしてインストールを続けます。

2. HP Data Protectorウィンドウで**[インストールData Protector]**を選択し、Data Protectorのセットアップ用ウィザードを開始します。

3. セットアップ用ウィザードの指示に従って操作を行い、ライセンス契約を十分にお読みください。記載内容に同意する場合は、**[Next]**をクリックして次に進みます。

4. **[Installatoin Type]**ページで、**[Client]**を選択します。Itaniumクライアントの場合は、自動的にタイプが選択されます。

5. Cell Managerの名前を入力します。詳細については、図18(95ページ)を参照してください。

   Cell Managerでデフォルトポート番号5555以外の番号を使用する場合は、ポート番号を変更します。[Check response...]をクリックすると、Cell Managerがアクティブかどうかと、選択したポート番号が使用されているかどうかをテストできます。

   [Next]をクリックします。

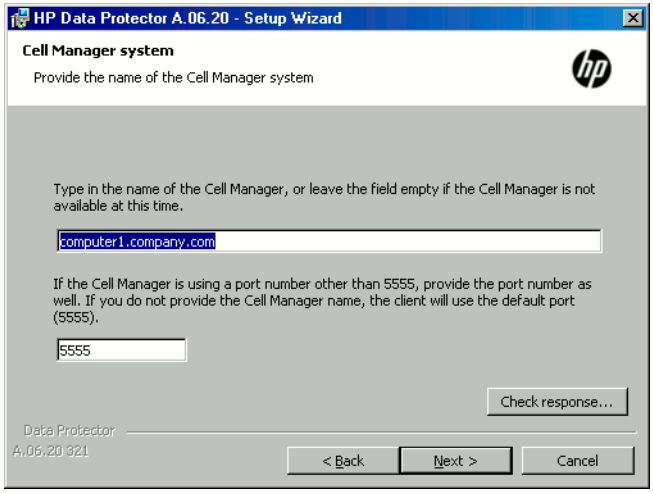


図 18 Cell Managerの選択

6. Data Protectorをデフォルトフォルダにインストールする場合には、[Next]をクリックします。

   それ以外の場合は、[Change]をクリックして[Change Current Destination Folder]ページを開き、パスを入力します。

7. Install対象のData Protectorコンポーネントを選択します。

   その他のData Protectorコンポーネントの詳細は、「Data Protectorコンポーネント」(76ページ)を参照してください。

   [Next]をクリックします。

8. *Data Protectorによってシステムに*Windows*ファイアウォールが検出されると、*[Windows Firewall configuration]ページが表示されます。Data Protectorのセットアッププログラムによって、必要なすべてのData Protector実行可能ファイルが登録されます。デフォルトでは、[Initially, enable newly registered Data Protector binaries to open ports as needed]オプションが選択されています。この時点で、Data Protectorによってポートがオープンされないようにするには、オプションを選択解除します。ただし、Data Protectorを適切に機能させるには、実行可能ファイルを有効にする必要があります。

   [Next]をクリックします。

9. コンポーネント選択サマリーページが表示されます。[Install]をクリックして、選択したコンポーネントをインストールします。

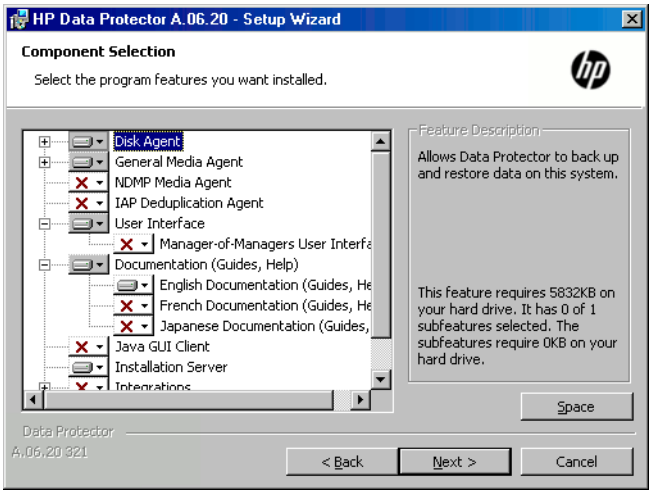


図 19 コンポーネント選択サマリーページ

10. Installステータスのページが表示されます。[Next]をクリックします。

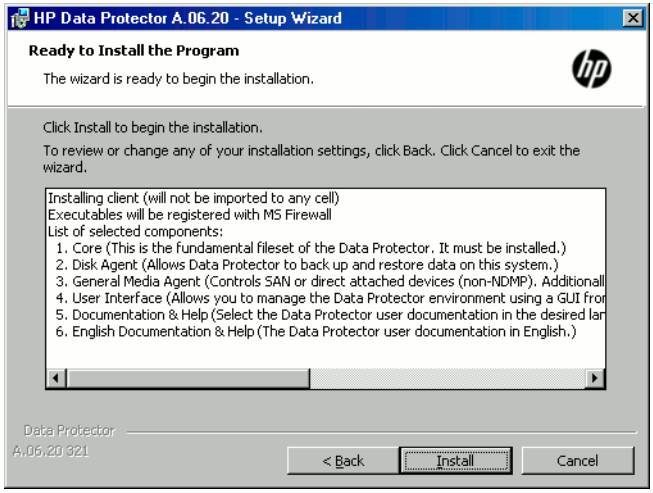


図 20 インストールサマリーページ

11. セットアップ後すぐにData Protectorを起動するには、[Launch Data Protector Manager]を選択します。

    『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を表示するには、[Open the Product Announcements]を選択します。

    [Finish]をクリックします。

Windowsシステムへのバックアップデバイスの接続

Media Agentコンポーネントのインストール後は、バックアップデバイスをWindowsシステムに接続できます。以下の手順に従ってください。

1. 利用可能なSCSIアドレスを確認し、接続するバックアップデバイスのドライブおよび制御デバイス(ロボティクス)に割り当てるSCSIアドレスを決定します(なおWindows上では、SCSIアドレスのことを*SCSIターゲットID*と呼びます)。詳細については、「Windowsシステム上の未使用のSCSIターゲットIDの取得」(415ページ)を参照してください。

2. まだ使用されていないSCSIターゲットIDを、ドライブおよび制御デバイス(ロボティクス)に割り当てます。デバイスの種類にもよりますが、通常はターゲットIDをデバイス上のスイッチで設定できます。詳細は、使用するデバイスのマニュアルを参照してください。

   サポート対象のデバイスの詳細は、http://www.hp.com/support/manualsも参照してください。

3. コンピュータの電源を切り、バックアップデバイスを本体に接続します。
4. デバイスとコンピュータの電源を順に投入し、ブート処理が完了するまで待ちます。
5. 新しいバックアップデバイスがシステムによって正しく認識されていることを確認します。Data_Protector_home¥binディレクトリからdevbra -devコマンドを実行してください。

   画面に表示されたリストに新しいデバイスが含まれていることを確認します。devbra -devコマンドの出力例を以下に示します。

   - 使用しているデバイスのテープドライバがロードされている場合。

     ```
     HP:C1533A
     tape3:0:4:0
     DDS
     ...
     ```

     1行目はデバイスの仕様を表し、2行目はデバイスファイル名を示します。

     この例の場合、ドライブインスタンス番号3のHP DDSテープデバイスがSCSIバス0に接続されており、SCSIターゲットID 4およびLUN番号0が割り当てられています。

   - 使用しているデバイスのテープドライバがロードされていない場合。

     ```
     HP:C1533A
     scsi1:0:4:0
     DDS
     ...
     ```

     1行目はデバイスの仕様を表し、2行目はデバイスファイル名を示します。

     この例の場合、HP DDSテープデバイスがSCSIバス0上のSCSIポート1に接続されており、テープドライブにSCSIターゲットID 4およびLUN番号0が割り当てられています。

デバイスのネイティブテープドライバをロードまたはアンロードする方法は、「Windowsでのテープドライバおよびロボティクスドライバの使用」(397ページ)を参照してください。デバイスファイル名の作成方法は、「Windows上でのデバイスファイル(SCSIアドレス)の作成」(400ページ)を参照してください。

この次に行う作業

クライアントコンポーネントをインストールし、バックアップデバイスを接続したら、バックアップデバイスおよびメディアプールを構成します。オンラインヘルプの索引「構成、バックアップデバイス」を参照して、構成タスクの詳細をご確認ください。

HP-UXクライアントのインストール

HP-UXクライアントは、HP-UX用またはSolaris/Linux用インストールDVD-ROMを使ってローカルにインストールすることも、UNIX用のインストールサーバーを使ってリモートでインストールすることもできます。

Install手順を開始する前に、どのコンポーネントをクライアントシステムにインストールするかを決定しておいてください。Data Protectorソフトウェアコンポーネントのリストと説明は、「Data Protectorコンポーネント」(76ページ)を参照してください。

前提条件

- システム要件、ディスクスペース要件、サポートされているプラットフォーム、プロセッサとData Protectorコンポーネントについては、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- この時点で、Cell ManagerおよびUNIX用のインストールサーバーをネットワーク上にインストールしておく必要があります。まだインストールしていない場合は、「Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール」(44ページ)の説明にしたがってインストールしてください。
- Installを実行するには、*root*ユーザーによるアクセスか、または*root*ユーザーの権限付きのアカウントが必要です。
- Java GUIクライアントの場合、Java実行時環境のサポート対象バージョンが必要です。『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』、または最新のサポート一覧(http://www.hp.com/support/manuals)を参照してください。

ローカルインストール

お使いの環境にUNIX用のインストールサーバーがない場合は、HP-UX用またはSolaris/Linux用インストールDVD-ROMを使用して、ローカルインストールを行う必要があります。この手順については、「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)を参照してください。

ローカルインストール後には、クライアントシステムをセルに手作業でインポートする必要があります。「セルへのクライアントのインポート 」(213ページ)も参照してください。

リモートインストール

UNIXクライアントソフトウェアは、Data Protectorグラフィカルユーザーインタフェースを使ってUNIX用のインストールサーバーからリモートにインストールできます。ソフトウェアのリモートインストール手順は、「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

リモートインストールが終了すると、クライアントシステムは自動的にData Protectorセルのメンバーになります。

クライアントにMedia Agentをインストールしたら、バックアップデバイスをシステムに物理的に接続しなければなりません。また、デバイスの種類に応じた適切なデバイスドライバがカーネルに組み込まれているかどうかを確認するため、バックアップの実行前にカーネルの構成をチェックしておかなければなりません。

クラスター対応クライアント

クラスター対応クライアントをインストールする場合は、上記以外にも必要となる前提条件があります。詳細は、「クラスター対応クライアントのインストール」(194ページ)を参照してください。

HP-UXのカーネル構成のチェック

*HP System Administration Manager (SAM)*ユーティリティを使って、HP-UX 11.x上のカーネルの構成をチェックおよびビルドするには、以下の手順に従ってください。なお、カーネルを手作業でビルドする手順は、「HP-UX上のSCSIロボティクス構成」(401ページ)を参照してください。

*HP System Administration Manager (SAM)*ユーティリティを使ってカーネルをビルドするには、以下の手順に従ってください。

1. rootユーザーとしてログインし、端末を開いてsamと入力します。
2. [System Administration Manager]ウィンドウで[Kernel Configuration]と[Drivers]を順にダブルクリックします。

3. [Kernel Configuration]ウィンドウで、以下の条件が満たされていることを確認します。

- 使用するデバイスのドライバがインストール済みドライバのリストに含まれていること。図21(101ページ)を参照してください。目的のドライバがリストに含まれていない場合は、/usr/sbin/swinstallユーティリティを使ってインストールする必要があります。たとえば、次のものが必要です。
  - テープデバイスにはテープデバイスドライバが必要です。システムにテープデバイスを接続する場合は、適切なテープデバイスドライバがインストールされていることを確認してください。たとえばstapeドライバはDLTやLTOなどの汎用的なSCSIテープドライブで使用され、tape2ドライバはDDSデバイスで使用されます。
  - テープライブラリデバイスのロボティクスを制御するには、使用するハードウェアに応じて、SCSIパススルードライバ(sctlまたはspt)か、オートチェンジャロボティクスドライバ(schgr)が必要です。

    詳細は、「HP-UX上のSCSIロボティクス構成」(401ページ)を参照してください。

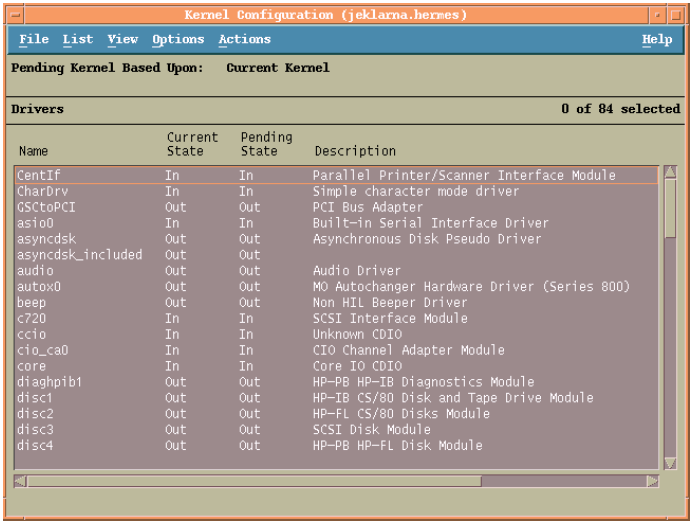


図 21 [Kernel Configuration]ウィンドウ

- [Current State]列でドライバのステータスが[In]に設定されていることを確認します。ステータスが[Out]に設定されている場合は、以下の操作を行ってください。
  1. リスト内のドライバを選択します。[Actions]をクリックして[Add Driver to Kernel]を選択します。[Pending State]列のステータスが[In]に変化したことを確認します。

     これを、[Current State]列が[In]に設定されている各ドライバに対して繰り返します。

2. [Actions]をクリックして[Create a New Kernel]を選択し、変更内容を確定します。これにより、[Pending Kernel]のラベルが[Current Kernel]に変化します。ただし、システムを再起動する必要があります。

必要なドライバをカーネルに組み込んだら、以下の手順に従って、バックアップデバイスをコンピュータに接続してください。

HP-UXシステムへのバックアップデバイスの接続

1. ドライブおよび制御デバイス(ロボティクス)に割り当てるSCSIアドレスを決定します。システムコマンドの/usr/sbin/ioscan -fを使います。

   詳細は、「HP-UX上の未使用のSCSIアドレスの取得」(408ページ)を参照してください。

2. デバイスのSCSIアドレスを設定します。デバイスの種類にもよりますが、通常はSCSIアドレスをデバイス上のスイッチで設定できます。詳細は、使用するデバイスのマニュアルを参照してください。

   サポート対象のデバイスの詳細は、http://www.hp.com/support/manualsを参照してください。

3. デバイスをコンピュータに接続し、デバイスとコンピュータの電源を順に投入します。ブート処理が完了するまで待ちます。通常、デバイスファイルは、ブート処理中に生成されます。

4. 新しいバックアップデバイスがシステムによって正しく認識されていることを確認します。ioscanユーティリティを以下のコマンドで実行してください。

   ```
   /usr/sbin/ioscan -fn
   ```

   このコマンドを実行すると、接続されている各バックアップデバイスに対するデバイスファイルのリストが表示されます。デバイスファイルがブート時に自動生成されない場合は、手作業でデバイスファイルを作成する必要があります。詳細については、「HP-UX上のデバイスファイルの作成」(406ページ)を参照してください。

Install手順が完了し、バックアップデバイスが正しくシステムに接続されたら、オンラインヘルプの索引「構成、バックアップデバイス」を参照して、デバイスおよびメディアプールまたはData Protectorのその他の構成タスクの詳細を確認してください。

Solaris用クライアントのインストール

Solarisクライアントは、HP-UX用またはSolaris/Linux用インストールDVD-ROMを使ってローカルにインストールすることも、UNIX用のインストールサーバーを使ってリモートインストールすることもできます。

Install手順を開始する前に、どのコンポーネントをクライアントシステムにインストールするかを決定しておいてください。Data Protectorソフトウェアコンポーネントのリストと説明は、「Data Protectorコンポーネント」(76ページ)を参照してください。

前提条件

- システム要件、ディスクスペース要件、サポートされているプラットフォームとData Protectorコンポーネントについては、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- この時点で、Cell ManagerおよびUNIX用のインストールサーバーをネットワーク上にインストールしておく必要があります。手順については、「Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール」(44ページ)を参照してください。
- Solarisクライアントをインストールするには、*root*ユーザーによるアクセスか、または*root*権限付きのアカウントが必要です。
- Java GUIクライアントの場合、Java実行時環境のサポート対象バージョンが必要です。『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』、または最新のサポート一覧(http://www.hp.com/support/manuals)を参照してください。

ローカルインストール

お使いの環境にUNIX用のインストールサーバーがない場合は、HP-UX用またはSolaris/Linux用インストールDVD-ROMを使用して、ローカルインストールを行う必要があります。手順については、「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)を参照してください。

リモートインストール

UNIXクライアントソフトウェアは、Data Protectorグラフィカルユーザーインタフェースを使ってUNIX用のインストールサーバーからリモートにインストールできます。ソフトウェアのリモートインストール手順は、「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

注記:

ユーザーインタフェース**コンポーネント(グラフィカルユーザーインタフェースとコマンドラインインタフェースが含まれる)を使用する場合は、事前に環境変数を更新する必要があります。詳細は、「環境変数の設定」(53ページ)を参照してください。**

Solaris 2.6クライアントにユーザーインタフェースをインストールした場合、コマンドラインインタフェースのみを使用できます。

クライアントコンポーネントのインストールが完了したターゲットシステムは、自動的にData Protectorセルに追加されます。

重要:

Data Protectorは、たとえば次のようなリンクディレクトリにインストールすることができます。

/opt/omni/ -> /prefix/opt/omni/

/etc/opt/omni/ -> /prefix/etc/opt/omni/

/var/opt/omni/ -> /prefix/var/opt/omni/

このようにする場合は、インストール前にリンクを作成しておき、インストール先ディレクトリが存在することを確認しておかなければなりません。

クラスター対応クライアント

クラスター対応クライアントをインストールする場合は、上記以外にも必要となる前提条件があります。詳細は、「クラスター対応クライアントのインストール」(207ページ)を参照してください。

インストール後の構成

構成ファイル

クライアントシステムにMedia Agentコンポーネントをインストールした後は、使用するデバイスの種類に応じて、構成ファイル(/kernel/drv/st.conf)の内容をチェックする必要があります。

- Exabyteデバイス(8 mm)を使用する場合は、/kernel/drv/st.confファイルの内容を変更する必要はありません。
- HP DATデバイス(4 mm)を使用する場合は、/kernel/drv/st.confファイルに以下の行を追加してください。

```
tape-config-list =

"HP     HP35470A", "HP DDS 4mm DAT", "HP-data1", "HP     HP35480A", "HP DDS-DC
4mm DAT", "HP-data1", "HP       C1533A", "HP DDS2 4mm DAT", "HP-data2", "HP
C1537A", "HP DDS3 4mm DAT", "HP-data3", "HP       C1553A", "HP DDS2 4mm
DATloader", "HP-data2", "HP       C1557A", "HP DDS3 4mm DATloader", "HP-data3";
HP-data1 = 1,0x34,0,0x8019,3,0x00,0x13,0x03,2; HP-data2 =
1,0x34,0,0x8239,4,0x0,0x13,0x24,0x3,3; HP-data3 =
1,0x34,0,0x8239,4,0x0,0x13,0x24,0x3,3;
```

重要:

これらのHPデータエントリは、HPのサポートで通常推奨しているデフォルトエントリとは異なっています。これらの行は必ず上に示したとおりに記述してください。記述に誤りがあると、そのドライブをData Protectorで使用できなくなります。

- DLT、DLT1、SuperDLT、LTO1、LTO2、およびSTK9840デバイスを使用する場合は、/kernel/drv/st.confファイルに以下の行を追加してください。

```
tape-config-list =

"HP      Ultrium 1-SCSI", "HP Ultrium 1-SCSI", "LTO-data", "HP
Ultrium 2-SCSI", "HP_LTO",      "HP-LTO2", "DEC DLT2000",
"Digital DLT2000",    "DLT2k-data", "Quantum DLT4000","Quantum
DLT4000", "DLT4k-data", "QUANTUM DLT7000", "Quantum DLT7000",
"DLT7k-data", "QUANTUM DLT8000", "Quantum DLT8000",    "DLT8k-data",
"HP C9264CB-VS80","HP DLT vs80 DLTloader","HP_data1"
"QUANTUM SuperDLT1", "QUANTUM SuperDLT",  "SDLT-data",
"TANDBERGSuperDLT1", "TANDBERG SuperDLT", "SDL-data", "STK
9840", "STK 9840",           "CLASS_9840";

DLT2k-data =
1,0x38,0,0x8639,4,0x17,0x18,0x80,0x81,3; DLT4k-data =
1,0x38,0,0x8639,4,0x17,0x18,0x80,0x81,3; DLT7k-data =
1,0x38,0,0x8639,4,0x82,0x83,0x84,0x85,3; DLT8k-data =
1,0x77,0,0x1D639,4,0x84,0x85,0x88,0x89,3; HP_data1 =
1,0x3a,0,0x8639,4,0x40,0x86,0x87,0x7f,0; LTO-data =
1,0x7a,0,0x1d679,4,0x00,0x00,0x00,0x40,3; HP-LTO2 =
1,0x7a,0,0xd639,4,0x00,0x00,0x00,0x42,3; SDLT-data =
1,0x79,0,0x8639,4,0x90,0x91,0x90,0x91,3; CLASS_9840 =
1,0x78,0,0x1d679,1,0x00,0;
```

- HP StorageWorks 12000e (48AL)オートローダー(HP C1553A)を使用する場合は、/kernel/drv/st.confファイル内のHPデータエントリに加えて、以下のエントリを追加してください。

```
name="st" class="scsi" target=ID lun=0; name="st" class="scsi" target=ID lun=1;
```

*ID*の箇所にオートローダーのSCSIアドレスを指定し、オートローダーのオプション番号スイッチを5に設定します(このスイッチは、デバイスの背面パネルにあります)。さらに、デバイスのDIPスイッチの設定を11111001に変更します(これらのスイッチは、オートローダーの底面から操作できます)。

注記:

HP StorageWorks 12000eライブラリには、ピッカーデバイス専用のSCSI IDはありませんが、同じSCSI IDからデータドライブアクセスコマンドとピッカーコマンドの両方を受け付けるようになっています。ただし、データドライブアクセスコマンドはSCSI lun=0にリダイレクトし、ピッカーコマンドはSCSI lun=1にリダイレクトする必要があります。

他のすべてのデバイスについて、st.confファイルに必要なエントリがあるかどうか、st.conf.templテンプレートファイル(/opt/omni/sptにあります)をチェックします。これは単なるテンプレートファイルであり、st.confファイルの代用となるものではありません。

- Solaris上でSCSIパススルードライバとともにSCSIエクスチェンジャデバイスを使用する場合は、SCSIパススルードライバをまず最初にインストールしてから、SCSIデバイスをインストールする必要があります。

  SCSIパススルードライバをインストールするには、以下の手順に従ってください。

  1. sstモジュールを/usr/kernel/drv/sparcv9ディレクトリにコピーし、構成ファイルsst.confを/usr/kernel/drvディレクトリにコピーします。以下のコマンドを実行してください。

     32ビット版Solarisの場合:

     ```
     $cp /opt/omni/spt/sst /usr/kernel/drv/sst
     ```

     ```
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```

     64ビット版Solarisの場合:

     ```
     $cp /opt/omni/spt/sst.64bit /usr/kernel/drv/sparcv9/sst
     ```

     ```
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```

  2. /etc/devlink.tabファイルに以下の行を追加します。

     重要:

     /etc/devlink.tabファイルの編集には、スペース文字を使用しないでください。タブ文字のみを使用してください。

     ```
     "type=ddi_pseudo;name=sst;minor=character rsst¥A1"
     ```

     この行を追加すると、devlinks(1M)によって、/dev/rsstX (XはSCSIターゲット番号)形式の名前のデバイスへのリンクが生成されます。

3. 以下のコマンドを入力して、システムにドライバをインストールします。

   add_drv sst

4. ここまでの段階で、SCSIデバイスをインストールする準備は完了です。インストールを開始する前に、各ドライブおよびエクスチェンジャデバイスのロボティクス(ピッカー)に正しいSCSIアドレスを割り当てておく必要があります。選択するアドレスは、システム上の他のデバイスに使用されていないものでなければなりません。

   SCSI構成をチェックするには、最初に以下のコマンドを入力してシステムをシャットダウンします。

   shutdown -i0

   次にokプロンプトからprobe-scsi-allコマンドを実行して、割り当て済みのアドレスをチェックします。

   ok probe-scsi-all

   チェックが完了したら、以下のコマンドでシステムを再起動します。

   ok boot -r

   SCSIデバイスをインストールするには、以下の手順に従ってください。

   a. /kernel/drv/st.confを編集し、割り当てたSCSIポートを使用するようにデバイスのドライブパラメータを構成します。詳細は、デバイスのマニュアルを参照してください。

      なお、ここでは、SCSIポート5をSCSIドライブに割り当て、SCSIポート4をADIC SCSI制御デバイス(ピッカー)に割り当てて、ADIC-VLS DLTデバイスをセットアップする場合を想定しています。

例

```
tape-config-list = “DEC     DLT2000″, ″ADIC DLTDlib” ,″ADIC2000-data″;
ADIC2000-data = 1,0x38,0,0x8639,4,0x17,0x18,0x80,0x81,3;
name=” st” class= “scsi” target=5 lun=0; name=” st” class= “scsi”
target=4 lun=0;
```

      上の例に示されたデータは、

      /kernel/drv/st.confファイルになければなりません。

   b. /usr/kernel/drv/sst.confファイルを編集して、割り当てたSCSIポート4を使用するようにADIC SCSI制御デバイスをセットアップします。ADICドライブに関して以下のデータを/usr/kernel/drv/sst.confファイルに追加します。

      ```
      name=” sst” class= “scsi” target=4 lun=0;
      ```

/kernel/drv/st.confファイルおよび/usr/kernel/drv/sst.confファイルを変更し終えたら、システムにバックアップデバイスを接続する準備が完了したことになります。

Solarisシステムへのバックアップデバイスの接続

Solarisシステムにバックアップデバイスを接続するには、以下の手順に従ってください。

1. reconfigureファイルを作成します。

   touch /reconfigure

2. 次に、$shutdown -i0コマンドを入力してシステムをシャットダウンし、コンピュータの電源を切ってから、デバイスをSCSIバスに物理的に接続します。選択したSCSIアドレスが他のデバイスに使用されていないことをチェックしてください。

   サポート対象のデバイスの詳細は、http://www.hp.com/support/manualsを参照してください。

   注記:

   Data Protectorは、Solarisシステム上ではクリーニングテープを自動認識しません。HP StorageWorks 12000e (48AL)デバイスで使用されているクリーニングテープをData Protectorが検出して挿入した場合は、テープドライバは未定義の状態となり、システムの再ブートが必要になります。Data Protectorがクリーニングテープのロード要求を出した場合は、手作業でロードしてください。

3. コンピュータの電源を投入し、ブート処理の途中でStop-Aキーを押して、ブート処理を中断させます。okプロンプトにコマンドをprobe-scsi-allと入力して、新しいデバイスが正しく認識されているかどうかを確認します。

   ok > probe-scsi-all

   次に

   ok > go

   と入力して操作を続行します。

4. この時点で、デバイスが正しく動作していることを確認します。ドライブのデバイスファイルは/dev/rmtディレクトリに格納する必要があり、SCSI制御デバイス(ピッカー)のデバイスファイルは/devディレクトリに格納する必要があります。

注記:

Solarisシステム上では(特に64ビット版Solarisの場合は)、SCSI制御デバイス(ピッカー)へのリンクが自動的に生成されないことがあります。この場合はシンボリックリンクを作成してください。以下に例を示します。`ln -s /devices/pci@1f,4000/scsi@3,1/sst@4,1:character /dev/rsst4`

デバイスの動作は、Data Protectorのumaユーティリティで確認できます。前に例示したSCSIエクスチェンジャデバイス(SCSIポート4を使用)のピッカーの動作をチェックするには、以下のように入力します。

```
echo "inq" |/opt/omni/lbin/uma -ioctl /dev/rsst4
```

ピッカーは、SCSI-2デバイスライブラリとして動作しなければなりません。ライブラリは、強制的に初期化することでチェックできます。以下のコマンドを入力してください。

```
echo "init" |/opt/omni/lbin/uma -ioctl /dev/rsst4
```

Berkeleyスタイルのデバイスファイルを必ず使用してください。この例の場合、エクスチェンジャドライブには、/dev/rmt/0hではなく/dev/rmt/ohbを使用し、SCSI制御デバイス(ピッカー)には/dev/rsst4を使用する必要があります。

この次に行う作業

Install手順が完了し、バックアップデバイスが正しくSolarisクライアントに接続されたら、オンラインヘルプの索引「構成、バックアップデバイス」を参照して、バックアップデバイス、メディアプール、またはその他の構成タスクの詳細を確認してください。

Linuxクライアントのインストール

Linuxクライアントシステムは、HP-UX用またはSolaris/Linux用インストールDVD-ROMを使ってローカルにインストールすることも、UNIX用のインストールサーバーを使ってリモートインストールすることもできます。

Install手順を開始する前に、どのコンポーネントをクライアントシステムにインストールするかを決定しておいてください。Data Protectorソフトウェアコンポーネントのリストと説明は、「Data Protectorコンポーネント」(76ページ)を参照してください。

前提条件

- システム要件、ディスクスペース要件、サポートされているプラットフォームとData Protectorコンポーネントについては、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- この時点で、Cell ManagerおよびUNIX用のインストールサーバーをネットワーク上にインストールしておく必要があります。この手順については、「Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール」(44ページ)を参照してください。
- rpmユーティリティをインストールして、セットアップしておく必要があります。その他のパッケージングシステム(debなど)はサポートされていません。
- Java GUIクライアントの場合、Java実行時環境のサポート対象バージョンが必要です。『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』、または最新のサポート一覧(http://www.hp.com/support/manuals)を参照してください。
- Data Protectorコンポーネントをリモートシステムにインストールする場合は、リモートシステム上で以下の前提条件を満たしている必要があります。
  - inetdまたはxinetdサービスが実行またはセットアップされ、Data Protectorが開始可能である。
  - sshサービス、またはsshがインストールされていない場合にはrexecサービスが有効になっている。
- カーネルがSCSIデバイス(SCSI support、SCSI tape support、SCSI generic supportの各モジュール)をサポートしていることを確認してください。パラメータProbe all LUNa on each SCSI deviceは省略可能です。

  Linuxカーネルでの SCSIサポートの詳細は、お使いのLinuxディストリビューションまたはLinuxカーネルのマニュアルを参照してください。

注記:

オリジナルのData Protector GUIがサポートされていないCell Managerのプラットフォームでは、Data Protector Java GUIを使用するか、オリジナルのData Protector GUIがサポートされているシステムにインストールできます。新しいCell Manager上にリモートユーザーアカウントを作成するには、omniusersコマンドを使用します。これにより、Data Protector GUIをインストールした任意のシステム上でこのユーザーアカウントを使ってGUIを起動し、新しいCell Managerに接続できます。詳細はomniusersのマンページを参照してください。

注記:

Data Protectorはデフォルトでポート番号5555を使用します。そのため、このポート番号が他のプログラムで使われていないことを確認する必要があります。一部のLinuxバージョンでは、このポート番号が別の目的で使われています。

ポート番号5555がすでに使われている場合は、Data Protectorで使えるようにこのポート番号を空けるか、あるいは、デフォルトのポート番号を未使用の番号に変更してください。「Data Protectorのデフォルトのポート番号の変更」(388ページ)を参照してください。

MC/ServiceGuardクラスター

MC/ServiceGuardクラスターの場合は、Data Protectorエージェント(Disk Agent、Media Agent)を、共有ディスク上ではなく、各クラスターノード(ローカルディスク)上に個別にインストールしなければなりません。

Installが終了したら、*仮想ホスト*(アプリケーションパッケージ)をクライアントとしてセルにインポートする必要があります。そのため、アプリケーションパッケージ(Oracleなど)はクラスター上で、クラスターの*仮想IP*を使って実行されていなければなりません。クライアントをインポートする前に、`cmviewcl -v`コマンドを使用して、この点をチェックしてください。

インストールサーバーのインストールにパッシブノードを使用できます。

Novell Open Enterprise Server (OES)

Novell OESシステムの場合は、Data ProtectorによってOES対応のDisk Agentが自動的にインストールされます。ただし、次のようなNovell OES固有の状況がいくつかあります。

- Novell OESを32ビットSUSE Linux Enterprise Server 9.0 (SLES)にインストールする場合は、Data Protector Linuxクライアントをシステムにインストールした後に、Data Protectorクライアントもアップグレードする必要があります。

  アップグレード処理中に、新しいNovell OES対応Disk Agentがクライアントシステムにリモートでインストールされます。

- Novell OESコンポーネントをSLESから削除する場合は、Data Protectorクライアントを再インストールする必要があります。

ローカルインストール

お使いの環境にUNIX用のインストールサーバーがない場合は、HP-UX用またはSolaris/Linux用インストールDVD-ROMを使用して、ローカルインストールを行う必要があります。この手順については、「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)を参照してください。

リモートインストール

Linuxクライアントシステムは、UNIX用のインストールサーバーからLinuxシステムにData Protectorコンポーネントを配布することにより、リモートでインストールできます。この操作には、Data Protectorグラフィカルユーザーインタフェースを使用します。ソフトウェア配布手順の詳細は、「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

クライアントコンポーネントのインストールが完了したターゲットシステムは、自動的にData Protectorセルに追加されます。

リモートインストールのトラブルシューティング

Linuxクライアントシステムへのリモートインストール中に問題が発生した場合は、rootアカウントに、execサービスまたはshellサービスを使ってシステムにアクセスする権限があるかどうかを確認します。以下の手順に従ってください。

1. /etc/xinetd.confを編集します。execサービスとshellサービスの定義を見つけ、これらの2つのサービスの定義に次の行を追加します。

   server_args = -h

   以下に例を示します。

   ```
   service shell { socket_type = stream
   protocol = tcp wait = no user = root server = /usr/sbin/in.rshd server_args =
   -L -h } service exec { socket_type = stream protocol = tcp wait = no user =
   root server = /usr/sbin/in.rexecd server_args = -h }
   ```

   注記:

   一部のLinuxディストリビューションでは、これらのサービスが/etc/xinetd.dディレクトリ内の個別のファイル内に構成されていることがあります。この場合は、適切なファイル(/etc/xinetd.d/rexecおよび/etc/xinetd.d/rsh)を探して、上記の変更を行ってください。

2. HUPシグナルを使用して、inetdプロセスを停止します。

   kill -HUP $(ps ax|grep inet|grep -v grep|cut -c1-6)

3. ~root/.rhostsファイルを作成して次のエントリを追加します。
   my_installation_server root これにより、インストールサーバーから管理アクセスが可能になります。

Data Protectorのインストールが終了したら、このエントリを-root/.rhostsファイルから削除し、-hフラグを/etc/xinetd.confファイル(Red Hat Enterprise Linuxの場合は/etc/

inetd.confファイル)から削除してもかまいません。その後、手順ステップ 2(112ページ)のkillコマンドを繰り返します。

詳細は、rexecd(8)、rexec(3)、rshd(8)、rsh(1)、pam(8)のマンページを参照してください。問題が発生した場合は、「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)を参照してください。

Linuxシステムへのバックアップデバイスの接続

LinuxクライアントにMedia Agentコンポーネントをインストールした後は、以下の手順に従って、システムにバックアップデバイスを接続してください。

1. cat /proc/scsi/scsiコマンドを実行して、ドライブおよび制御デバイス(ロボティクス)用に使用可能なSCSIアドレスを調べます。
2. デバイスのSCSIアドレスを設定します。デバイスの種類にもよりますが、通常SCSIアドレスはデバイス上のスイッチで設定できます。詳細は、使用するデバイスのマニュアルを参照してください。

   サポート対象のデバイスの詳細は、http://www.hp.com/support/manualsを参照してください。
3. デバイスをコンピュータに接続し、デバイスとコンピュータの電源を順に投入して、ブート処理が完了するまで待ちます。ブート処理中にデバイスファイルが生成されます。(RedHat Linuxの場合は、コンピュータに新しいデバイスを接続すると、ブート処理中にアプリケーションKudzuが起動されます。任意のキーを押してアプリケーションを開始し、[Configure]ボタンをクリックしてください。
4. 新しいバックアップデバイスをシステムが正しく認識しているかどうかを検証するため、cat /proc/scsi/scsiを実行し、次に、dmesg |grep scsiを実行します。接続されている個々のバックアップデバイスについて、デバイスファイルが一覧表示されます。

例

ロボティクスの場合は、dmesg |grep scsiコマンドの出力は次のようになります。

```
Detected scsi generic sg2 at scsi2, channel 0, id 4, lun 0, type 8
```

ドライブの場合は次のようになります。

```
Detected scsi tape st0 at scsi2, channel 0, id 5, lun 0
```

5. デバイスファイルは/devディレクトリ内に生成されます。次のコマンドを実行して、デバイスファイルへのリンクが作成されていることを確認します。

   ```
   ll /dev | grep device_file
   ```

   たとえば、次のように入力してください。

   ```
   ll /dev | grep sg2
   ```

   このコマンドの出力は次のようになります。

   ```
   lrwxrwxrwx 1 root root 3 Nov 27 2001 sg2 -> sgc
   ```

   /dev/sg2はデバイスファイル/dev/sgcへのリンクです。これは、Data Protectorで使用されるデバイスファイルが、ロボティクス用は/dev/sgc、デバイス用は/dev/st0であることを意味しています。ロボディクス用のデバイスファイルはsga、sgb、sgc、… sghで、ドライブ用のデバイスファイルはst0、st1、... st7です。

この次に行う作業

Install手順が完了し、バックアップデバイスが正しくLinuxクライアントシステムに接続されたら、オンラインヘルプの索引「構成、バックアップデバイス」を参照して、バックアップデバイスおよびメディアプール、またはその他の構成タスクの詳細を確認してください。

ESX Serverクライアントのインストール

ESX Serverは、Modified Linuxオペレーティングシステムです。ESX ServerシステムにData Protectorコンポーネントをインストールする方法については、「Linuxクライアントのインストール」(109ページ)を参照してください。

Mac OS Xクライアントのインストール

Mac OS Xクライアントは、HP-UX用またはSolaris/Linux用インストールDVD-ROMを使ってローカルにインストールすることも、UNIX用のインストールサーバーを使ってリモートインストールすることもできます。

Disk Agent(DA)のみがサポートされています。

前提条件

- システム要件、ディスクスペース要件、サポートされているOSバージョン、およびData Protectorコンポーネントについては、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- この時点で、Cell ManagerおよびUNIX用のインストールサーバーをネットワーク上にインストールしておく必要があります。その手順については、「Data Protector Cell

Manager (CM)およびCell Manager (IS)のインストール」(44ページ)を参照してください。

ローカルインストール

お使いの環境にUNIX用のインストールサーバーがない場合は、HP-UX用またはSolaris/Linux用インストールDVD-ROMを使用して、ローカルインストールを行う必要があります。その手順については、「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)を参照してください。

リモートインストール

Mac OS Xクライアントソフトウェアは、Data Protectorグラフィカルユーザーインタフェースを使ってUNIX用のインストールサーバーからクライアントにインストールできます。ソフトウェアのリモートインストール手順の詳細は、「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

クライアントコンポーネントのインストールが完了したターゲットシステムは、自動的にData Protectorセルに追加されます。

AIXクライアントのインストール

AIXクライアントは、HP-UX用またはSolaris/Linux用インストールDVD-ROMを使ってローカルにインストールすることも、UNIX用のインストールサーバーを使ってリモートインストールすることもできます。

Install手順を開始する前に、どのコンポーネントをクライアントシステムにインストールするかを決定しておいてください。Data Protectorソフトウェアコンポーネントのリストと説明は、「Data Protectorコンポーネント」(76ページ)を参照してください。

前提条件

- システム要件、ディスクスペース要件、サポートされているプラットフォームとData Protectorコンポーネントについては、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- この時点で、Cell ManagerおよびUNIX用のインストールサーバーをネットワーク上にインストールしておく必要があります。手順については、「Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール」(44ページ)を参照してください。

重要:

AIXシステムにDisk Agentコンポーネントをインストールする前に、ポートマッパーが動作していることを確認する必要があります。/etc/rc.tcpipファイルを開き、ポートマッパーを起動する行が以下のように記述されていることを確認してください。

```
start /usr/sbin/portmap  "$src_running"
```

srcmstrデーモンが実行されている場合は、src_runningフラグは1に設定されます。srcmstrデーモンは、System Resource Controller (SRC)です。srcmstrデーモンは、サブシステムの生成と管理、サブシステムステータスに関するショートリクエストの処理、サブシステムへのリクエストの送信、エラー通知の処理を行います。

IBM HACMP Cluster

IBM High Availability Cluster Multi-processing environment for AIXの場合、すべてのクラスターノードにData Protector Disk Agentコンポーネントをインストールします。クラスター対応アプリケーションデータベースがインストールされたクラスター環境にData Protectorをインストールする方法については、「Data Protector統合クライアントのインストール」(151ページ)を参照してください。

Installが終了したら、クラスターノードと仮想サーバー(仮想環境パッケージのIPアドレス)をData Protectorセルにインポートします。

ローカルインストール

お使いの環境にUNIX用のインストールサーバーがない場合は、HP-UX用またはSolaris/Linux用インストールDVD-ROMを使用して、ローカルインストールを行う必要があります。構成手順については、「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)を参照してください。

リモートインストール

AIXクライアントソフトウェアは、Data Protectorグラフィカルユーザーインタフェースを使ってUNIX用のインストールサーバーからリモートにインストールできます。ソフトウェアのリモートインストール手順は、「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

クライアントコンポーネントのインストールが完了したターゲットシステムは、自動的にData Protectorセルに追加されます。

AIXクライアントへのバックアップデバイスの接続

AIXクライアントにMedia Agentをインストールした後は、以下の作業を実行してください。

1. コンピュータをシャットダウンし、バックアップデバイスをSCSIバスに接続します。バックアップデバイスに使用するSCSIアドレスが、他のデバイスに使用されていないことを確認してください。

   サポート対象のデバイスの詳細は、http://www.hp.com/support/manualsを参照してください。

2. コンピュータの電源を投入し、ブート処理が完了するまで待ちます。AIXシステム管理ツールのsmitを起動し、新しいバックアップデバイスがシステムによって正しく認識されていることを確認します。

   重要:

   smitを使って、デバイスのデフォルトブロックサイズを0（可変長ブロック）に変更してください。

3. /devディレクトリから適切なデバイスファイルを選択し、Data Protectorバックアップデバイスを構成します。

重要:

巻き戻しなしのデバイスファイルのみを使用してください。たとえば、/dev/rmt0ではなく、/dev/rmt0.1を選択してください。

この次に行う作業

Install手順が完了し、バックアップデバイスが正しくAIXシステムに接続されたら、オンラインヘルプの索引「構成、バックアップデバイス」を参照して、バックアップデバイス、メディアプール、またはData Protectorのその他の構成タスクの詳細を確認してください。

Tru64クライアントのインストール

Tru64クライアントは、HP-UX用またはSolaris/Linux用インストールDVD-ROMを使ってローカルにインストールすることも、UNIX用のインストールサーバーを使ってリモートインストールすることもできます。

Install手順を開始する前に、どのコンポーネントをクライアントシステムにインストールするかを決定しておいてください。Data Protectorソフトウェアコンポーネントのリストと説明は、「Data Protectorコンポーネント」(76ページ)を参照してください。

前提条件

- システム要件、ディスクスペース要件、サポートされているプラットフォームとData Protectorコンポーネントについては、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- この時点で、Cell ManagerおよびUNIX用のインストールサーバーをネットワーク上にインストールしておく必要があります。この手順については、「Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール」(44ページ)を参照してください。

ローカルインストール

お使いの環境にUNIX用のインストールサーバーがない場合は、HP-UX用またはSolaris/Linux用インストールDVD-ROMを使用して、ローカルインストールを行う必要があります。この手順については、「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)を参照してください。

リモートインストール

Tru64クライアントソフトウェアは、Data Protectorグラフィカルユーザーインタフェースを使ってUNIX用のインストールサーバーからリモートにインストールできます。ソフトウェアのリモートインストール手順は、「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

クライアントコンポーネントのインストールが完了したターゲットシステムは、自動的にData Protectorセルに追加されます。

Tru64クラスター

すべてのターゲットシステムに対するrootパーミッションが必要です。

Data Protectorは、Tru64クラスターの共有ディスクにローカルまたはリモートにインストールする必要があります。インストールを実行するには、クラスターノードのいずれかを使用します。

Install後、クラスター仮想ホスト名および個々のノードをData Protectorセルにインポートする必要があります。詳細な手順については、「セルへのクラスター対応クライアントのインポート」(217ページ)を参照してください。

Tru64クライアントへのバックアップデバイスの接続

Tru64クライアントにMedia Agentをインストールした後は、以下の作業を実施してください。

1. コンピュータをシャットダウンし、バックアップデバイスをSCSIバスに接続します。

   注記：

   バックアップデバイスをハードディスクドライブと同じSCSIバスに接続することは、お勧めしません。

   バックアップデバイス用に選択したSCSIアドレスが、他のデバイスに使用されていないことを確認します。

   サポート対象のデバイスの詳細は、http://www.hp.com/support/manualsを参照してください。

2. コンピュータの電源を投入し、ブート処理が完了するまで待ちます。新しいバックアップデバイスがシステムによって正しく認識されていることを確認します。

この次に行う作業

Install手順が完了し、バックアップデバイスが正しくTru64システムに接続されたら、オンラインヘルプの索引「構成、バックアップデバイス」を参照して、バックアップデバイス、メディアプール、またはData Protectorのその他の構成タスクの詳細を確認してください。

SCOクライアントのインストール

SCOクライアントは、HP-UX用またはSolaris/Linux用インストールDVD-ROMを使ってローカルにインストールすることも、UNIX用のインストールサーバーを使ってリモートインストールすることもできます。

なお、UnixWareでは、リモートインストールができません。

Install手順を開始する前に、どのコンポーネントをクライアントシステムにインストールするかを決定しておいてください。Data Protectorソフトウェアコンポーネントのリストと説明は、「Data Protectorコンポーネント」(76ページ)を参照してください。

前提条件

- システム要件、ディスクスペース要件、サポートされているプラットフォームとData Protectorコンポーネントについては、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- この時点で、Cell ManagerおよびUNIX用のインストールサーバーをネットワーク上にインストールしておく必要があります。この手順については、「Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール」(44ページ)を参照してください。

ローカルインストール

お使いの環境にUNIX用のインストールサーバーがない場合は、HP-UX用またはSolaris/Linux用インストールDVD-ROMを使用して、ローカルインストールを行う必要があります。この手順については、「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)を参照してください。

リモートインストール

SCOクライアントソフトウェアは、Data Protectorグラフィカルユーザーインタフェースを使ってUNIX用のインストールサーバーからリモートにインストールできます。ソフトウェアのリモートインストール手順は、「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

クライアントコンポーネントのインストールが完了したターゲットシステムは、自動的にData Protectorセルに追加されます。

SCOシステムへのバックアップデバイスの接続

SCOクライアントシステムにMedia Agentコンポーネントをインストールした後は、以下の手順に従って、システムにバックアップデバイスを接続してください。

1. `/etc/conf/cf.d/mscsi`ファイルをチェックして、利用可能なSCSIアドレスを調べます。このファイルには、現在接続されているSCSIデバイスのリストが示されます。

   サポート対象のデバイスの詳細とデバイスのマニュアルは、http://www.hp.com/support/manualsを参照してください。

2. コンピュータをシャットダウンし、バックアップデバイスをSCSIバスに接続します。
3. コンピュータを再起動します。

4. mkdev tapeコマンドを使用してデバイスを構成します。テープドライブデバイスのリストからGeneric SCSI-1 / SCSI-2 tape driveを選択します。

注記:

UNIT IDは、mkdev tapeコマンドの実行時に表示されます。デバイスファイル名を認識するには、このIDが必要となります。

5. デバイスを構成し、システムを再起動した後、/etc/conf/cf.d/mscsiファイルをチェックし、デバイスが正しく接続されていることを確認します。
6. /devディレクトリから、適切なデバイスファイル名を選択します。

   名前の末尾にデバイスのUNIT IDを付けます。UNIT IDを#とすると、nrStp#のように指定してください。デバイスのUNIT IDは、手順ステップ 4(121ページ)で定義されています。図22(122ページ)では、デバイスファイル/dev/nrStp#を例に、デバイスファイル名について説明しています。

注意:

可変長ブロックサイズの非巻き戻しデバイスファイルのみを使用してください。tape -s getblk /dev/nrStp#コマンドを使って、可変長ブロックサイズを確認してください。可変長ブロックサイズの値は0にする必要があります。値が0でない場合、tape -a 0 setblk /dev/nrStp#コマンドを使用してブロックサイズの値を0に設定してください。

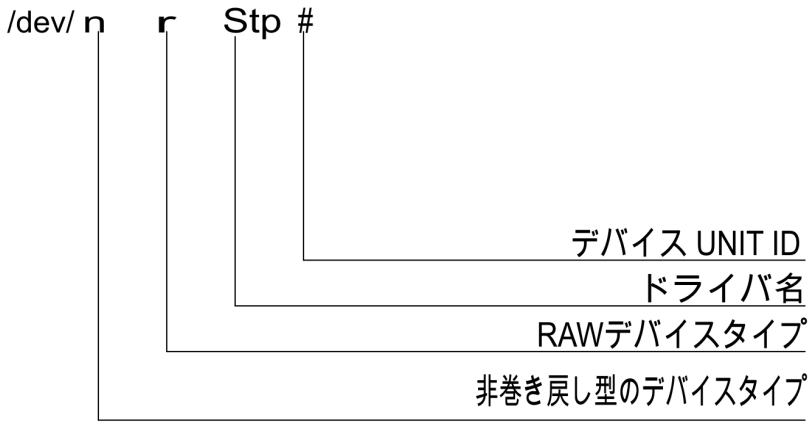


図 22 デバイスファイル名の形式

この次に行う作業

Install手順が完了し、バックアップデバイスが正しくSCOクライアントシステムに接続されたら、オンラインヘルプの索引「構成、バックアップデバイス」を参照して、バックアップデバイスおよびメディアプール、またはその他の構成タスクの詳細を確認してください。

ADIC/GRAUライブラリ用またはStorageTekライブラリ用のMedia Agentのインストール

Data Protectorには、専用のADIC/GRAUとStorageTek ACSライブラリが用意されています。ポリシーは、Data Protectorバックアップデバイスとしてのの ADIC/GRAUライブラリまたはStorageTek ACSライブラリの構成に使用されます。ADIC/GRAUライブラリ内またはStorageTekライブラリ内のドライブに物理的に接続されるすべてのシステムに、Data Protector Media Agent (General Media AgentまたはNDMP Media Agent)をインストールする必要があります。また、マルチホスト構成の場合は、ADIC/GRAUライブラリまたはStorageTekライブラリのロボティクスを制御するシステムにも、Data Protector Media Agentをインストールする必要があります。なお、マルチホスト構成とは、ライブラリとドライブが互いに別のコンピュータに接続される構成を意味します。

ADIC/GRAUライブラリでは、Media Agentソフトウェアがインストールされ、GRAU/ADIC DAS Serverを介し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。**STK ACS用統合ソフトウェアでは、Media Agentソフトウェアがインストールされ、STK ACS Serverを介し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、**ACSクライアントと呼ばれます。**

注記：

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。詳細は、第5章（309ページ）を参照してください。

ライブラリドライブの接続

Media Agentソフトウェアのインストール先のシステムにライブラリドライブを物理的に接続します。

サポート対象のADIC/GRAUまたはSTKライブラリの詳細は、http://www.hp.com/support/manualsを参照してください。

バックアップデバイスをシステムに物理的に接続する方法は、「HP-UXクライアントのインストール」（99ページ）を参照してください。また、ADIC/GRAUライブラリまたはStorageTekライブラリのマニュアルも参照してください。

バックアップデバイスをサポート対象のWindowsシステムに物理的に接続する方法は、「Windows用クライアントのインストール」（92ページ）を参照してください。また、ADIC/GRAUライブラリまたはStorageTekライブラリのマニュアルも参照してください。

ADIC/GRAUライブラリを使用するData Protectorクライアントの準備作業

Media Agentソフトウェアをインストールする前に、以下の手順でADIC/GRAUライブラリを構成してください。

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上のC:¥DAS¥ETC¥CONFIGファイルを作成または更新してください。このファイルには、すべてのDASクライアントを定義する必要があります。Data Protectorの場合は、ライブラリロボティクスを制御することが可能な各Data Protectorクライアントをファイルに定義する必要があります。

   各DASクライアントは、たとえばDP_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。C:¥DAS¥ETC¥CONFIGファイルには、たとえば、以下のようなリストを記述します。

   ```
   client client_name = DP_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))
   ```

2. ADIC/GRAU DASライブラリロボティクスへのアクセスを必要とするData Protector Media Agentがインストールされた各Data Protectorクライアント上で、omnircファイル(Windowsの場合はData_Protector_home¥omnircファイル、HP-UXおよびSolarisの場合は/opt/omni/.omnircファイル、AIXの場合は/usr/omni/omnircファイル)を開いて以下の変数を設定します。

DAS_CLIENT	DASサーバー上に定義される一意なGRAUクライアント名です。たとえば、クライアントの名前が“DP_C1”の場合、omnircファイルの該当する行はDAS_CLIENT=DP_C1です。
DAS_SERVER	DASサーバー名です。

3. ADIC/GRAUライブラリスロットの割り当て方針には、静的な割り当てと動的な割り当ての2種類があるため、現在、そのどちらの方針が適用されているかを確認する必要があります。割り当て方針の種類をチェックする方法は、『*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。静的方針の場合は、以下のようなData Protectorの構成作業が必要です。

   静的割り当て方針が設定されている場合は、ライブラリのロボティクスを制御するシステムに、以下のomnirc変数を追加する必要があります。

   OB2_ACIEJECTTOTAL = 0

注記:

これは、HP-UXおよびWindowsに当てはまります。

ADIC/GRAUライブラリの構成に関して、さらに詳しい情報が必要な場合は、最寄りのADIC/GRAUサポートに問い合わせるか、ADIC/GRAUのマニュアルなどを参照してください。

ADIC/GRAUライブラリ用のMedia Agentのインストール

前提条件

Media Agentをインストールするシステムは、以下の条件を満たしている必要があります。

- ADIC/GRAUライブラリが構成済みで、実行されていること。ADIC/GRAUライブラリのマニュアルを参照してください。

- Data Protectorのインストールと構成が完了していること。この章の「Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール」(44ページ)を参照してください。
- DASサーバーが実行されていること。

  ADIC/GRAUライブラリを制御するには、DASクライアントソフトウェアが必要です。各DASクライアントには、DASクライアントソフトウェアをインストールする必要があります。Data Protectorからメディアおよびデバイスに対して開始されたアクションは、DASクライアントを介してDASサーバーに送信されます。さらに、ADIC/GRAUライブラリ内で、ロボティクスの制御と、メディアの移動またはロードを受け持つ部分(AMU - AML Management Unit)に渡されます。アクションが完了すると、DASサーバーがDASクライアントに応答を返します。ADIC/GRAUライブラリのマニュアルを参照してください。

- Media Agentをインストールする前に、以下の情報を用意しておく必要があります。
  - DAS Server (OS/2上で実行されるアプリケーション)のホスト名。
  - 対応するDAS名とともにドライブを示すリスト。取得されたドライブ名は、Data ProtectorにADIC/GRAUドライブを構成する際に使用されます。

    ADIC/GRAUシステムに対してDASクライアントがすでに定義されている場合は、以下のいずれかのdasadminコマンドでこのリストを取得できます。

    ```
    dasadmin listd2 client
    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、OS/2ホスト上のC:¥DAS¥BINディレクトリから実行できます。他のシステムにインストールした場合は、DASクライアントソフトウェアがインストールされているディレクトリから実行できます。UNIXクライアントシステムの場合、通常、このディレクトリは/usr/local/aci/binシステムディレクトリとなります。

  - 利用可能な挿入/取り出しエリア、および、対応するフォーマット仕様のリスト。

    OS/2ホスト上のAMSのグラフィカル構成(AML Management Software)では、以下の手順で、利用可能な挿入/取り出しエリアのリストを取得できます。

    1. [Admin] - [Configuration]メニューをクリックして、この構成を起動します。

2. [I/O unit]アイコンをダブルクリックして[EIF-Configuration]ウィンドウを開き、[Logical Ranges]フィールドをクリックします。このテキストボックスに、利用可能な挿入/取り出しエリアのリストが表示されます。

注記:

1つのData Protectorライブラリデバイスでは、1つのメディアタイプのみ処理できます。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。

- ドライブに対応するUNIXデバイスファイルのリスト — Media AgentをUNIXシステムにインストールする場合。

  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。

  UNIXデバイスファイルの詳細は、「HP-UXシステムへのバックアップデバイスの接続」(102ページ)を参照してください。

- ドライブに対応するSCSIアドレスのリスト — Media AgentをWindowsシステムにインストールする場合。たとえば、`scsi4:0:1:0`のようなアドレスです。

  SCSIアドレスの詳細は、「Windowsシステムへのバックアップデバイスの接続」(97ページ)を参照してください。

設置

Install手順は以下のとおりです。

1. Data Protectorグラフィカルユーザーインタフェースとインストールサーバーを使って、クライアントにMedia Agentコンポーネントを配布します。この章の「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

2. ADIC/GRAUライブラリをインストールします。

- Windowsシステムでは、以下の操作を行ってください。
  a. 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。
  b. この3つのファイルは、%SystemRoot%¥system32ディレクトリにもコピーしてください。
  c. 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。(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。インストールメディアに記載されています。
  d. コントロールパネルの[管理ツール] - [サービス]から、portinstを起動してportmapperをインストールします。portmapperサービスを実行するには、DASクライアントを再起動する必要があります。
  e. システムを再ブートした後、portmapperサービスとrpcサービスがともに実行されているか確認します(コントロールパネルの**[管理ツール]-[サービス]**で、これらのサービスの状態を確認します)。
- HP-UXシステムの場合は、共有ライブラリlibaci.slを/opt/omni/libディレクトリにコピーします。このディレクトリにアクセスするには、適切なパーミッションが必要です。すべてのユーザー(rootとそのユーザーグループ、およびその他[others])に対する読み取りパーミッションと実行パーミッションが共有ライブラリに設定されていることを確認してください。libaci.sl共有ライブラリは、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に含まれています。
- AIXシステムの場合は、共有ライブラリlibaci.oを/usr/omni/libディレクトリにコピーします。このディレクトリにアクセスするには、適切なパーミッションが必要です。すべてのユーザー(rootとそのユーザーグループ、およびその他[others])に対する読み取りパーミッションと実行パーミッションが共有ライブラリに設定されていることを確認してください。libaci.o共有ライブラリは、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に含まれています。

この時点で、ハードウェアが正しく接続されており、DASソフトウェアが適切にインストールされている必要があります。

次のコマンドを実行して、ライブラリドライブがシステムに正しく接続されているかどうかをチェックします。

Windowsシステムの場合: Data_Protector_home¥bin¥devbra -dev

HP-UXシステムの場合: /opt/omni/lbin/devbra -dev

AIXシステムの場合: /usr/omni/bin/devbra -dev

ライブラリデバイスが正しく接続されていれば、ライブラリデバイスおよび対応するデバイスファイルがリストに表示されます。

この次に行う作業

Media Agentがインストールされ、ADIC/GRAUライブラリが物理的にシステムに接続されたら、オンラインヘルプの索引「構成、バックアップデバイス」を参照して、その他の構成タスク(バックアップデバイスやメディアプールの構成など)の詳細を確認してください。

StorageTekライブラリを使用するData Protectorクライアントの準備作業

Media Agentをインストールするシステムは、以下の条件を満たしている必要があります。

- StorageTekライブラリが構成済みで、実行されていること。StorageTekライブラリのマニュアルを参照してください。
- Data Protectorのインストールと構成が完了していること。「Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール」(44ページ)を参照してください。
- Media Agentソフトウェアをインストールする前に、以下の情報を用意しておく必要があります。
  - ACSLSを実行するホストのホスト名。
  - Data Protectorで使用するACSドライブIDのリスト。取得されたドライブIDは、Data ProtectorにStorageTekドライブを構成する際に使用されます。このリストを表示するには、ACSLSを実行しているホストにログインし、以下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、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、以下のように定義されていなければなりません。

    ACS DRIVE:ID:#,#,#,# - (ACS num, LSM num, PANEL, DRIVE)
  - 利用可能なACS CAP IDのリストとACS CAPフォーマットの仕様。このリストを表示するには、ACSLSを実行しているホストにログインし、以下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、以下のように定義されていなければなりません。

ACS CAP:ID:#,#,# - (ACS num, LSM num, CAP num)

- ドライブに対応するUNIXデバイスファイルのリスト — Media AgentをUNIXシステムにインストールする場合。

  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。

  UNIXデバイスファイルの詳細は、「HP-UXシステムへのバックアップデバイスの接続」(102ページ)を参照してください。

- ドライブに対応するSCSIアドレスのリスト — Media AgentをWindowsシステムにインストールする場合。たとえば、scsi4:0:1:0のようなアドレスです。

  SCSIアドレスの詳細は、「Windowsシステムへのバックアップデバイスの接続」(97ページ)を参照してください。

- Data Protectorで使用するドライブがオンライン状態になっていることを確認します。ドライブがオンライン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
- Data Protectorに使用するCAPがオンライン状態になっており、動作モードが手動になっていることを確認します。

  CAPがオンライン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が手動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

StorageTekライブラリ用のMedia Agentのインストール

Install手順は以下のとおりです。

1. Data Protectorグラフィカルユーザーインタフェースと UNIX用インストールサーバーを使って、クライアントにMedia Agentコンポーネントを配布します。この章の「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

2. 以下に示すように、各ACSクライアントでACSのssiデーモンを起動します。
   - HP-UXとSolarisのACSクライアントの場合は、以下のコマンドを実行します。

     /opt/omni/acs/ssi.sh start ACS_LS_hostname
   - Windows ACSクライアントの場合は、LibAttachサービスをインストールします。詳細は、ACSのマニュアル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、システムを再ブートすると、必ずこのサービスが自動的に開始されます。
   - AIX ACSクライアントの場合は、以下のコマンドを実行します。

     /usr/omni/acs/ssi.sh start ACS_LS_hostname

注記:

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、手作業で追加してください。

LibAttachサービスの詳細は、StorageTekライブラリのマニュアルを参照してください。

3. 次のコマンドを実行して、ライブラリドライブがシステムに正しく接続されているかどうかをチェックします。
   - HP-UX、Solaris、およびLinux ACSクライアントの場合: /opt/omni/lbin/devbra -dev
   - Windows ACSクライアントの場合: Data_Protector_home¥bin¥devbra -dev
   - AIX ACSクライアントの場合: /usr/omni/bin/devbra -dev

   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。

この次に行う作業

Media Agentがインストールされ、StorageTekライブラリが物理的にシステムに接続されたら、オンラインヘルプの索引「構成、バックアップデバイス」を参照して、バックアップデバイスおよびメディアプールの構成などのその他の構成タスクの詳細を確認してください。

Novell NetWareクライアントのローカルインストール

Novell NetWareクライアントのインストールは、Novellネットワークに接続されているサポート対象のWindowsシステムから行わなければなりません。

Data Protector Disk AgentおよびGeneral Media Agentは、Novell NetWareを実行しているシステムにインストールすることができます。Data Protectorコンポーネントの詳細は、「Data Protectorコンポーネント」(76ページ)を参照してください。

サポート対象のデバイスやNovell NetWareプラットフォームバージョンの詳細、これまでに報告されている問題とその解決策については、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。

前提条件

Novell NetWareプラットフォームにData Protectorをインストールする前に、以下の条件が満たされていることを確認してください。

- システム要件、ディスクスペース要件、サポートされているプラットフォームとData Protectorコンポーネントについては、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- TCP/IPプロトコルがインストールされており、正しく動作していること。
- Windowsシステム上で、以下のサービスのいずれかが実行されていることを確認してください。
  - Novell NetWare用のGateway Service。

    このサービスは、Windows Serverからインストールを行うときに、Windows上で実行されている必要があります。
  - Windows用のNovell Client、またはNetWare用のMicrosoft Client Service。

    このサービスは、Windowsワークステーションからインストールを行うときに、Windows上で実行されている必要があります。
- Windowsシステムから、ターゲットのNetWareサーバー(または適切なNDS/eDirectoryツリー)にログインします。
- ターゲットのNetWareサーバーのSYSボリュームにスーパバイザ権限があることを確認してください。
- Windowsシステム上に、利用可能なローカルデバイス名が少なくとも1つあることを確認してください。

クラスター対応クライアント

クラスター対応クライアントをインストールする場合は、上記以外にも必要となる前提条件があります。詳細は、「クラスター対応クライアントのインストール」(208ページ)を参照してください。

設置

このインストール手順は、Data ProtectorのWindows用DVD-ROMから実行できます。Novell NetWareのインストールは、インストールサーバーからは実行できない点に注意してください。

Novell NetWareサーバーにData Protectorをインストールするには、以下の手順に従ってください。

1. Windowsシステム上でコマンドプロンプトを実行して、現在のパスをDVD-ROMのルートディレクトリに変更します。

2. Installスクリプトを実行します。

Data Protector Novell NetWareクライアントをインストールするには、現在のパスをNetWareディレクトリに変更して次のように入力します。

NWInstall target server name ALL|DA|MA *port_number*

2番目のパラメータは、Data Protector Novell Clientのどの機能をインストールするかを定義します。

- すべてのData Protector Novell NetWareクライアント機能をインストールするには、ALLと入力します。
- Novell NetWare用のData Protector Disk Agentのみインストールする場合は、DAと入力します。
- Novell NetWare用のData Protector General Media Agentのみインストールする場合は、MAと入力します。

注記:

Novell NetWareにData Protectorをインストールする場合、Novell NetWareのバージョンに関わらず、ポート番号は任意に指定できます。番号を指定しなければ、デフォルトのポート番号5555が使われます。

Data Protectorでサポートされていない Novell NetWare OSのバージョンを使用している場合、インストールは可能ですが警告が表示されます。

Installを行う段階で、ターゲットサーバーにすでにData Protectorファイルが存在するかどうかが確認されます。ファイルがすでに存在する場合、すでにインストールされているData Protectorは、SYS:¥usr¥Omni.oldディレクトリに移されます。

インストールされているNetWareクライアントのバージョンに応じて、サーバー上でOMNIINET.NLM、HPINET.NLMまたはHPBRAND.NLMが実行されていないか確認します。いずれかが実行されている場合は、Novell NetWareコンソールから以下のコマンドを実行してモジュールをアンロードしてください。

UNLOAD HPINET (UNLOAD OMNIINET / UNLOAD HPBRAND)

Installを行うと、自動的にData Protectorのディレクトリ構造が作成され、ターゲットサーバーにData Protectorのすべてのファイルがコピーされます。

3. 以下のモジュールがシステムにロードされていることを確認してください。
   - NETDB.NLM
   - TSAFS.NLM
   - TSANDS.NLM

   上記のモジュールによって、ローダーは、HPINET.NLMをロードする際に、パブリックシンボルを解決できます。

   Novell NetWare 6.xシステム上にNovell NetWare Cluster Servicesが構成されている場合は、NCSSDK.NLMモジュールがロードされていることを確認してください。

4. HPINET.NLMをロードするには、Novell NetWareコンソールで以下のコマンドを入力します。

   SEARCH ADD SYS:USR¥OMNI¥BIN

   LOAD HPINET.NLM

注記:

デフォルトのポート番号5555を使用しない場合は、-port *port_number*オプションを追加してLOADコマンドを実行し、ポート番号を指定します。たとえば、次のように入力してください。

LOAD HPINET.NLM -port *port_number*

Novell NetWareのインストールを行うと、Novell NetWareサーバーが自動的にData Protector Cell Managerを認識できるように、AUTOEXEC.NCFファイルに自動的に上記のコンソールコマンドが追加されます。これにより、HPINET.NLMファイルが常にロードされ、Novell NetWareサーバーがいつでも Data Protector Cell Managerに接続できる状態になります。

注記:

Installが完了したら、AUTOEXEC.NCFファイルを確認してください。必要なコンソールコマンドがAUTOEXEC.NCFファイルに追加されていない場合は、手作業で追加してください。

NDS/eDirectoryデータベースのバックアップと復元を可能にするには、以下の手順を行ってください。

1. NDS/eDirectoryのバックアップと復元の実行時に使用するユーザーアカウントを定義します。
2. Novell NetWareコンソールから、HPLOGIN.NLMモジュールをロードします。

   LOAD HPLOGIN.NLM

3. NDS/eDirectoryデータベースにログインできるように、以下のユーザー情報をHPLOGIN.NLMファイルに追加します。

- NDS/eDirectoryコンテキスト:

  ユーザーオブジェクトが格納されているコンテナを指定します。コンテナ名は、完全修飾名構文として指定する必要があります。たとえば、次のように入力してください。

  OU=SDM.O=MYDOMAIN

- NDS/eDirectoryオブジェクト名:

  これは、Data Protector Disk AgentがNDS/eDirectoryのバックアップ/復元を実行する際に、正規のNDS/eDirectoryユーザーがNDS/eDirectoryデータベースへのログインに使用するユーザーオブジェクトの共通名です。この正規のNDSユーザーは、前述のコンテキスト内に記述されている必要があります。たとえば、次のように入力してください。

  CN=MarcJ

  選択したユーザーの完全修飾名は、.CN=MarcJ.OU=SDM.O=MYDOMAINとなります。

- NDS/eDirectoryオブジェクトパスワード:

  正規のユーザーパスワードは、NDS/eDirectoryデータベースへログインする際、またはNDS/eDirectoryデータベースのバックアップや復元を開始する際に、ユーザー名とともに使用します。

  HPLOGINモジュールに入力されたユーザー情報は暗号化され、SYS:SYSTEMディレクトリに保存されます。Novell NetWare SMSモジュールのロードにも、パスワードが使用されます。

注記:

HPLOGINモジュールで選択するユーザーアカウントには、NDS/eDirectoryデータベースのバックアップと復元を実行するためのパーミッションがなければなりません。

NDS/eDirectoryユーザーオブジェクトに対して変更を行った場合(別のコンテナへの移動、削除、名前の変更、パスワードの変更)、SYS:SYSTEMディレクトリで暗号化されている情報をHPLOGINモジュール内で更新する必要があります。

4. Novell NetWare Storage Management Services (SMS)でNDS/eDirectoryをバックアップおよび復元するには、NDS/eDirectoryツリー内の1つ以上のサーバー上にSMDR.NLMモジュールおよびTSANDS.NLMモジュールをロードする必要があります。TSANDS.NLMとSMDR.NLMの最新バージョンは、Webページhttp://support.novell.com/filefinder/からダウンロードできます。

   Installが完了すると、LOAD TSANDS.NLM行がAUTOEXEC.NCFファイルに追加されます。これにより、Novell NetWareサーバーは、TSANDS.NLMをすぐに認識できるようになります。Novell NetWareのSMSモジュールのSMDR.NLMは、TSANDS.NLMがロードされるとすぐにロードされます。

注記:

Install後、コンソールコマンドがAUTOEXEC.NCFファイルに追加されていなければ、手作業で追加してください。

ヒント:

バックアッププロセス中のネットワーク負荷を最小限にするには、最大のNDS/eDirectoryパーティションのレプリカを含むサーバー上にモジュールをロードします。

以上で、NDS/eDirectoryのバックアップおよび復元の要件を満たしたことになります。オンラインヘルプの索引「構成」を参照して、その他の構成タスクの手順についてご確認ください。

Media Agentの構成

この時点で、Data Protectorコンポーネントはすべてインストールされています。ただし、インストールの始めの段階でALLまたはMAパラメータを選択している場合は、Data Protector General Media AgentがNovell NetWareサーバーに接続されているバックアップデバイスを使用するための追加の構成作業が必要です。

Data Protectorでは、Adaptec SCSIホストアダプタコントローラとそれに対する.HAMドライバがサポートされています。Data Protector Media Agentは、.HAMドライバと直接通信して、SCSIホストアダプタにアクセスできます。そのため、SCSIホストアダプタドライバをインストールしておく必要があります。Adaptecドライバの最新バージョンは、http://www.adaptec.comからダウンロードできます。

STARTUP.NCFファイルにLOADコマンドが追加されていれば、サーバーが再起動時されるたびにドライバが自動的にロードされます。このコマンドには、ドライバのロケーション、使用可能なオプション、およびスロット番号を指定しなければなりません。使用可能なオプ

ションのリストとスロット番号の計算については、『*Adaptec Driver User's Guide*』を参照してください。

例

サーバーが再起動されるたびにAHA-2940 AdaptecドライバがNovell NetWare 6.xサーバーに自動的にロードされるようにするには、STARTUP.NCFファイルに次の行を追加します。

```
SET RESERVED BUFFERS BELOW 16 MEG=200
LOAD AHA2940.HAM SLOT=4 lun_enable=03
```

SLOTには、ホストアダプタデバイスが格納されているスロット番号を指定します。また、lun_enableは、すべてのターゲット上で特定のLUN(論理ユニット番号)をスキャンするマスクを指定します。

各LUNをすべてのSCSIアドレスに対してスキャンするには、そのLUNに対応するビットを1に設定します。上の例ではlun_enable=03と指定していますが、この場合、LUN 0およびLUN 1がすべてのターゲット上でスキャンされます。

注記:

lun_enableは、SCSI LUNが0より大きいデバイスを使用する場合にのみ指定する必要があります。たとえば、HP StorageWorks 12000eテープライブラリデバイスを構成する場合などです。

ヒント:

サーバーが再起動されるたびに、Novell NetWareサーバーに接続されたすべてのデバイスとそのLUNを自動的にスキャンするには、AUTOEXEC.NCFファイルに次の行を追加します。

```
SCAN FOR NEW DEVICES
SCAN ALL LUNS
```

以上で、General Media Agentの構成が完了します。

この次に行う作業

Novell NetWareプラットフォームにGeneral Media Agentソフトウェアをインストールした後は、Data Protector General Media Agentのインストール状態をチェックすることをお勧め

します。「Novell NetWare上にインストールしたGeneral Media Agentのチェック」(431ページ)を参照してください。

Install状態を確認したら、Novell NetWareクライアントをData Protectorグラフィカルユーザーインタフェースを使ってData Protectorセルにインポートします。オンラインヘルプの索引「Novell NetWare」を参照して、その他の構成タスクの詳細をご確認ください。

HP OpenVMSクライアントのローカルインストール

OpenVMSクライアントのインストール手順は、サポートされているOpenVMSシステムでローカルに行う必要があります。リモートインストールはサポートされていません。

Data Protector Disk Agent、General Media Agent、およびそのユーザーインタフェース(コマンドラインインタフェースのみ)は、OpenVMS 7.3-2/IA64 8.2-1を実行しているシステムにインストールできます。また、Oracle Integrationコンポーネントは、OpenVMS 7.3-2以上を実行しているシステムにインストールできます。Data Protectorコンポーネントの詳細は、「Data Protectorコンポーネント」(76ページ)を参照してください。

サポートされているデバイス、OpenVMSプラットフォームのバージョン、制限事項、既知の問題および回避策の詳細は、*HP Data Protector製品案内*、*ソフトウェアノート*、*リファレンス*を参照してください。

OpenVMS固有の詳細情報については、SYS$COMMON:[SYSHLP]DPA0611.RELEASE_NOTESなど、OpenVMSのデフォルトのヘルプドキュメントのディレクトリにある*OpenVMSリリースノート*を参照してください。

前提条件

OpenVMSプラットフォームにData Protectorクライアントをインストールする前に、以下を確認してください。

- HP TCP/IPトランスポートプロトコルがインストールおよび実行されていること。
- SYS$MANAGER:UTC$TIME_SETUP.COMコマンドで、システムのTIMEZONEが設定されていること。
- OpenVMSシステムのSYSTEMアカウントにログインしていること。適切なパーミッションが必要であることに注意してください。
- クライアントのインストールパッケージを収録したData ProtectorのインストールDVD-ROMにアクセスできること。

設置

このインストール手順は、Data ProtectorのWindows用インストールDVD-ROMから実行できます。OpenVMSインストールは、インストールサーバーの機能の一部ではないことに注意してください。

OpenVMSシステムにData Protectorクライアントをインストールするには、以下の手順に従ってください。

1. PCSIインストールファイルがすでにある場合は、手順ステップ 2(140ページ)に進みます。PCSIインストールファイルを取得するには、OpenVMSサーバー上のインストールDVDをマウントして、あて先ロケーションにコピーしてください。WindowsシステムからPCSIファイルをFTPで取得することもできます。

2. 次のコマンドを実行します。

   ```
   $ PRODUCT INSTALL DP /SOURCE=device:[directory]
   ```

   device:[directory]は、.PCSIインストールファイルがある場所です。

3. プロンプトにYESと応答して、キットのバージョンを確認します。

   ```
   The following product has been selected:HP AXPVMS DP A06.20-xx Layered
   Product Do you want to continue?[YES]
   ```

4. Installするソフトウェアコンポーネントを選択します。デフォルトでは、Disk Agent、General Media Agent、およびユーザーインタフェースがインストールされます。各コンポーネントを個別に選択することもできます。

   選択した製品がインストールされるほか、ソフトウェアの依存関係を満たすために必要な製品もインストールされます。これらの製品に関するオプションを選択するように促すプロンプトが表示されます。

例

```
HP IA64VMS DP A06.20-xx:HP OpenVMS IA64 Data Protector V6.20

COPYRIGHT HEWLETT-PACKARD COMPANY 2010

Do you want the defaults for all options?[YES] NO

Do you wish to install Disk Agent for this client node?

[YES] YES

Do you wish to install Media Agent for this client node?

[YES] YES

Do you wish to install Command Language Interface for this client
node?

[YES] YES
```

Do you wish to install Oracle Integration Agent for this client node?

[YES] YES

Do you want to review the options?

[NO] YES

HP IA64VMS DP X06.20-xx:HP OpenVMS IA64 Data Protector V6.20 [Installed]

Do you wish to install Disk Agent for this client node?

YES

Do you wish to install Media Agent for this client node?

YES

Do you wish to install Command Language Interface for this client node?

YES

Do you wish to install Oracle Integration Agent for this client node?

[YES] YES

Are you satisfied with these options?

[YES] YES

Data Protectorディレクトリとファイルのデフォルト位置は、以下のとおりです。

SYS$SYSDEVICE:[VMS$COMMON.OMNI]

ディレクトリ構造は自動的に作成され、ファイルはこのディレクトリツリー内に格納されます。

Data Protectorの起動コマンドプロシジャおよびシャットダウンコマンドプロシジャは、以下のディレクトリに格納されます。

SYS$SYSDEVICE:[VMS$COMMON.SYS$STARTUP]

このディレクトリには、OpenVMSクライアントに常に表示される4つのファイルと、CLIオプションを選択した場合にのみ存在する5つ目のファイルがあります。これら5つのファイルを以下に示します。

- SYS$STARTUP:OMNI$STARTUP.COMノード上でData Protectorを起動するためのコマンドプロシジャです。
- SYS$STARTUP:OMNI$SYSTARTUP.COMOMNI$ROOTの論理名を定義するためのコマンドプロシジャです。このクライアントに必要な他の論理名も、このコマンドプロシジャに追加できます。
- SYS$STARTUP:OMNI$SHUTDOWN.COMノード上でData Protectorをシャットダウンするためのコマンドプロシジャです。
- OMNI$ROOT:[BIN]OMNI$STARTUP_INET.COMTCP/IP INETプロセスを起動するのに使用するコマンドプロシジャです。その後、Cell Managerにより送信されたコマンドが実行されます。
- OMNI$ROOT:[BIN]OMNI$CLI_SETUP.COMData Protector CLIの起動に必要なシンボルを定義するためのコマンドプロシジャです。インストール中にCLIオプションが選択された場合のみ、システム上に存在します。

  CLIを使用するすべてのユーザに対して、login.comプロシジャからこのコマンドプロシジャを実行してください。このプロシジャには、CLIコマンドを正しく実行するために必要ないくつかの論理名が定義されています。

5. SYS$MANAGER:SYSTARTUP_VMS.COMに以下の行を挿入します。

   @sys$startup:omni$startup.com

6. SYS$MANAGER:SYSHUTDWN.COMに以下の行を挿入します。

   @sys$startup:omni$shutdown.com

7. OpenVMSクライアントから、Cell Managerの可能なすべてのTCP/IPのエイリアスに接続できることを確認してください。
8. 「セルへのクライアントのインポート」(213ページ)で説明されているように、Data Protectorのグラフィカルユーザーインタフェースを使用して、OpenVMSクライアントをData Protectorのセルにインポートします。

OMNIADMINという名前のアカウントがインストール中に作成されます。OMNIサービスは、このアカウントの下で実行されます。

このアカウントのログインディレクトリはOMNI$ROOT:[LOG]で、ここにOMNI$STARTUP_INET.LOGというログファイルがData Protectorコンポーネントの起動ごとに作成されます。このログファイルには、要求を実行しているプロセスの名前、使用されているData Protectorイメージの名前、要求のオプションが記録されます。

予期しないエラーは、すべてこのディレクトリのDEBUG.LOGファイルに記録されます。

注記:

OpenVMS 8.3以降では、Data Protectorインストールで次のメッセージが表示されます。

%PCSI-I-CANNOTVAL, cannot validate [PATH]HP-AXPVMS-DP-A0611

-XXX-1.PCSI;1 -PCSI-I-NOTSIGNED, product kit

is not signed and therefore has no manifest file

警告が表示されないようにするには、製品のインストールコマンドに/OPTION=NOVALIDATE_KIT**を指定します。**

クラスター環境でのインストール

共用システムディスクを使用する場合、クライアントソフトウェアのインストールが一度のみ必要になります。ただし、OMNI$STARTUP.COMプロシジャは、Data Protectorクライアントとして使用する各ノードで実行する必要があります。共用システムディスクを使用しない場合、クライアントソフトウェアは各クライアントにインストールする必要があります。

クラスターのTCP/IPエイリアス名を使用する場合で、クラスターの共用システムディスクを使用する場合、クライアントのエイリアス名も定義できます。エイリアスクライアントを定義すれば、個々のクライアントノードで構成作業を行う必要はありません。クライアント定義かエイリアス定義のいずれかを選択し、クラスター内でバックアップや復元の作業を実行できます。使用する構成によって、テープデバイスやテープライブラリに対する直接パスを、保存や復元に使用できる場合と、使用できない場合があります。

Disk Agentの構成

OpenVMSのData Protector Disk Agentは、マウントされたFILES-11 ODS-2およびODS-5のディスクボリュームをサポートしています。OpenVMS Disk Agentを構成する必要はありません。ただし、Disk Agentを使用するバックアップ仕様の作成時には、いくつか留意点があります。以下に留意点を示します

- GUIに入力される、またはCLIに受け渡されるファイル仕様の構文は、UNIXスタイルである必要があります。以下に例を示します。

  /disk/directory1/directory2/.../filename.ext.n

  - 文字列はスラッシュ(/)で始め、その後にディスク、ディレクトリ、ファイル名をスラッシュで区切って記述します。
  - 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仕様は、ODS-5ディスクに常駐するファイル以外は大文字小文字を区別しません。

例

OpenVMSのファイル仕様

1DGA100:[USERS.DOE]LOGIN.COM;1

Data Protectorでは、以下の形式で指定する必要があります。

/1DGA100/USERS/DOE/LOGIN.COM.1

注記:

暗黙に使用されるバージョン番号はありません。バージョン番号は必ず指定する必要があり、バックアップ対象として指定されたファイルバージョンのみがバックアップされます。

一部のオプションでは、バージョン番号のワイルドカードをアスタリスク(*)に置き換えることが可能です。

バックアップにすべてのバージョンのファイルを含めたい場合は、GUIでそれらをすべて選択するか、CLIで-onlyオプションの後ろにファイル指定を含める必要があります。以下のように、バージョン番号にワイルドカードを使用します。以下に例を示します。

/DKA1/dir1/filename.txt.*

Media Agentの構成

OpenVMSとハードウェアマニュアルをガイドとして使用して、OpenVMSシステム上のデバイスを構成する必要があります。最初に、テープライブラリの擬似デバイスを、SYSMANを使用して以下のように作成する必要があります。

$ RUN SYS$SYSTEM:SYSMAN

SYSMAN> IO CONNECT gcan/NOADAPTER/DRIVER=SYS$GcDRIVER

内容は以下のとおりです。

- c = K (直接接続型のSCSIテープライブラリの場合)
- a = A、B、C、…(SCSIコントローラのアダプタの文字)
- n =テープライブラリロボティクス制御デバイスのユニット番号

注記:

このコマンドは、システムのブート後に実行する必要があります。

テープライブラリに接続されたSANの場合、SANのガイドラインに従ってSANドライブを構成すると、OpenVMSにテープドライブとロボットデバイス名が自動的に表示されます。

Data Protectorで使用するテープジュークボックスをインストールする場合は、Data Protectorでの構成前に、ハードウェアが正常動作することを確認してください。ハードウェアの検証には、Hewlett-PackardからMedia Robot Utility (MRU)を入手して使用することができます。

注記:

これらのデバイスを手動または自動で構成するには、通常Data Protector GUIを使用します。

ただし、一部の旧型テープライブラリや、HSxコントローラに接続されたテープライブラリでは、自動構成ができません。これらのデバイスをData Protectorに追加するには、手作業で構成してください。

クラスターのMedia Agent

クラスターシステムに接続されたデバイスは、以下のように取り扱います。

1. 各テープデバイスと各テープライブラリを構成し、各ノードからアクセスできるようにします。
2. デバイスを識別するため、デバイス名の最後にノード名を付加します。
3. テープデバイスでは、Devices/Properties/Settings/Advanced/Otherに共通のDevice Lock Nameを設定します。

例

ノードAとノードBで構成されているクラスター内で、TZ89がノードAに接続され、MSCPがノードBで動作しているとします。TZ89_Aという名前のデバイスを、ノードAでクライアントとして構成し、TZ89_Bという名前のデバイスを、ノードBでクライアントとして構成します。TZ89は、両方のデバイスに共通なデバイスロック名です。これで、Data Protectorでは、いずれのパスを介した場合でも、両方が1つのデバイスであると認識されたうえで、デバイスが使用されます。TZ89_Aを使用してノードBでバックアップを実行すると、Data Protectorによりデータがノード Bからノード Aのデバイスに移動されます。TZ89_Bを使用してノードBでバックアップを実行すると、OpenVMS MSCPサーバーによりデータがノードBからノードAのデバイスに移動されます。

注記:

クラスター内のMSCPにより機能するテープデバイスで、HSxコントローラまたはファイバーチャネルを介して接続されるすべてのテープデバイスの場合、オンラインヘルプの索引「SAN、デバイスの構成」のSAN構成のガイドラインに従ってください。

コマンドラインインタフェース

OpenVMSでData Protectorのコマンドラインインタフェースを使用する前に、以下のようにCLIコマンドのセットアップ手順を実行する必要があります。

$ @OMNI$ROOT:[BIN]OMNI$CLI_SETUP.COM使用可能なCLIコマンドの説明は、『*HP Data Protector Command Line Interface Reference*』を参照してください。

Oracle用統合ソフトウェア

『*HP Data Protectorインテグレーションガイド－Oracle、SAP*』の手順に従ってOracle用統合ソフトウェアのインストールと構成を完了したら、OMNI$ROOT:[CONFIG.CLIENT]omni_infoに-key Oracle8エントリが含まれていることを確認します。例を次に示します。

-key oracle8 -desc “Oracle Integration” -nlsset 159 -nlsId 12172 -flags 0x7 -ntpath “” -uxpath “” -version 6.20

このエントリが存在しない場合は、OMNI$ROOT:[CONFIG.CLIENT]omni_formatからコピーしてください。このエントリが含まれていないと、OpenVMSクライアント上でOracle用統合ソフトウェアがインストール済みとして示されません。

この次に行う作業

オンラインヘルプの索引「HP OpenVMS」を参照して、その他の構成タスクの詳細をご確認ください。

UNIXおよびMac OS Xクライアントのローカルインストール

ネットワーク上にUNIX用のインストールサーバーがない場合、または何らかの理由によりクライアントシステムをリモートインストールできない場合は、HP-UX用インストールまたはSolaris/Linux用インストールDVD-ROMを使用してData Protectorクライアントをローカルにインストールできます。

Install手順を開始する前に、どのコンポーネントをクライアントシステムにインストールするかを決定しておいてください。Data Protectorソフトウェアコンポーネントのリストと説明は、「Data Protectorコンポーネント」(76ページ)を参照してください。

前提条件

- システム要件、ディスクスペース要件、サポートされているプラットフォーム、プロセッサ、およびData Protectorコンポーネントについては、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- すべてのターゲットシステムに対するrootパーミッションが必要です。

インストールするには、POSIXシェル(sh)が必要です。

注記:

以下の手順を実行することにより、UNIXクライアントをローカルにアップグレードすることも可能です。スクリプトを実行すると、従来のインストール状況が検出されて、アップグレードを促すメッセージが表示されます。

手順

UNIXおよびMac OS Xクライアントをローカルにインストールするには、以下の手順に従ってください。

1. HP-UX用またはSolarisおよびLinux用のDVD-ROMをドライブに挿入し、マウントポイントにマウントします。

2. Mount_Point/LOCAL_INSTALLディレクトリから、omnisetup.shコマンドを実行します。

このコマンドの構文は、以下のとおりです。

omnisetup.sh [-source directory] [-server name] [-install component_list]

内容は以下のとおりです。

- *directory*には、インストールDVD-ROMのマウント位置を指定します。指定しなければ、カレントディレクトリが使用されます。
- *name*には、クライアントのインポート先となるセルのCell Managerの完全なホスト名を指定します。指定しなければ、クライアントが自動的にセルにインポートされることはありません。

注記:

Cell Manager以外のシステムのクライアントをアップグレードする場合は、-install component_listを指定する必要はありません。この場合、プロンプトは表示されず、アップグレード前にシステムにインストールされていたのと同じコンポーネントが自動的に選択されます。

ただし、Cell Managerに存在するクライアントコンポーネントをアップグレードするには、Cell Managerのアップグレードが完了した後に、-install component_listパラメータを設定してomnisetup.shコマンドを実行します。

- *component_list*には、インストールするコンポーネントコードの一覧をカンマで区切って指定します。スペースは使用できません。-installパラメータを指定しなければ、システムで利用可能な各コンポーネントについて、インストールするかどうか確認するプロンプトが個別に表示されます。

注記:

クライアントをアップグレードする場合に-installパラメータを指定しなければ、メッセージは返されず、アップグレード開始前にシステム上にインストールされていたのと同じコンポーネントが自動的に選択されます。

次の表はコンポーネントの一覧を示したものです。使用可能なコンポーネントの正確な一覧は、システムによって異なります。コンポーネントの説明については、「Data Protectorコンポーネント」(76ページ)を参照してください。

表 7 Data Protectorコンポーネントコード

コンポーネントコード	コンポーネント
cc	ユーザーインタフェース
da	Disk Agent
ma	General Media Agent
ndmp	NDMP Media Agent
informix	Informix用統合ソフトウェア
lotus	Lotus用統合ソフトウェア
oracle	Oracle用統合ソフトウェア
vmware	VMware用統合ソフトウェア(レガシー)
veagent	仮想環境統合ソフトウェア
ov	HP Network Node Manager
sybase	Sybase用統合ソフトウェア
sap	SAP R/3用統合ソフトウェア
sapdb	SAP DB用統合ソフトウェア
db2	DB2用統合ソフトウェア
emc	EMC Symmetrix Agent
ssea	HP StorageWorks P9000 XP Agent
smisa	HP StorageWorks P6000 EVA SMI-S Agent
vls_am	VLS自動移行
javagui	Javaグラフィカルユーザーインタフェース(グラフィカルユーザーインタフェース、Manager-of-Managersユーザーインタフェース)

コンポーネントコード	コンポーネント
docs	英語版マニュアル(ガイド、ヘルプ)
fra_ls	フランス語版マニュアル(ガイド、ヘルプ)
jpn_ls	日本語版マニュアル(ガイド、ヘルプ)
chs_ls	簡体字中国語版マニュアル(ガイド、ヘルプ)

例

次の例は、Disk Agent、General Media Agent、ユーザーインタフェース、およびInformix用統合ソフトウェアの各コンポーネントを、Cell Manager computer.company.comを使用してセルに自動的にインポートされるクライアントにインストールする方法を示しています。

```
./omnisetup.sh -server computer.company.com -install da,ma,cc,informix
```

3. Installが完了している場合や、クライアントがData Protectorセルにインポートされている場合は、そのことを示すメッセージが表示されます。

   いずれかのソフトウェアコンポーネントがインストール対象として選択されると、CORE コンポーネントが最初にインストールされます。

   いずれかの統合ソフトウェアコンポーネントがインストールまたは再インストール対象として選択されると、CORE-INTEGコンポーネントが最初にインストールされます。

ハードディスクからのインストール実行

InstallDVD-ROMをお使いのコンピュータにコピーして、UNIXおよびMac OS Xクライアントのインストールまたはアップグレードをハードディスクから実行するには、少なくともhpux/DP_DEPOTまたはsolaris/DP_DEPOTディレクトリ、およびLOCAL_INSTALLディレクトリをコピーしてください。

注記:

Linuxデポではローカルインストールはサポートされません。Linuxシステム上でも、HP-UXデポ(HP-UX用インストールDVDからクライアントをインストールする場合)またはSolarisデポ(Solaris/Linux用インストールDVDからクライアントをインストールする場合)のいずれかをコピーする必要があります。この制限は、DVDからインストールする場合には適用されません。

たとえば、インストールパッケージを/var/dp62にコピーする場合、ディレクトリは/var/dp62のサブディレクトリでなければなりません。

```
# pwd
/var/dp62
# ls
DP_DEPOT
LOCAL_INSTALL
```

これをハードディスクにコピーした後、LOCAL_INSTALLディレクトリに変更してから、次のコマンドを実行します。

```
omnisetup.sh [-server name] [-install component_list]
```

たとえば、次のように入力します。

```
./omnisetup.sh -install da
```

ディスク容量の制約などにより、DP_DEPOTディレクトリを別のディレクトリにコピーした場合は、-sourceオプションも必要になります。

この次に行う作業

Install時にCell Managerの名前を指定しておかなければ、クライアントはセルにインポートされません。この場合は、Data Protectorグラフィカルユーザーインタフェースを使用して、後からインポートする必要があります。作業手順は、「セルへのクライアントのインポート」(213ページ)を参照してください。追加の構成作業の詳細は、オンラインヘルプを参照してください。

Data Protector統合クライアントのインストール

Data Protector用統合ソフトウェアは、Oracle ServerやMicrosoft Exchange Serverなどのデータベースアプリケーションのオンラインバックアップを Data Protectorで実行可能にするソフトウェアコンポーネントです。Data Protector ZOB用統合ソフトウェアは、HP StorageWorks P6000 EVAディスクアレイファミリなどのディスクアレイを使用してゼロダウンタイムバックアップおよびインスタントリカバリを実行可能にするソフトウェアコンポーネントです。

データベースアプリケーションを実行しているシステムは、**統合クライアントと呼ばれ、**バックアップとデータの保存にZDBディスクアレイを使用するシステムは**ZDB統合クライアントと呼ばれます。**これらのクライアントは、WindowsやUNIX上の他のクライアントと同じ手順でインストールできますが、そのためには適切なソフトウェアコンポーネントを選択しておくことが必要です(たとえば、MS Exchange Serverデータベースのバックアップには MS Exchange用統合ソフトウェアコンポーネント、HP StorageWorks P6000 EVAディスクア

レイファミリによるZDBおよびIRにはHP StorageWorks P6000 EVA SMI-S Agentコンポーネントなど)。

前提条件

- システム要件、ディスクスペース要件、サポートされているプラットフォーム、プロセッサとData Protectorコンポーネントについては、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- データベースアプリケーションでData Protector用統合ソフトウェアを使用する場合は、ライセンスが必要です。ライセンスの詳細は「Data Protector 6.20の製品構成とライセンス」(336ページ)を参照してください。
- この時点で、Cell Managerおよびインストールサーバー(リモートインストールを行う場合)をネットワーク上にインストールしておく必要があります。この手順については、「Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール」(44ページ)を参照してください。

インストール手順を開始する前に、統合コンポーネントとともにクライアントシステムにインストールするその他のData Protectorソフトウェアコンポーネントを決定しておいてください。Data Protectorソフトウェアコンポーネントのリストと説明は、「Data Protectorコンポーネント」(76ページ)を参照してください。

以下に示すように、特定のData Protectorコンポーネントのインストールが必要となる場合があります。

- Data Protectorを使ってファイルシステムデータをバックアップする場合、Disk Agentコンポーネントが必要。Disk Agentは、以下の目的に使用することができます。
  - データベースアプリケーションバックアップ機能を使用してバックアップできない重要なデータがあるファイルシステムで、バックアップを実行する。
  - データベースアプリケーションサーバー(Oracle ServerやMS SQL Serverなど)のファイルシステムでテストバックアップを実行する。データベースアプリケーションでData Protector用統合ソフトウェアを構成し、アプリケーションとData Protectorに関連する通信やその他の問題点を解決する*前*に、ファイルシステムバックアップをテストする必要があります。
  - ディスクイメージとファイルシステムのZDBを実行する。
  - SAP R/3 ZDB統合ソフトウェアを使用する場合に、LAN上でバックアップメディアからアプリケーションシステムに復元する。
- Data Protector統合クライアント上でData Protector GUIおよびData Protector CLIを利用する場合、ユーザーインタフェースコンポーネントが必要。
- Data Protector統合クライアントに接続されたバックアップデバイスがある場合、General Media Agentコンポーネントが必要。NDMPサーバーを介してNDMP専用ドライブにアクセスするためにData Protectorクライアントを使用する場合は、NDMP Media Agentが必要です。

統合クライアントは、Windows用、HP-UX用またはSolaris/Linux用インストールDVD-ROMを使ってローカルにインストールすることも、Windows用またはUNIX用のインストールサーバーを使ってリモートインストールすることもできます。

個々の統合クライアントに関するその他の詳細は、以下の該当する項を参照してください。

- 「Microsoft Exchange Serverクライアント」(155ページ)
- 「Microsoft SQL Serverクライアント」(157ページ)
- 「Microsoft SharePoint Serverクライアント」(157ページ)
- 「Microsoft Hyper-Vクライアント」(164ページ)
- 「Sybaseクライアント」(159ページ)
- 「Informix Serverクライアント」(159ページ)
- 「SAP R/3クライアント」(160ページ)
- 「SAP MaxDBクライアント」(161ページ)
- 「Oracle Serverクライアント」(161ページ)
- 「VMwareクライアント」(162ページ)
- 「DB2クライアント」(165ページ)
- 「NNMクライアント」(165ページ)
- 「NDMP Serverクライアント」(165ページ)
- 「Microsoftボリュームシャドウコピーサービスクライアント」(166ページ)
- 「Lotus Notes/Domino Serverクライアント」(166ページ)
- 「EMC Symmetrix用統合ソフトウェア」(181ページ)
- 「HP StorageWorks P9000 XPディスクアレイファミリ用統合ソフトウェア」(174ページ)
- 「HP StorageWorks P6000 EVAディスクアレイファミリ用統合ソフトウェア」(167ページ)
- 「VLS自動移行クライアント」(186ページ)

上の項に示すData Protector統合クライアントへのData Protector統合ソフトウェアのインストールが完了していれば、適切な『*HP Data Protectorインテグレーションガイド*』、『*HP Data Protector Zero Downtime Backup Administrator's Guide*』、または『*HP Data Protector Zero Downtime Backup Integration Guide*』を参照して、Data Protector統合クライアントを構成します。

ローカルインストール

お使いの環境にそれぞれのオペレーティングシステム用のインストールサーバーがない場合は、クライアントをインストールするプラットフォームに応じて、Windows用、HP-UX用、またはSolaris/Linux用のインストールDVD-ROMを使用して、ローカルインストールを

行う必要があります。詳細は「Windows用クライアントのインストール」(92ページ)か「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)を参照してください。

Installする際にCell Managerを選択しなかった場合、ローカルインストール後にクライアントシステムをセルに手動でインポートする必要があります。「セルへのクライアントのインポート」(213ページ)も参照してください。

リモートインストール

クライアントソフトウェアは、Data Protectorグラフィカルユーザーインタフェースを使ってインストールサーバーからリモートにインストールできます。ソフトウェアのリモートインストール手順は、「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

リモートインストールが終了すると、クライアントシステムは自動的にData Protectorセルのメンバーになります。

クラスター対応統合ソフトウェアのインストール

Data Protectorクラスター対応統合クライアントは、各クラスターノードで、DVD-ROMからローカルにインストールする必要があります。ローカルクライアントのセットアップ中には、他のクライアントソフトウェアコンポーネントに加え、適切な統合ソフトウェアコンポーネント(Oracle IntegrationやHP Data Protector P6000 EVA SMI-S Agentなど)をインストールしてください。

Data Protector Cell Managerには、クラスター対応データベースアプリケーションとZDB Agentもインストールできます。Cell Managerのセットアップ中に、適切な統合ソフトウェアコンポーネントを選択してください。

Install手順は、統合クライアントをインストールするクラスター環境により、異なります。該当するオペレーティングシステムのクラスター化に関する項を参照してください。

- 「MC/ServiceGuardへのData Protectorのインストール」(193ページ)
- 「Microsoft Cluster ServerへのData Protectorのインストール」(195ページ).
- 「Veritas ClusterへのData Protectorクライアントのインストール」(207ページ)
- 「Novell NetWare ClusterへのData Protectorクライアントのインストール」(208ページ)
- 「Data ProtectorのIBM HACMP Clusterへのインストール」(210ページ)

クラスターリングの詳細は、オンラインヘルプの索引「クラスター、MC/ServiceGuard」および*HP Data Protectorコンセプトガイド*を参照してください。

この次に行う作業

Installの完了後に統合ソフトウェアを構成する方法は、適切な『*HP Data Protectorインテグレーションガイド*』を参照してください。

Microsoft Exchange Serverクライアント

Microsoft Exchange Serverシステムにインストールする必要があるData Protectorコンポーネントは、使用するバックアップおよび復元のソリューションによって異なります。以下のソリューションから選択できます。

- 「Data ProtectorMicrosoft Exchange Server 2003/2007用統合ソフトウェア」(155ページ)
- 「Data Protector Microsoft Exchange Server 2010用統合ソフトウェア」(155ページ)
- 「Data Protector Microsoft Exchange Server Single Mailbox用統合ソフトウェア」(156ページ)
- 「Data Protector Microsoftボリュームシャドウコピーサービス用統合ソフトウェア」(157ページ)

Data ProtectorMicrosoft Exchange Server 2003/2007用統合ソフトウェア

ここでは、Microsoft Exchange Serverが正しく動作していることが前提となります。

Microsoft Exchange Serverデータベースをバックアップできるようにするには、Microsoft Exchange ServerシステムにMS Exchange用統合ソフトウェアコンポーネントをインストールします。

Microsoft Exchangeシングルメールボックス用統合ソフトウェアエージェントは、Data Protector Microsoft Exchange Serverの統合パッケージの一部としてインストールされます。

Data Protector Microsoft Exchange Server 2010用統合ソフトウェア

ここでは、Microsoft Exchange Server 2010環境が正しく稼働していることが前提となります。

Microsoft Exchange Serverデータベースをバックアップできるようにするには、Microsoft Exchange Serverシステムに次のData Protectorコンポーネントを必ずインストールします。

- MS Exchange Server 2010統合ソフトウェア
- MS ボリュームシャドウコピー用統合ソフトウェア
- 適切なData Protectorディスクアレイエージェント(Microsoft Exchange Serverデータがディスクアレイに存在する場合)

注記:

VSSトランスポータブルバックアップセッションでは、バックアップシステムにMS ボリュームシャドウコピー用統合ソフトウェア**コンポーネントと適切なData Protector ディスクアレイエージェントもインストールする必要があります。**

DAG環境では、DAG仮想システム(ホスト)もData Protectorセルにインポートする必要があります。Data Protectorセルにクライアントをインポートする方法については、オンラインヘルプの索引「インポート、クライアントシステム」を参照してください。

注記:

- **Data ProtectorのMS Exchange Server 2010用統合ソフトウェアはVSS技術に基づいているため、**MS Exchange Server 2010用統合ソフトウェア**コンポーネントのインストール時に、自動的に**MS ボリュームシャドウコピー用統合ソフトウェア**コンポーネントがインストールされます。**MS ボリュームシャドウコピー用統合ソフトウェア**コンポーネントがすでにインストールされている場合は、アップグレードされます。**
- MS Exchange Server 2010用統合ソフトウェア**コンポーネントをシステムから削除しても、**MS ボリュームシャドウコピー用統合ソフトウェア**コンポーネントは自動的に削除されません。**MS Exchange Server 2010用統合ソフトウェア**コンポーネントがインストールされているシステムから**MS ボリュームシャドウコピー用統合ソフトウェア**コンポーネントを削除することはできないので注意してください。**

Data Protector Microsoft Exchange Server Single Mailbox用統合ソフトウェア

ここでは、Microsoft Exchange Serverが正しく動作していることが前提となります。

Microsoft Exchange Serverのメールボックスフォルダとパブリックフォルダの項目をバックアップできるようにするには、Microsoft Exchange ServerシステムにMS Exchange用統合ソフトウェアコンポーネントをインストールします。DAG環境では、DAGの一部に含まれるすべてのMicrosoft Exchange Serverシステムにこのコンポーネントをインストールします。

Microsoft Exchange Server 2007システムの場合、追加パッケージをインストールして、Data Protector Microsoft Exchange Single Mailbox用統合ソフトウェアの機能を有効にする必要があります。パッケージは、Microsoft Exchange Server MAPIクライアントおよびCollaboration Data Objects (ExchangeMapiCdo. EXE)という名前で、Microsoft Webサイト

http://www.microsoft.com/downloads/Search.aspx?DisplayLang=enから無料でダウンロードできます。

Data Protector Microsoftボリュームシャドウコピーサービス用統合ソフトウェア

「Microsoftボリュームシャドウコピーサービスクライアント」(166ページ)を参照してください。

Microsoft SQL Serverクライアント

ここでは、Microsoft SQL Serverが正しく動作していることが前提となります。

Microsoft SQL Serverデータベースをバックアップできるようにするには、インストール手順でMS SQL用統合ソフトウェアコンポーネントを選択する必要があります。

Microsoft SharePoint Serverクライアント

Microsoft SharePoint Server環境にインストールする必要があるData Protectorコンポーネントは、使用するバックアップおよび復元のソリューションによって異なります。以下のソリューションから選択できます。

- 「Data Protector Microsoft SharePoint Server 2003用統合ソフトウェア」(157ページ)
- 「Data Protector Microsoft SharePoint Server 2007/2010用統合ソフトウェア」(158ページ)
- 「Data Protector Microsoft SharePoint Server 2007/2010 VSSを使用するソリューション」(158ページ)
- 「Data Protector Microsoftボリュームシャドウコピーサービス用統合ソフトウェア」(158ページ)
- 「Microsoft SharePoint Server向けData Protector Granular Recovery Extension」(159ページ)

Data Protector Microsoft SharePoint Server 2003用統合ソフトウェア

ここでは、Microsoft SharePoint Portal Serverインスタンスと関連するMicrosoft SQL Serverインスタンスが正しく動作していることが前提となります。

Microsoft SharePoint Portal Serverオブジェクトをバックアップできるようにするには、次のData Protectorコンポーネントをインストールします。

- MS SharePoint用統合ソフトウェア – Microsoft SharePoint Portal Serverシステム上
- MS SQL用統合ソフトウェア – Microsoft SQL Serverシステム上

Data Protector Microsoft SharePoint Server 2007/2010用統合ソフトウェア

ここでは、Microsoft SharePoint Serverインスタンスと関連するMicrosoft SQL Serverインスタンスが正しく動作していることが前提となります。

Microsoft SharePoint Serverオブジェクトをバックアップできるようにするには、次のData Protectorコンポーネントをインストールします。

- MS SharePoint 2007/2010用統合ソフトウェア - Microsoft SharePoint Serverシステム上
- MS SQL用統合ソフトウェア - Microsoft SQL Serverシステム上

Data Protector Microsoft SharePoint Server 2007/2010 VSSを使用するソリューション

ここでは、Microsoft SharePoint Serverインスタンスと関連するMicrosoft SQL Serverインスタンスが正しく動作していることが前提となります。

Microsoft SharePoint Serverオブジェクトをバックアップできるようにするには、次のData Protectorコンポーネントをインストールします。

- MS ボリュームシャドウコピー用統合ソフトウェア - Microsoft SharePoint Serverシステムおよび Microsoft SQL Serverシステム上にインストールします。少なくとも次のサービスのいずれか 1 つが有効である必要があります。

  Microsoft Office SharePoint Server 2007

  - Windows SharePoint Services Database
  - Windows SharePoint Serviceヘルプ検索
  - Office SharePoint Server Search

  Microsoft SharePoint Server 2010

  - SharePoint Foundation Database
  - SharePoint Foundation Help Search
  - SharePoint Server Search

- ユーザーインタフェースコンポーネント - MS ボリュームシャドウコピー用統合ソフトウェアがインストールされたMicrosoft SharePoint Serverの 1 つ、およびバックアップを構成し開始する予定のMicrosoft SharePoint Serverにインストールします。

Data Protector Microsoftボリュームシャドウコピーサービス用統合ソフトウェア

「Microsoftボリュームシャドウコピーサービスクライアント」(166ページ)を参照してください。

Microsoft SharePoint Server向けData Protector Granular Recovery Extension

ここでは、Microsoft SharePoint Serverインスタンスと関連するMicrosoft SQL Serverインスタンスが正しく動作していることが前提となります。

Microsoft SharePoint Server の各オブジェクトを復元できるようにするには、Microsoft SharePoint Serverの全体管理システムにMS SharePoint Granular Recovery Extensionをインストールします。

- コンポーネントをローカルにインストールすると、Data Protectorインストールウィザードに MS SharePoint GREオプションのダイアログボックスが表示されます。ファーム管理者のユーザー名とパスワードを指定します。
- このコンポーネントをリモートにインストールするには、[MS SharePoint Granular Recovery Extension]を選択して**[構成]**をクリックし、MS SharePoint GREオプションのダイアログボックスにファーム管理者ユーザー名とパスワードを指定します。

注記:

Microsoft SharePoint Serverデータをバックアップするために必要なData Protectorコンポーネントも Microsoft SharePoint Server環境にインストールされていることを確認します。

Sybaseクライアント

Sybase Backup Serverはすでに実行されているものとします。

Sybaseデータベースをバックアップする場合は、インストール手順で以下のData Protectorコンポーネントを選択する必要があります。

- Sybase用統合ソフトウェア – Sybaseデータベースをバックアップする場合
- Disk Agent – 以下の2つの理由でDisk Agentをインストールする場合
  - Sybase Backup Serverのファイルシステムバックアップを行うため。Sybase用統合ソフトウェアを構成し、Sybase Backup ServerとData Protectorに関連するすべての問題点を解決する*前に*、このバックアップを行ってください。
  - Sybase Backup Serverを使用してバックアップできない重要なデータがあるファイルシステムでのバックアップを実行するため。

Informix Serverクライアント

Informix Serverはすでに実行されているものとします。

Informix Serverデータベースをバックアップする場合は、インストール手順で以下のData Protectorコンポーネントを選択する必要があります。

- Informix用統合ソフトウェア - Informix Serverデータベースをバックアップする場合
- Disk Agent - 以下の2つの理由でDisk Agentをインストールする場合
  - Informix Serverのファイルシステムバックアップを行うため。Informix用統合ソフトウェアを構成し、Informix ServerとData Protectorに関連するすべての問題点を解決する*前に*、このバックアップを行ってください。
  - ON-Barを使用してバックアップ*できない*重要なInformix Serverデータ(ONCONFIGファイル、sqlhostsファイル、ON-Bar緊急ブートファイル、oncfg_INFORMIXSERVER.SERVERNUM、構成ファイルなど)があるファイルシステムでのバックアップを実行するため。

IBM HACMP Cluster

If Informix ServerがIBM HACMPクラスター環境にインストールされている場合は、すべてのクラスターノードにInformix用統合ソフトウェアコンポーネントをインストールします。

SAP R/3クライアント

前提条件

- 次のOracleソフトウェアがインストールされて構成されていることを確認します。
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net8ソフトウェア
  - SQL*Plus
- SAP R/3 Database Serverはすでに実行されているものとします。

注記:

Data ProtectorのSAP R/3用統合ソフトウェアのバックアップ仕様では、以前のバージョンのData Protectorに対する互換性が完全に確保されています。Data Protectorでは、旧バージョンのData Protectorで作成したバックアップ仕様をすべて実行できます。ただし、最新バージョンのData Protectorで作成したバックアップ仕様を、旧バージョンのData Protectorで使用することはできません。

SAP R/3データベースをバックアップする場合は、インストール手順で以下のコンポーネントを選択する必要があります。

- SAP R/3用統合ソフトウェア
- Disk Agent

  Data Protectorでは、Disk Agentをバックアップサーバー(バックアップされるファイルシステムデータがあるクライアント)にインストールする必要があります。

SAP MaxDBクライアント

SAP MaxDBサーバーはすでに実行されているものとします。

SAP MaxDBデータベースのバックアップを可能にするには、インストール手順で以下のData Protectorコンポーネントを選択する必要があります。

- SAP DB用統合ソフトウェア - SAP MaxDBデータベースの統合オンラインバックアップを実行する場合
- Disk Agent - SAP MaxDBデータベースの非統合オフラインバックアップを実行する場合

Oracle Serverクライアント

Oracle Serverはすでに実行されているものとします。

Oracleデータベースをバックアップする場合は、インストール手順でOracle用統合ソフトウェアコンポーネントを選択する必要があります。

HP OpenVMS

HP OpenVMSでは、*HP Data Protectorインテグレーションガイド－Oracle、SAP*で説明されているようにOracle用統合ソフトウェアをインストールして構成した後、-key Oracle8エントリがOMNI$ROOT:[CONFIG.CLIENT]omni_infoに表示されていることを確認します。次に例を示します。

-key oracle8 -desc “Oracle Integration” -nlsset 159 -nlsId 12172 -flags 0x7 -ntpath “” -uxpath “” -version 6.20

このエントリが存在しない場合は、OMNI$ROOT:[CONFIG.CLIENT]omni_formatからコピーしてください。このエントリが含まれていないと、OpenVMSクライアント上でOracle用統合ソフトウェアがインストール済みとして示されません。

VMwareクライアント

VMwareシステムへのインストールが必要になるData Protectorコンポーネントは、使用するバックアップと復元ソリューションによって異なります。以下のソリューションから選択できます。

- 「Data Protector仮想環境統合ソフトウェア」(162ページ)
- 「Data ProtectorVMware(レガシー)用統合ソフトウェア」(162ページ)
- 「VMware vSphere向けData Protector Granular Recovery Extension」(163ページ)

Data Protector仮想環境統合ソフトウェア

バックアップホストはすでに実行されているものとします。

バックアップホストとして使用する各システム上にData Protector 仮想環境統合ソフトウェアコンポーネントをインストールします。

Data ProtectorVMware(レガシー)用統合ソフトウェア

VirtualCenter Serverシステム(存在する場合)およびESX Serverシステムはすでに実行されているものとします。VMwareクライアントをインストールできるようにするには、最初にOpenSSHを設定します。詳細は、オンラインヘルプの索引「インストール、クライアントシステム」を参照してください。

Data Protector VMware用統合ソフトウェア（レガシー）コンポーネントを以下のクライアントにインストールします。

- 仮想マシンをバックアップするすべてのESX Serverシステム
- VirtualCenterシステム(存在する場合)
- バックアッププロキシーシステム(**VCBfile**および**VCBimage**バックアップ方式を使用する場合)
- 仮想マシンのファイルシステムを復元するWindowsシステム(物理または仮想l)

注記:

Data Protector VMware用統合ソフトウェア(レガシー)コンポーネントは、ESXi Serverシステムにはインストールできません。そのため、ESXi Serverシステム上で実行している仮想マシンに使用できないバックアップおよび復元機能が存在します。

Clusters

クラスター内のESX ServerシステムまたはVirtualCenterシステムの有無に関係なく、VMware用統合ソフトウェア(レガシー)コンポーネントを両方のクラスターノードにインストールします。

VMware vSphere向けData Protector Granular Recovery Extension

Data Protectorの仮想環境統合ソフトウェアが『*HP Data Protector Integration Guide for Virtualization Environments*ガイド』の手順に従ってインストールおよび構成されていることと、復元を行う仮想マシンにバージョン4.x以降のVMwareツールがインストールされていることが前提となります。

制限事項

- VMware向けData Protector Granular Recovery Extensionでは、リモートインストールのみがサポートされています。

マウントプロキシシステムに次のData Protectorコンポーネントをリモートインストールしてます。詳細については、オンラインヘルプの索引「インストール、クライアントシステム」を参照してください。

- ユーザーインタフェース
- 仮想環境統合ソフトウェア
- VMware Granular Recovery Extension Agent

Virtual Center (vCenter) Serverシステムで、次の手順を実行します。

1. VMware Granular Extension Web Plug-Inコンポーネントをリモートインストールします。
2. Data Protector GUIを使用して、vCenter ServerシステムをVMware vCenterタイプのData Protectorセルにインポートします。詳細は、オンラインヘルプの索引「インポート、クライアントシステム」を参照してください。

注記:

vCenter Serverに仮想システム統合ソフトウェアをインストールすると、そのシステムには他のData Protectorコンポーネントをリモートインストールできなくなります。仮想環境統合ソフトウェアをインストールしたvCenter ServerにVMware Granular Extension Web Plug-Inをインストールするには、次の手順を実行します。

1. vCenter Serverを、Data Protector ClientタイプのData Protectorセルにインポートします。
2. vCenter Serverシステムを、VMware vCenterタイプのData Protectorセルにインポートします。
3. VMware Granular Extension Web Plug-Inコンポーネントをリモートインストールします。

Microsoft Hyper-Vクライアント

Microsoft Hyper-Vシステムにインストールする必要があるData Protectorコンポーネントは、使用するバックアップおよび復元のソリューションによって異なります。以下のソリューションから選択できます。

- 「Data Protector仮想環境統合ソフトウェア」(162ページ)
- 「Data Protector Microsoftボリュームシャドウコピーサービス用統合ソフトウェア」(164ページ)

Data Protector仮想環境統合ソフトウェア

バックアップホストと、バックアップおよび復元の対象となるMicrosoft Hyper-Vシステムはすでに稼働中であることが前提となります。

次のData Protectorコンポーネントをバックアップホストと Microsoft Hyper-Vシステムの両方にインストールします。

- 仮想環境統合ソフトウェア
- MSボリュームシャドウコピー用統合ソフトウェア

Data Protector Microsoftボリュームシャドウコピーサービス用統合ソフトウェア

Microsoft Hyper-Vシステムにインストールする必要があるコンポーネントの詳細については、「Microsoftボリュームシャドウコピーサービスクライアント」(166ページ)を参照してください。

DB2クライアント

DB2 Serverはすでに実行されているものとします。

DB2データベースをバックアップする場合は、インストール手順でDB2用統合ソフトウェアコンポーネントおよびDisk Agentコンポーネントを選択する必要があります。

物理的にパーティション化された環境の場合は、データベースが置かれている各物理ノード(システム)にDB2用統合ソフトウェアコンポーネントおよびDisk Agentコンポーネントをインストールします。

注記:

rootとしてログオンした後、インストールを実行します。

NNMクライアント

NNMシステムはすでに実行されているものとします。

NNMデータベースをバックアップできるようにするには、インストール手順でHP NNM Backup用統合ソフトウェアコンポーネントとDisk Agentコンポーネントを選択する必要があります。Disk Agentでは、バックアップ目的でバックアップ前スクリプトとバックアップ後スクリプトを実行する必要があります。

NDMP Serverクライアント

NDMP Serverはすでに実行されているものとします。

Install手順中で、NDMP Media Agentを選択し、NDMP専用ドライブにアクセスするすべてのData Protectorクライアントにインストールします。

注記:

Data Protectorクライアントが、NDMP Serverを介したNDMP専用ドライブへのアクセスに使用されず、ライブラリロボティクスの制御のみに使用される場合、そのようなクライアントには、NDMP Media AgentかGeneral Media Agentのいずれかをインストールできます。

1台のData Protectorクライアントには、1つのMedia Agentしかインストールできないことに、注意してください。

Microsoftボリュームシャドウコピーサービスクライアント

VSSライター、またはVSSを使用したファイルシステムのみをバックアップするには、アプリケーションシステム(ローカルバックアップの場合)、またはアプリケーションシステムとバックアップシステムの両方(トランスポータブルバックアップの場合)に、以下のData Protectorソフトウェアをインストールします。

- MS ボリュームシャドウコピー用統合ソフトウェア
- ディスクアレイを(ハードウェアプロバイダとともに)使用する場合は、適切なディスクアレイエージェント(HP StorageWorks P6000 EVA SMI-S Agent、HP StorageWorks P9000 XP Agent、またはHP StorageWorks P4000 Agent)。

VSS用統合ソフトウェアをインストールした後、ディスクへのZDBセッションおよびディスク+テープへのZDBセッション(インスタントリカバリが有効なセッション)を実行する場合は、アプリケーションシステム上のソースボリュームを解決する必要があります。セルのVSSクライアントからの解決操作は、以下のように実行します。

```
omnidbvss -resolve {-apphost ApplicationSystem | -all}
```

ただし、アプリケーションシステムを解決しないか解決に失敗する場合、omnircファイル内でOB2VSS_DISABLE_AUTO_RESOLVE変数が0(デフォルト)に設定されていれば、アプリケーションシステムが自動で解決されます。この場合、複製作成のバックアップ時間が長くなります。

詳細は、『*HP Data Protector Zero Downtime backup Integration guide*』を参照してください。

Lotus Notes/Domino Serverクライアント

Lotus Notes/Domino Serverはすでに実行されているものとします。

Lotus Notes/Domino Serverデータベースのバックアップを可能にするには、インストール手順でLotus用統合ソフトウェアコンポーネントとDisk Agentコンポーネントを選択する必要があります。以下の目的で、Data Protectorでファイルシステムデータをバックアップできるようにするには、Disk Agentコンポーネントが必要です。

- Lotus統合エージェントを使用してバックアップできない重要なデータのバックアップを実行するため。これらは、非データベースファイルと呼ばれており、notes.ini、desktop.dsk、すべての*.idファイルなどがあります。Lotus Notes/Domino Serverでは、データを完全に保護するため、これらのファイルのバックアップを実行する必要があります。
- アプリケーションとData Protectorに関連する通信やその他の問題点を解決する目的で、ファイルシステムバックアップをテストするため。

Lotus Domino Cluster

Install the Lotus用統合ソフトウェアおよびDisk Agentのコンポーネントを、バックアップに使用するDominoサーバーにインストールします。また、Dominoデータベースをこのデータベースの複製を含む他のDominoサーバーに復元する場合は、これらのDominoサーバーにもコンポーネントをインストールします。

HP StorageWorks P6000 EVAディスクアレイファミリ用統合ソフトウェア

HP StorageWorks P6000 EVAディスクアレイファミリをData Protectorと統合する場合は、以下のData Protectorソフトウェアコンポーネントをアプリケーションシステムとバックアップシステムにインストールします。

- HP StorageWorks P6000 EVA SMI-S Agent
- General Media Agent

  General Media Agentコンポーネントは、バルクデータをバックアップする場合に、バックアップシステムにインストールします。またアーカイブログのバックアップやアプリケーションシステムへの復元を行う場合は、アプリケーションシステムにインストールします。

- Disk Agent

  Disk Agentコンポーネントは、ディスクイメージおよびファイルシステムのZDBを実行する場合に、アプリケーションシステムとバックアップシステムにインストールします。Disk Agentがインストールされていないクライアントは、ZDBバックアップ仕様を作成する際に、[アプリケーションシステム]ドロップダウンリストおよび[バックアップシステム]ドロップダウンリストに表示されません。

重要:

Microsoft Windows Server 2008システムでは、Data Protector HP StorageWorks P6000 EVAディスクアレイファミリ用統合ソフトウェアを正常に動作させるために、2つのWindows Server 2008修正プログラムをインストールする必要があります。必要な修正プログラムパッケージは、Microsoft Web サイトhttp://support.microsoft.com/kb/952790からダウンロードできます。

クラスターへのインストール

HP StorageWorks P6000 EVAディスクアレイファミリ用統合ソフトウェアは、クラスター環境にインストールできます。サポート対象のクラスター構成とインストール要件の詳細は、

『*HP Data Protector Zero Downtime Backup Administrator's Guide*』を参照してください。

他のアプリケーションの統合

HP StorageWorks P6000 EVAディスクアレイファミリ用統合ソフトウェアをデータベースアプリケーションと組み合わせてインストールする場合は、この組み合わせに必要なData Protectorコンポーネントをアプリケーションシステムとバックアップシステムにインストールし、この組み合わせ特有のインストール作業を実行してください。HP StorageWorks P6000 EVAディスクアレイファミリ用統合ソフトウェアは、Oracle Server、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server、およびMicrosoftボリュームシャドウコピーサービスと組み合わせてインストールできます。

HP StorageWorks P6000 EVAディスクアレイファミリとOracle Serverの統合

前提条件

- アプリケーションシステムと、バックアップセットZDBの方法のバックアップシステムには、以下のソフトウェアをインストールし、構成を完了しておく必要があります。
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net Services
  - SQL*Plus

  バックアップシステム上のOracleソフトウェアは、アプリケーションシステムと同じディレクトリにインストールする必要があります。また、バックアップシステム上のバイナリは、アプリケーションシステム上のバイナリと同一に設定する必要があります。これは、アプリケーションシステムからバックアップシステムにファイルとシステム環境をコピーするか、アプリケーションシステムと同じインストールパラメータを使用して、バックアップシステムでOracleバイナリのクリーンインストールを実行することにより、実現できます。

- アプリケーションシステムで使用されるOracleデータファイルは、インストールしたSMI-S Agentを使用してレプリケートされるソースボリュームにインストールする必要があります。

  Oracleの制御ファイル、オンラインREDOログファイル、およびOracle SPFILEの配置場所は、次の2つのオプションから選択できます。
  - Oracle制御ファイル、オンラインREDOログファイル、およびOracle SPFILEを、Oracleデータファイルとは**異なる**ボリュームグループ(LVMを使用する場合)またはソースボリュームに配置する。

    この構成では、デフォルトでインスタントリカバリが使用可能です。
  - Oracle制御ファイル、オンラインREDOログファイル、およびOracle SPFILEを、Oracleデータファイルと**同じ**ボリュームグループ(LVMを使用する場合)またはソースボリュームに配置する。

この構成では、デフォルトではインスタントリカバリは使用不可です。インスタントリカバリを使用可能にするには、ZDB_ORA_INCLUDE_CF_OLF、ZDB_ORA_INCLUDE_SPF、およびZDB_ORA_NO_CHECKCONF_IR omnirc変数を設定します。詳細については、*HP Data Protector Zero Downtime Backup Integration Guide*を参照してください。

Oracleのアーカイブ REDOログファイルは、ソースボリュームに配置する必要はありません。

Oracleデータファイルの一部がシンボリックリンクにインストールされている場合、バックアップシステムにもこれらのリンクを作成する必要があります。

インストール手順

Install作業は、以下のとおり実行します。

1. Oracleのリカバリカタログデータベースをインストールします。このカタログデータベースは、非ミラー化ディスク上の個々のシステムにインストールすることをお勧めします。リカバリカタログは、登録しない状態で残しておきます。データベースのインストール方法については、Oracleのマニュアルを参照してください。
2. 以下のData Protectorソフトウェアコンポーネントをインストールします。
   - HP StorageWorks P6000 EVA SMI-S Agent – アプリケーションシステムとバックアップシステムの両方
   - Oracle用統合ソフトウェア – アプリケーションシステムとバックアップシステムの両方

注記:

- **バックアップシステムのData Protector Oracle用統合ソフトウェアコンポーネントは、バックアップセットZDB方式にのみ必要です。プロキシーコピーZDBのプロキシーコピー方法の場合は必要ありません。**
- **RACクラスター環境の場合、Oracleアプリケーションデータベースは、複数のOracleインスタンスによりアクセスされます。そのため、Oracleインスタンスを実行するすべてのシステムにData Protector Oracle用統合ソフトウェアおよびHP StorageWorks P6000 EVA SMI-S Agentコンポーネントをインストールしてください。**
- **Oracleリカバリカタログデータベースが個々のシステムにインストールされている場合は、そこにData Protectorソフトウェアコンポーネントをインストールする必要はありません。**

HP StorageWorks P6000 EVAディスクアレイファミリとSAP R/3の統合

前提条件

- アプリケーションシステムには、以下のOracleソフトウェアがインストールされている必要があります。
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net Services
  - SQL*Plus
- SAP準拠のZDBセッション(アプリケーションシステムではなくバックアップシステムで開始されたBRBACKUP)を実行する場合、バックアップシステムを構成します。詳細は、Oracle用のSAPデータベースガイド(スプリットミラーバックアップ、ソフトウェア構成)を参照してください。
- アプリケーションシステム上のデータベースは、ディスクイメージ、論理ボリューム、またはファイルシステムにインストールすることが可能です。
  - Oracleのデータファイルは、ディスクアレイに配置する必要があります。
  - オンラインバックアップの場合、オンラインのREDOログをディスクアレイに配置する必要はありません。オンラインSAP対応ZDBセッションは例外です。コントロールファイルはディスクアレイに配置する必要があります。
  - オフラインバックアップの場合、コントロールファイルとオンラインのREDOログはディスクアレイに配置する必要があります。
  - アーカイブされたREDOログファイルは、ディスクアレイに配置する必要はありません。

  Oracle制御ファイル、オンラインREDOログファイル、およびOracle SPFILEを、Oracleデータファイルと*同じ*LVMボリュームグループまたはソースボリュームに配置する場合、Data ProtectorのZDB_ORA_NO_CHECKCONF_IR、ZDB_ORA_INCLUDE_CF_OLF、ZDB_ORA_INCLUDE_SPF omnirc変数を設定します。設定しないと、ZDB-to-diskセッションとZDB-to-disk+tapeセッションを実行できません。詳細は、『*HP Data Protector Zero Downtime Backup Integration Guide*』を参照してください。

注記:

Oracleデータファイルの一部がシンボリックリンクにインストールされている場合、バックアップシステムにもリンクを作成します。

***UNIXの場合のみ*、Oracleデータベースがrawパーティション(rawディスクまたはraw論理ボリューム)にインストールされている場合、アプリケーションシステムとバックアップシステムでのボリューム/ディスクグループ名が同じであることを確認してください。**

- UNIXの場合、アプリケーションシステムに以下のユーザーが存在しているかどうかを確認します。
  - プライマリグループがdbaのoraORACLE_SID
  - UNIXグループsapsysに属するORACLE_SIDadm
- SAP R/3ソフトウェアは、アプリケーションシステムに正しくインストールする必要があります。

  SAP R/3のインストール後にアプリケーションシステムにインストールする必要がある標準ディレクトリのリストは、以下のとおりです。

注記:

ディレクトリの場所は、環境変数(UNIXシステムの場合)またはレジストリ(Windowsシステムの場合)によって異なります。詳細は、SAP R/3のマニュアルを参照してください。

- ORACLE_HOME/dbs(UNIXシステムの場合)*ORACLE_HOME*¥database (Windowsシステムの場合) - OracleとSAPのプロファイル
- ORACLE_HOME/bin (UNIXシステムの場合) *ORACLE_HOME*¥bin (Windowsシステムの場合) - Oracleのバイナリ
- SAPDATA_HOME/sapbackup (UNIXシステムの場合)または*SAPDATA_HOME*¥sapbackup(Windowsシステムの場合) - BRBACKUPログファイルが置かれるSAPBACKUPディレクトリ
- SAPDATA_HOME/saparch (UNIXシステムの場合) SAPDATA_HOME¥saparch (Windowsシステムの場合) - BRARCHIVEログファイルが置かれるSAPARCHディレクトリ
- SAPDATA_HOME/sapreorg (UNIXシステムの場合)または*SAPDATA_HOME*¥sapreorg (Windowsシステムの場合)
- SAPDATA_HOME/sapcheck (UNIXシステムの場合)または*SAPDATA_HOME*¥sapcheck (Windowsシステムの場合)
- SAPDATA_HOME/saptrace (UNIXシステムの場合)またはSAPDATA_HOME¥saptrace (Windowsシステムの場合)
- /usr/sap/ORACLE_SID/SYS/exe/run (UNIXシステム)

  c:¥Oracle¥ORACLE_SID¥sys¥exe¥run (Windowsシステム)

注記:

インスタントリカバリを行う場合、sapbackup、saparch、およびsapreorgの各ディレクトリが、Oracleデータファイルとは異なるソースボリュームに存在していることを確認します。

UNIXシステム

UNIXシステムでは、最後の6つのディレクトリが前述の場所にない場合、適切なリンクを作成してください。

UNIXシステムの場合、ディレクトリ/usr/sap/ORACLE_SID/SYS/exe/runの所有者は、UNIXユーザーora*ORACLE_SID*でなければなりません。SAP R/3ファイルの所有者は、UNIXユーザーora*ORACLE_SID*であり、setuidビットがセットされた(chmod 4755 ...) UNIXグループdbaに属していなければなりません。例外はBRRESTOREファイルの場合で、その所有者はUNIXユーザー*ORACLE_SID*admでなければなりません。

UNIXでの例

*ORACLE_SID*がPROの場合、/usr/sap/PRO/SYS/exe/runディレクトリ内のパーミッションは、以下のとおりに設定する必要があります。

```
-rwsr-xr-x   1 orapro dba 4598276
Apr 17  2010 brarchive -rwsr-xr-x   1 orapro dba 4750020 Apr 17  2010 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  2010 brconnect -rwsr-xr-x   1 proadm
sapsys 430467 Apr 17  2010

brrestore -rwsr-xr-x   1 orapro dba 188629 Apr 17  2010 brtools
```

インストール手順

1. SAP R/3 BRTOOLSを、アプリケーションシステムにインストールします。
2. 以下のData Protectorソフトウェアコンポーネントを、アプリケーションシステムとバックアップシステムの両方にインストールします。
   - HP StorageWorks P6000 EVA SMI-S Agent
   - SAP R/3用統合ソフトウェア
   - Disk Agent

注記:

SAP R/3 Integrationは、バックアップシステムでBRBACKUPが開始されるSAP対応ZDBセッションを実行する場合にのみインストールする必要があります。

Windowsシステムの場合、Data ProtectorソフトウェアコンポーネントをSAP R/3管理者用ユーザーアカウントを使用してインストールする必要があります。また、このアカウントは、SAP R/3インスタンスが実行されているシステム上のORA_DBAローカルグループかORA_SID_DBAローカルグループに含まれている必要があります。

HP StorageWorks P6000 EVAディスクアレイファミリとMicrosoft Exchange Serverの統合

前提条件

Microsoft Exchange Serverデータベースは、アプリケーションシステムのソースボリューム上にインストールする必要があります。以下のオブジェクトは、ソースボリュームに配置する必要があります。

- Microsoft Information Store (MIS)
- Key Management Service (KMS) (オプション)
- Site Replication Service (SRS) (オプション)

トランザクションログをバックアップする場合は、Microsoft Exchange Serverの循環ログを無効に設定します。

インストール手順

以下のData Protectorソフトウェアコンポーネントをインストールします。

- HP StorageWorks P6000 EVA SMI-S Agent – アプリケーションシステムとバックアップシステムの両方
- MS Exchange用統合ソフトウェア – アプリケーションシステムのみ

HP StorageWorks P6000 EVAディスクアレイファミリとMS SQLの統合

前提条件

Microsoft SQL Serverは、アプリケーションシステムにインストールする必要があります。ユーザーデータベースは、ディスクアレイのソースボリュームに配置することが必要ですが、システムデータベースは任意の場所にインストールできます。ただし、システムデータベースがディスクアレイ上にもインストールされている場合は、システムデータベースはユーザーデータベースとは異なるソースボリューム上にインストールすることが必要です。

インストール手順

以下のData Protectorソフトウェアコンポーネントを、アプリケーションシステムとバックアップシステムの両方にインストールします。

- HP StorageWorks P6000 EVA SMI-S Agent – アプリケーションシステムとバックアップシステムの両方
- MS SQL用統合ソフトウェア – アプリケーションシステムのみ

HP StorageWorks P9000 XPディスクアレイファミリ用統合ソフトウェア

HP StorageWorks P9000 XPディスクアレイファミリをData Protectorと統合する場合は、以下のData Protectorソフトウェアコンポーネントをアプリケーションシステムとバックアップシステムにインストールします。

- HP StorageWorks P9000 XP Agent
- General Media Agent

  General Media Agentコンポーネントは、バルクデータをバックアップする場合に、バックアップシステムにインストールします。またアーカイブログのバックアップやアプリケーションシステムへの復元を行う場合は、アプリケーションシステムにインストールします。

- Disk Agent

  Disk Agentコンポーネントは、ディスクイメージおよびファイルシステムのZDBを実行する場合に、アプリケーションシステムとバックアップシステムにインストールします。Disk Agentがインストールされていないクライアントは、ZDBバックアップ仕様を作成する際に、[アプリケーションシステム]ドロップダウンリストおよび[バックアップシステム]ドロップダウンリストに表示されません。

重要:

Microsoft Windows Server 2008システムでは、Data Protector HP StorageWorks P9000 XPディスクアレイファミリ用統合ソフトウェアを正常に動作させるために、2つのWindows Server 2008修正プログラムをインストールする必要があります。必要な修正プログラムのパッケージは、MicrosoftのWebサイト http://support.microsoft.com/kb/952790および http://support.microsoft.com/kb/973928からダウンロードしてください。

クラスターへのインストール

HP StorageWorks P9000 XPディスクアレイファミリ用統合ソフトウェアは、クラスター環境にインストールできます。サポート対象のクラスター構成とインストール要件の詳細は、『*HP Data Protector Zero Downtime Backup Administrator's Guide*』を参照してください。

他のアプリケーションの統合

HP StorageWorks P9000 XPディスクアレイファミリ用統合ソフトウェアをデータベースアプリケーションと組み合わせてインストールする場合は、この組み合わせに必要なData Protectorコンポーネントをアプリケーションシステムとバックアップシステムにインストール

し、この組み合わせ特有のインストール作業を実行してください。HP StorageWorks P9000 XPディスクアレイファミリ用統合ソフトウェアは、Oracle Server、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server、およびMicrosoftボリュームシャドウコピーサービスと組み合わせてインストールできます。

HP StorageWorks P9000 XPディスクアレイファミリとOracle Serverの統合

前提条件

- アプリケーションシステムと、バックアップセットZDBの方法のバックアップシステムには、以下のソフトウェアをインストールし、構成を完了しておく必要があります。
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net Services
  - SQL*Plus

  バックアップシステム上のOracleソフトウェアは、アプリケーションシステムと同じディレクトリにインストールする必要があります。また、バックアップシステム上のバイナリは、アプリケーションシステム上のバイナリと同一に設定する必要があります。これは、アプリケーションシステムからバックアップシステムにファイルとシステム環境をコピーするか、アプリケーションシステムと同じインストールパラメータを使用して、バックアップシステムでOracleバイナリのクリーンインストールを実行することにより、実現できます。

- アプリケーションシステム上のOracleデータファイルは、バックアップシステムにミラーリングされるHP StorageWorks P9000 XPディスクアレイファミリ LDEVにインストールする必要があります。

  バックアップセット方法を使用する場合で、Oracleデータファイルの一部がシンボリックリンクにインストールされている場合、バックアップシステムにもこれらのリンクを作成する必要があります。

  Oracleの制御ファイル、オンラインREDOログファイル、およびOracle SPFILEの配置場所は、次の2つのオプションから選択できます。
  - Oracle制御ファイル、オンラインREDOログファイル、およびOracle SPFILEを、Oracleデータファイルとは**異なる**ボリュームグループ(LVMを使用する場合)またはソースボリュームに配置する。

    この構成では、デフォルトでインスタントリカバリが使用可能です。
  - Oracle制御ファイル、オンラインREDOログファイル、およびOracle SPFILEを、Oracleデータファイルと**同じ**ボリュームグループ(LVMを使用する場合)またはソースボリュームに配置する。

    この構成では、デフォルトではインスタントリカバリは使用*不可*です。インスタントリカバリを使用可能にするには、ZDB_ORA_INCLUDE_CF_OLF、ZDB_ORA_INCLUDE_SPF、およびZDB_ORA_NO_CHECKCONF_IR omnirc変数を設定します。詳細については、

*HP Data Protector Zero Downtime Backup Integration Guide*を参照してください。

Oracleのアーカイブ REDOログファイルは、ソースボリュームに配置する必要はありません。

インストール手順

Install作業は、以下のとおり実行します。

1. Oracleのリカバリカタログデータベースをインストールします。このカタログデータベースは、非ミラー化ディスク上の個々のシステムにインストールすることをお勧めします。リカバリカタログは、登録しない状態で残しておきます。データベースのインストール方法については、Oracleのマニュアルを参照してください。
2. 以下のData Protectorソフトウェアコンポーネントをインストールします。
   - HP StorageWorks P9000 XP Agent – アプリケーションシステムとバックアップシステムの両方
   - Oracle用統合ソフトウェア – アプリケーションシステムとバックアップシステムの両方

注記:

- **バックアップシステムのData Protector Oracle用統合ソフトウェアコンポーネントは、バックアップセットZDB方式にのみ必要です。プロキシコピーZDBのプロキシコピー方法の場合は必要ありません。**
- **RACクラスター環境の場合、Oracleアプリケーションデータベースは、複数のOracleインスタンスによりアクセスされます。そのため、Oracleインスタンスを実行するすべてのシステムにData Protector Oracle用統合ソフトウェアおよびHP StorageWorks P9000 XP Agentコンポーネントをインストールしてください。**
- **Oracleリカバリカタログデータベースが個々のシステムにインストールされている場合は、そこにData Protectorソフトウェアコンポーネントをインストールする必要はありません。**

HP StorageWorks P9000 XPディスクアレイファミリとSAP R/3の統合

前提条件

- 以下のOracleソフトウェアを、アプリケーションシステムにインストールし、構成を完了しておく必要があります。

- Oracle Enterprise Server (RDBMS)
- Oracle Net Services
- SQL*Plus

- SAP準拠のZDBセッション(アプリケーションシステムではなくバックアップシステムで開始されたBRBACKUP)を実行する場合、バックアップシステムを構成します。詳細は、Oracle用のSAPデータベースガイド(スプリットミラーバックアップ、ソフトウェア構成)を参照してください。
- アプリケーションシステム上のデータベースは、ディスクイメージ、論理ボリューム、またはファイルシステムにインストールすることが可能です。
  - Oracleのデータファイルは、ディスクアレイに配置する必要があります。
  - オンラインバックアップの場合、オンラインのREDOログをディスクアレイに配置する必要はありません。オンラインSAP対応ZDBセッションは例外です。コントロールファイルはディスクアレイに配置する必要があります。
  - オフラインバックアップの場合、コントロールファイルとオンラインのREDOログはディスクアレイに配置する必要があります。
  - アーカイブされたREDOログファイルは、ディスクアレイに配置する必要はありません。

  Oracle制御ファイル、オンラインREDOログファイル、およびOracle SPFILEを、Oracleデータファイルと*同じ*LVMボリュームグループまたはソースボリュームに配置する場合、Data ProtectorのZDB_ORA_NO_CHECKCONF_IR、ZDB_ORA_INCLUDE_CF_OLF、ZDB_ORA_INCLUDE_SPF omnirc変数を設定します。設定しないと、ZDB-to-diskセッションとZDB-to-disk+tapeセッションを実行できません。詳細は、『*HP Data Protector Zero Downtime Backup Integration Guide*』を参照してください。

注記:

Oracleデータファイルの一部がシンボリックリンクにインストールされている場合、バックアップシステムにもリンクを作成します。

***UNIXの場合のみ*、Oracleデータベースがrawパーティション(rawディスクまたはraw論理ボリューム)にインストールされている場合、アプリケーションシステムとバックアップシステムでのボリューム/ディスクグループ名が同じであることを確認してください。**

- UNIXの場合、アプリケーションシステムに以下のユーザーが存在しているかどうかを確認します。
  - プライマリグループがdbaのora0RACLE_SID
  - UNIXグループsapsysに属する0RACLE_SIDadm

- SAP R/3ソフトウェアは、アプリケーションシステムに正しくインストールする必要があります。

  SAP R/3のインストール後にアプリケーションシステムにインストールする必要がある標準ディレクトリのリストは、以下のとおりです。

注記:

ディレクトリの場所は、環境変数(UNIXシステムの場合)またはレジストリ(Windowsシステムの場合)によって異なります。詳細は、SAP R/3のマニュアルを参照してください。

- ORACLE_HOME/dbs (UNIXシステム)

  ORACLE_HOME¥database (Windowsシステム) - OracleおよびSAP R/3プロファイル
- ORACLE_HOME/bin (UNIXシステム)または

  ORACLE_HOME¥bin (Windowsシステム) - Oracleバイナリ
- SAPDATA_HOME/sapbackup (UNIXシステム)

  SAPDATA_HOME¥sapbackup (Windowsシステム) - BRBACKUPログファイルが置かれるSAPBACKUPディレクトリ
- *SAPDATA_HOME*/saparch (UNIXシステム)

  SAPDATA_HOME¥saparch (Windowsシステム) - BRARCHIVEログファイルが置かれるSAPARCHディレクトリ
- SAPDATA_HOME/sapreorg (UNIXシステム)

  SAPDATA_HOME¥sapreorg (Windowsシステム)
- SAPDATA_HOME/sapcheck (UNIXシステム)

  SAPDATA_HOME¥sapcheck (Windowsシステム)
- SAPDATA_HOME/saptrace (UNIXシステム)

  SAPDATA_HOME¥saptrace (Windowsシステム)
- /usr/sap/ORACLE_SID/SYS/exe/run (UNIXシステム)

  c:¥Oracle¥ORACLE_SID¥sys¥exe¥run (Windowsシステム)

注記:

インスタントリカバリを行う場合、sapbackup、saparch、およびsapreorgの各ディレクトリが、Oracleデータファイルとは異なるソースボリュームに存在していることを確認します。

UNIXシステム

UNIXシステムでは、最後の6つのディレクトリが前述の場所にない場合、適切なリンクを作成してください。

UNIXシステムの場合、ディレクトリ/usr/sap/ORACLE_SID/SYS/exe/runの所有者は、UNIXユーザーora*ORACLE_SID*でなければなりません。SAP R/3ファイルの所有者は、UNIXユーザーora*ORACLE_SID*であり、setuidビットがセットされた(chmod 4755 ...) UNIXグループdbaに属していなければなりません。例外はBRRESTOREファイルの場合で、その所有者はUNIXユーザー*ORACLE_SID*admでなければなりません。

UNIXでの例

*ORACLE_SID*がPROの場合、/usr/sap/PRO/SYS/exe/runディレクトリ内のパーミッションは、以下のとおりに設定する必要があります。

```
-rwsr-xr-x   1 orapro dba 4598276
Apr 17  2010 brarchive -rwsr-xr-x   1 orapro dba 4750020 Apr 17  2010 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  2010 brconnect -rwsr-xr-x   1 proadm
sapsys 430467 Apr 17  2010

brrestore -rwsr-xr-x   1 orapro dba 188629 Apr 17  2010 brtools
```

インストール手順

1. SAP R/3 BRTOOLSを、アプリケーションシステムにインストールします。
2. 以下のData Protectorソフトウェアコンポーネントを、アプリケーションシステムとバックアップシステムの両方にインストールします。
   - HP StorageWorks P9000 XP Agent
   - SAP R/3用統合ソフトウェア
   - Disk Agent

注記:

SAP R/3 Integrationは、バックアップシステムでBRBACKUPが開始されるSAP対応ZDBセッションを実行する場合にのみインストールする必要があります。

Windowsシステムの場合、Data Protectorソフトウェアコンポーネントを SAP R/3管理者用ユーザーアカウントを使用してインストールする必要があります。また、このアカウントは、SAP R/3インスタンスが実行されているシステム上のORA_DBAローカルグループかORA_SID_DBAローカルグループに含まれている必要があります。

HP StorageWorks P9000 XPディスクアレイファミリとMicrosoft Exchange Serverの統合

前提条件

Microsoft Exchange Serverデータベースは、アプリケーションシステムのHP StorageWorks P9000 XPディスクアレイファミリボリューム(LDEV)にインストールする必要があります。このボリュームは、バックアップシステムにミラーリングされます。ミラーリングは、HP BC P9000 XPまたはHP CA P9000 XPで設定でき、データベースはファイルシステムにインストールされます。以下のオブジェクトは、ミラーリングされるボリュームに配置する必要があります。

- Microsoft Information Store (MIS)
- Key Management Service (KMS) (オプション)
- Site Replication Service (SRS) (オプション)

トランザクションログをバックアップする場合は、Microsoft Exchange Serverの循環ログを無効に設定します。

インストール手順

以下のData Protectorソフトウェアコンポーネントをインストールします。

- HP StorageWorks P9000 XP Agent – アプリケーションシステムとバックアップシステムの両方
- MS Exchange用統合ソフトウェア – アプリケーションシステムのみ

HP StorageWorks P9000 XPディスクアレイファミリとMicrosoft SQL Serverの統合

前提条件

Microsoft SQL Serverは、アプリケーションシステムにインストールする必要があります。ユーザーデータベースは、ディスクアレイのソースボリュームに配置することが必要ですが、システムデータベースは任意の場所にインストールできます。ただし、システムデータベースがディスクアレイ上にもインストールされている場合は、システムデータベースはユーザーデータベースとは異なるソースボリューム上にインストールすることが必要です。

インストール手順

以下のData Protectorソフトウェアコンポーネントを、アプリケーションシステムとバックアップシステムの両方にインストールします。

- HP StorageWorks P9000 XP Agent
- MS SQL用統合ソフトウェア

HP StorageWorks P4000 SANソリューション用統合ソフトウェア

HP StorageWorks P4000 SANソリューションをData Protectorと統合する場合は、以下のData Protectorソフトウェアコンポーネントをアプリケーションシステムとバックアップシステムにインストールします。

- MS ボリュームシャドウコピー用統合ソフトウェア
- HP StorageWorks P4000 Agent

EMC Symmetrix用統合ソフトウェア

EMC SymmetrixをData Protectorと統合する場合は、以下のData Protectorソフトウェアコンポーネントをアプリケーションシステムとバックアップシステムにインストールします。

- EMC Symmetrix Agent (SYMA)

  EMC Symmetrix Agentコンポーネントをリモートでインストールする前に、次の2つのEMCコンポーネントをインストールします。

  - EMC Solution Enabler
  - EMC Symmetrix TimeFinderまたはEMC Symmetrix Remote Data Facility (SRDF) マイクロコードとライセンス

- General Media Agent

  General Media Agentコンポーネントは、バルクデータをバックアップする場合に、バックアップシステムにインストールします。またアーカイブログのバックアップやアプ

リケーションシステムへの復元を行う場合は、アプリケーションシステムにインストールします。

- Disk Agent

  Disk Agentコンポーネントは、ディスクイメージおよびファイルシステムのZDBを実行する場合に、アプリケーションシステムとバックアップシステムにインストールします。Disk Agentがインストールされていないクライアントは、ZDBバックアップ仕様を作成する際に、[アプリケーションシステム]ドロップダウンリストおよび[バックアップシステム]ドロップダウンリストに表示されません。

クラスターへのインストール

EMC Symmetrix用統合ソフトウェアは、クラスター環境にインストールできます。サポート対象のクラスター構成とインストール要件の詳細は、『*HP Data Protector Zero Downtime Backup Administrator's Guide*』を参照してください。

他のアプリケーションの統合

EMC Symmetrix用統合ソフトウェアをデータベースアプリケーションと組み合わせてインストールする場合は、この組み合わせに必要なData Protectorコンポーネントをアプリケーションシステムとバックアップシステムにインストールし、この組み合わせ特有のインストール作業を実行してください。EMC Symmetrix用統合ソフトウェアは、OracleとSAP R/3と組み合わせてインストールできます。

EMC Symmetrix用統合ソフトウェアとOracleの組み合わせ

前提条件

- 以下のソフトウェアを、アプリケーションシステムにインストールし、構成を完了しておく必要があります。
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net Services
  - SQL*Plus
- アプリケーションシステムで使用されるOracleデータベースファイルは、バックアップシステムにミラーリングされるEMC Symmetrixデバイスにインストールする必要があります。

  データベースは、ディスクイメージ、論理ボリューム、またはファイルシステムにインストールすることが可能です。以下のOracleファイルは、ミラーリングする必要があります。
  - データファイル
  - 制御ファイル

- オンラインREDOログファイル

アーカイブREDOログファイルは、非ミラー化ディスクに配置する必要があります。

インストール手順

Install作業は、以下のとおり実行します。

1. Oracleのリカバリカタログデータベースをインストールします。このカタログデータベースは、非ミラー化ディスク上の個々のシステムにインストールすることをお勧めします。リカバリカタログは、登録しない状態で残しておきます。データベースのインストール方法については、Oracleのマニュアルを参照してください。
2. 以下のData Protectorソフトウェアコンポーネントをインストールします。
   - EMC Symmetrix Agent－アプリケーションシステムとバックアップシステムの両方
   - Oracle用統合ソフトウェア－アプリケーションシステムとバックアップシステムの両方

注記：

- **バックアップシステムのData Protector Oracle用統合ソフトウェアコンポーネントは、バックアップセットZDB方式にのみ必要です。プロキシーコピーZDBのプロキシーコピー方法の場合は必要ありません。**
- **RACクラスター環境の場合、Oracleアプリケーションデータベースは、複数のOracleインスタンスによりアクセスされます。そのため、Oracleインスタンスを実行するすべてのシステムにData Protector Oracle IntegrationおよびEMC Symmetrix Agentコンポーネントをインストールしてください。**
- **Oracleリカバリカタログデータベースが個々のシステムにインストールされている場合は、そこにData Protectorソフトウェアコンポーネントをインストールする必要はありません。**

EMC Symmetrix用統合ソフトウェアとSAP R/3との組み合わせ

前提条件

- 以下のOracleソフトウェアを、アプリケーションシステムにインストールし、構成を完了しておく必要があります。
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net8ソフトウェア
  - SQL*Plus

- SAP準拠のZDBセッション(アプリケーションシステムではなくバックアップシステムで開始されたBRBACKUP)を実行する場合、バックアップシステムを構成します。詳細は、Oracle用のSAPデータベースガイド(スプリットミラーバックアップ、ソフトウェア構成)を参照してください。
- アプリケーションシステム上のデータベースは、ディスクイメージ、論理ボリューム、またはファイルシステムにインストールすることが可能です。
  - Oracleのデータファイルは、ディスクアレイに配置する必要があります。
  - オンラインバックアップの場合、オンラインのREDOログをディスクアレイに配置する必要はありません。オンラインSAP対応ZDBセッションは例外です。コントロールファイルはディスクアレイに配置する必要があります。
  - オフラインバックアップの場合、コントロールファイルとオンラインのREDOログはディスクアレイに配置する必要があります。
  - アーカイブされたREDOログファイルは、ディスクアレイに配置する必要はありません。

注記:

Oracleデータファイルの一部がシンボリックリンクにインストールされている場合、バックアップシステムにもリンクを作成します。

UNIXの場合のみ、Oracleデータベースがrawパーティション(rawディスクまたはraw論理ボリューム)にインストールされている場合、アプリケーションシステムとバックアップシステムでのボリューム/ディスクグループ名が同じであることを確認してください。

- UNIXの場合、アプリケーションシステムに以下のユーザーが存在しているかどうかを確認します。
  - プライマリグループがdbaのora0RACLE_SID
  - UNIXグループsapsysに属する0RACLE_SIDadm
- SAP R/3ソフトウェアは、アプリケーションシステムに正しくインストールする必要があります。

  SAP R/3のインストール後にアプリケーションシステムにインストールする必要がある標準ディレクトリのリストは、以下のとおりです。

注記:

ディレクトリの場所は、環境変数によって変わります。詳細は、SAP R/3のマニュアルを参照してください。

- ORACLE_HOME/dbs – OracleおよびSAP R/3のプロファイル
- ORACLE_HOME/bin – Oracleバイナリファイル
- SAPDATA_HOME/sapbackup – BRBACKUPログファイルが置かれるSAPBACKUPディレクトリ
- SAPDATA_HOME/saparch – BRARCHIVEログファイルが置かれるSAPARCHディレクトリ
- SAPDATA_HOME/sapreorg
- SAPDATA_HOME/sapcheck
- SAPDATA_HOME/saptrace
- /usr/sap/ORACLE_SID/SYS/exe/run

注記:

インスタントリカバリを行う場合、sapbackup、saparch、およびsapreorgの各ディレクトリが、Oracleデータファイルとは異なるソースボリュームに存在していることを確認します。

最後の6つのディレクトリが前述の場所にない場合は、適切なリンクを作成してください。

ディレクトリ/usr/sap/ORACLE_SID/SYS/exe/runの所有者は、UNIXユーザーora*ORACLE_SID*でなければなりません。SAP R/3ファイルの所有者は、UNIXユーザーora*ORACLE_SID*であり、setuidビットがセットされた(chmod 4755 ...) UNIXグループdbaに属していなければなりません。例外はBRRESTOREファイルの場合で、その所有者はUNIXユーザー*ORACLE_SID*admでなければなりません。

例

*ORACLE_SID*がPROの場合、/usr/sap/PRO/SYS/exe/runディレクトリ内のパーミッションは、以下のとおりに設定する必要があります。

```
-rwsr-xr-x   1 orapro dba 4598276
Apr 17  2010 brarchive -rwsr-xr-x   1 orapro dba 4750020 Apr 17  2010 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  2010 brconnect -rwsr-xr-x   1 proadm
sapsys 430467 Apr 17  2010 brrestore -rwsr-xr-x   1 orapro dba 188629 Apr 17
2010 brtools
```

インストール手順

1. SAP R/3 BRTOOLSを、アプリケーションシステムにインストールします。

2. 以下のData Protectorソフトウェアコンポーネントを、アプリケーションシステムとバックアップシステムの両方にインストールします。
   - EMC Symmetrix Agent
   - SAP R/3用統合ソフトウェア
   - Disk Agent

注記:

SAP R/3 Integrationは、バックアップシステムでBRBACKUPが開始されるSAP対応ZDBセッションを実行する場合にのみインストールする必要があります。

EMC Symmetrix用統合ソフトウェアとMicrosoft SQL Serverとの組み合わせ

前提条件

Microsoft SQL Serverは、アプリケーションシステムにインストールする必要があります。ユーザーデータベースは、ディスクアレイのソースボリュームに配置することが必要ですが、システムデータベースは任意の場所にインストールできます。ただし、システムデータベースがディスクアレイ上にもインストールされている場合は、システムデータベースはユーザーデータベースとは異なるソースボリューム上にインストールすることが必要です。

インストール手順

以下のData Protectorソフトウェアコンポーネントを、アプリケーションシステムとバックアップシステムの両方にインストールします。

- EMC Symmetrix Agent
- MS SQL用統合ソフトウェア

VLS自動移行クライアント

Data Protectorメディアコピー機能では、バックアップ実行後にメディアをコピーできます。HP StorageWorks仮想ライブラリシステム(VLS)との統合によって、内部VLSコピー機能をData Protectorメディア管理機能や監視機能と組み合わせたソリューションが提供されることとなり、メディアコピー機能が強化されました。

Data ProtectorとVLSの自動移行機能を統合してスマートメディアコピー機能を実行するには、VLS自動移行Data Protectorソフトウェアコンポーネントをインストールします。

前提条件

この場合、以下の手順を実行します。

1. 必要に応じてCommand View VLSを使用してVLS仮想記憶領域を構成します。詳細については、VLSのドキュメントを参照してください。
2. 1つまたは複数の物理テープライブラリをVLSに接続します。
3. Data ProtectorセルにVLSクライアントをインポートします。

各国語版Data Protectorユーザーインタフェースのインストール

Data Protector 6.20には、WindowsおよびUNIXシステム上で動作する各国語版Data Protectorユーザーインタフェースがあります。これは、各国語版のData Protector GUIおよびCLIで構成されています。各国語版のドキュメント(ガイドおよびオンラインヘルプ)も用意されています。各国語版にローカライズされたData Protectorドキュメントセットについては、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。

注記:

デフォルトでは、Data Protectorのインストール時に、サポートされるすべての言語の言語サポートがインストールされ、システムの地域設定にあわせてData Protectorユーザーインタフェースが起動されます。

トラブルシューティング

英語以外の言語サポートをインストールした後、英語のData Protectorの元のGUIが起動した場合は、以下を確認してください。

1. 以下のファイルが存在するかを確認します。

   フランス語のサポートの場合:

   - Windowsの場合: Data_Protector_home¥bin¥OmniFra.dll
   - HP-UXの場合: /opt/omni/lib/nls/fr.iso88591/omni.cat
   - Solarisの場合: /opt/omni/lib/nls/fr.ISO8859-1/omni.cat

   日本語のサポートの場合:

   - Windowsの場合: Data_Protector_home¥bin¥OmniJpn.dll
   - HP-UXの場合: /opt/omni/lib/nls/ja.eucJP/omni.catおよび/opt/omni/lib/nls/ja.SJIS/omni.cat
   - Solarisの場合: /opt/omni/lib/nls/ja.eucJP/omni.catおよび/opt/omni/lib/nls/ja.PCK/omni.cat

   簡体字中国語のサポートの場合:

   - Windowsの場合:Data_Protector_home¥bin¥OmniChs.dll
   - HP-UXの場合:/opt/omni/lib/nls/zh_CN.gb18030/omni.catおよび/opt/omni/lib/nls/zh_CN.gb18030/omni.cat
   - Solarisの場合:/opt/omni/lib/nls/zh_CN.GB18030/omni.catおよび/opt/omni/lib/nls/zh_CN.GB18030/omni.cat

2. システムの地域設定を確認します。

   - Windowsの場合: Windowsのコントロールパネルで、[地域のオプション]をクリックし、地域と言語の設定で適切な言語が選択されているかを確認してください。
   - UNIXの場合: 以下のコマンドを実行して地域設定(ロケール)環境を設定してください。

     export LANG=lang locale

     ここでは、*lang*は次のフォーマットでロケール環境設定を示しています。
     language[_territory].codeset.

     たとえば、日本語ロケールの場合はja_JP.eucJP、ja_JP.SJIS、またはja_JP.PCK、簡体字中国語ロケールの場合はzh_CN.GB18030、フランス語ロケールの場合はfr_FR.iso88591となります。LANG変数のcodeset部分は必須であり、対応するディレクトリ名のcodeset部分と一致している必要があります。

各国語版Data Protectorマニュアルのインストール

Windowsシステムへの各国語版Data Protectorマニュアルのインストール

ローカルインストール

Windowsシステムに各国語版Data Protectorマニュアルをローカルにインストールするには、**セットアップ**ウィザードの[**カスタムセットアップ**]ページで、必要なコンポーネントを選択します。図23(189ページ)を参照してください。

ローカルインストール手順については、「Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール」(44ページ)を参照してください。

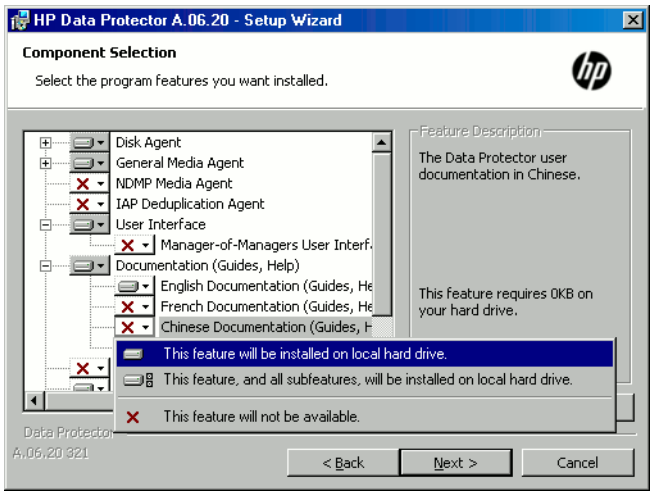


図 23 セットアップ時の各国語版マニュアルの選択

リモートインストール

インストールサーバーを利用してData Protector各国語版マニュアルをリモートで配布するには、[**コンポーネント追加**]ウィザードの[**コンポーネント選択**]ページで、必要な各国語版マニュアルを選択します。図24(190ページ)を参照してください。

Data Protectorソフトウェアコンポーネントをクライアントにリモートで追加する手順は、「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

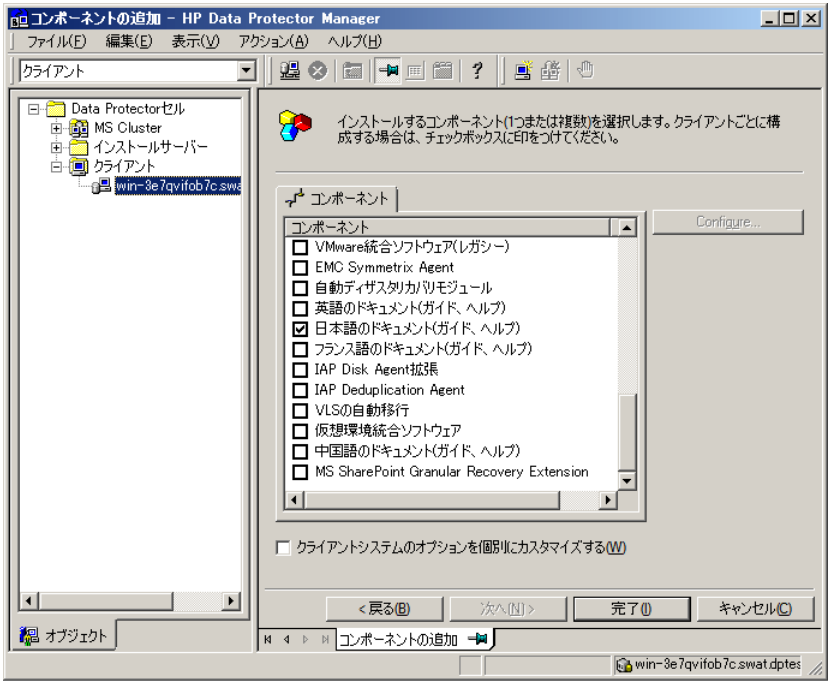


図 24 各国語版マニュアルのリモートでのインストール

UNIXシステムへの各国語版Data Protectorマニュアルのインストール

ローカルインストール

日本語、フランス語または簡体字中国語のマニュアルのローカルインストールは、omnisetup.shコマンドを使用して、Data Protectorクライアント上でのみ行えます。必要な言語サポートに応じて、jpn_ls、fra_ls、またはchs_lsソフトウェアコンポーネントを指定してください。手順の詳細は、「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)を参照してください。

Data Protector Cell Managerまたはインストールサーバーのインストールにswinstall、pkgadd、またはrpmユーティリティを使用している場合は、英語版のマニュアルしかインストールできません。各国語版Data ProtectorマニュアルをCell Managerまたはインストールサーバーと同じシステムにインストールしたい場合は、それらの言語パックをリモートでインストールする必要があります。

リモートインストール

インストールサーバーを利用してData Protector各国語版マニュアルをリモートで配布するには、**[コンポーネント追加]**ウィザードの**[コンポーネント選択]**ページで、必要な各国語版マニュアルを選択します。図24(190ページ)を参照してください。

Data Protectorソフトウェアコンポーネントをクライアントにリモートで追加する手順は、「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

Data Protectorシングルサーバー版のインストール

Data Protectorのシングルサーバー版(SSE: Single Server Edition)は、1つのCell Managerに接続された1台のデバイス上でのみバックアップを実行するような、小規模な環境向けに設計されたものです。シングルサーバー版は、サポート対象のWindowsプラットフォーム、およびサポート対象のHP-UXまたはSolarisプラットフォーム上で使用できます。

Cell Managerと(必要に応じて)インストールサーバーをインストールする手順は、「Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール」(44ページ)を参照してください。

制限事項

SSEライセンスを使用する場合、以下の制限があることに注意してください。

Windows用SSEの制限

- SSEでバックアップを行う場合、一度にバックアップできるのは1台のCell Managerに接続されている1台のデバイスのみです。
- 10スロットのDDSオートチェンジャを1台だけ使用できます。
- UNIX (HP-UX)クライアントとサーバーはサポートされていません。UNIXのマシンに対してバックアップを行おうとすると、セッションが中止されます。
- Windows用Cell Managerを使用するセルの場合は、バックアップ対象はWindowsクライアントに限られます。Novell Netwareクライアントへのバックアップはサポートされていません。
- 拡張製品をSSEに追加することはできません。
- SSEでクラスター化を行うことはできません。
- SSEでディザスタリカバリを行うことはできません。

Windowsクライアントの数に制限はありません。

サポート対象のデバイスについては、『HP Data Protector製品案内、ソフトウェアノート、リファレンス』を参照してください。

HP-UXおよびSolaris用のSSEの制限事項

- SSEでバックアップを行う場合、一度にバックアップできるのは1台のCell Managerに接続されている1台のデバイスのみです。
- 10スロットのDDSオートチェンジャを1台だけ使用できます。
- UNIX用Cell Managerでは、サーバーのバックアップはできません。UNIX、Windows、Solaris、およびNovell NetWareの各クライアントのバックアップのみが可能です。
- 拡張製品をSSEに追加することはできません。
- SSEでクラスター化を行うことはできません。

クライアント(UNIX、Windows)の数に制限はありません。

サポート対象のデバイスについては、『HP Data Protector製品案内、ソフトウェアノート、リファレンス』を参照してください。

パスワードのインストール

Cell Managerへのパスワードの詳しいインストール手順は、「Data Protectorパスワード」(327ページ)を参照してください。

Data Protector Web Reportingのインストール

Data Protector Web Reportingは、デフォルトで他のData Protectorコンポーネントとともにローカルシステムにインストールされます。

したがって、システムからローカルに使用する場合は、このコンポーネントを明示的にインストールする必要はありません。Data Protector Web Reportingは、Webサーバーにもインストールできます。

前提条件

システムでData Protector Web Reportingを使用する場合の前提条件と制限は、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。

設置

Data Protector Web ReportingをWebサーバーにインストールするには、以下の手順に従ってください。

1. 以下のData Protector Java Reportingファイルをサーバーにコピーします。コピー先のサーバーは、Data Protectorクライアントでなくてもかまいません。
   - WindowsシステムにData Protectorユーザーインタフェースをインストールしている場合は、以下のディレクトリからWeb Reporting用のファイルをコピーします。

     Data_Protector_home¥java¥bin
   - UNIXシステムにData Protectorユーザーインタフェースをインストールしている場合は、以下のディレクトリからWeb Reporting用のファイルをコピーします。

     /opt/omni/java/bin
2. ブラウザでWebReporting.htmlファイルを開くと、Data Protector Web Reportingが表示されます。

   このファイルは、Web Reportingのユーザーが完全なURLを通じてアクセスできるように設定しておく必要があります。たとえば、イントラネットサイトからこのファイルにアクセスするためのリンクなどを用意します。

ヒント:

デフォルトでは、Data Protector Web Reportingはパスワードなしで使用できます。Web Reportingへのアクセスを制限したい場合は、パスワード保護を追加できます。手順については、オンラインヘルプの索引「Webレポート、アクセスの制限」を参照してください。

この次に行う作業

Installが完了したら、オンラインヘルプの索引「Webレポートのインタフェース、通知の構成」を参照して、構成上の問題および独自のレポートを作成する方法を確認してください。

MC/ServiceGuardへのData Protectorのインストール

Data Protectorは、HP-UX用およびLinux用のMC/ServiceGuard (MC/SG)をサポートしています。サポート対象オペレーティングシステムのバージョンの詳細は、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。

Cell Managerをクラスター対応にする場合は、ライセンスで仮想サーバーIPアドレスを使用する必要があります。

クラスター対応Cell Managerのインストール

前提条件

MC/SeviceGuardにData Protector Cell Managerをインストールする前に、以下の条件が満たされていることを確認してください。

- 1次Cell Managerとなるシステムと2次Cell Managerとなるシステムが決定されていること。これらのシステムのすべては、MC/ServiceGuardがインストールされ、クラスターのメンバーとして構成されていること。
- Data Protector Cell Manager (推奨パッチ適用済み)と、クラスター内に必要な統合ソフトウェア用のその他すべてのData Protectorソフトウェアコンポーネントが、一次ノードと各二次ノードにインストールされていること。

  これらのインストール手順は、Cell Managerシステムを標準構成でインストールする場合と同じです。「Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール」(44ページ)を参照してください。

この次に行う作業

Installが完了したら、インストールした1次Cell Managerと2次Cell Manager、およびCell Managerパッケージを構成する必要があります。オンラインヘルプの索引「クラスター、MC/ServiceGuard」を参照して、MC/ServiceGuardとData Protectorとの構成の詳細をご確認ください。

インストールサーバーのクラスターノードへのインストール

インストールサーバーを二次MC/ServiceGuardノードにインストールし、リモートインストールに利用できます(「UNIX用のインストールサーバーのインストール」(63ページ))。

クラスター対応クライアントのインストール

重要:

Data Protectorクラスター対応クライアントは、クラスター内のすべてのノードにインストールする必要があります。

Install手順は、Data Protectorを標準構成のUNIXクライアントにインストールする場合と同じです。詳細な手順については、「HP-UXクライアントのインストール」(99ページ)と「Linuxクライアントのインストール」(109ページ)を参照してください。

この次に行う作業

Installが完了したら、仮想サーバー(クラスターパッケージで指定されたホスト名)をData Protectorセルにインポートする必要があります。「セルへのクラスター対応クライアントのインポート」(217ページ)を参照してください。

オンラインヘルプの索引「*構成*」を参照して、バックアップデバイスおよびメディアプールの作成方法、またはData Protectorのその他の構成タスクの詳細をご確認ください。

Microsoft Cluster ServerへのData Protectorのインストール

Microsoft Cluster Server用統合ソフトウェアでサポートされているオペレーティングシステムについては、http://www.hp.com/support/manualsの最新のサポート一覧を参照してください。

注記:

Cell Managerをクラスター対応にする場合は、Cell Managerの仮想サーバーIPアドレスをライセンスに使用する必要があります。

クラスター対応Cell Managerのインストール

前提条件

クラスター対応のData Protector Cell Managerをインストールするには、次の前提条件を満たす必要があります。

- すべてのクラスターノード上にクラスター機能が正しくインストールされていること。たとえば、ディスク共有の問題なしに、グループをノード間で必要な回数だけ移動できる必要があります。
- クラスター内に以下の名前を持つリソースが存在しないこと。

  OBVS_MCRS、OBVS_VELOCIS、OmniBack_Share

  Data Protectorでは、これらの名前がData Protector仮想サーバーに使用されます。そのようなリソースが存在する場合は、削除するか名前を変更してください。

  以下の手順に従ってください。

  1. **[スタート]** > **[プログラム]** > **[管理ツール]** > **[クラスターアドミニストレータ]**をクリックします。

2. リソースのリストを確認し、必要な場合はリソースの削除または名前の変更を行います。

- クラスター内の最低1つのグループにファイルクラスータリソースが定義されていること。Data Protectorは、このファイルクラスターリソースの一部のデータファイルを指定したフォルダにインストールします。

  Windows Server 2008の場合、データファイルはインストール時にユーザーが選択した共有フォルダの下にある*File Server*リソースにインストールされます。

  その他のWindowsシステムの場合、データファイルはファイルクラスターリソースが作成されたときに指定したフォルダの下にある*File Share*リソースにインストールされます。

  ファイルクラスターリソースを定義する方法については、各クラスターのマニュアルを参照してください。ファイルクラスターリソースのファイル共有名をOmniBackにすることはできません。

- ファイルクラスターリソースと同じグループ内に仮想サーバーが存在しない場合は、登録済みのIPアドレスのうち未使用のものを使って新しい仮想サーバーを作成し、これをネットワーク名と関連付けます。
- Data Protectorのインストール先となるファイルクラスターリソースのIPアドレス、ネットワーク名、および物理ディスクが、ファイルクラスターリソースの依存関係に含まれていること。これでData Protectorクラスターグループが、他のグループと関係なく、いずれのノード上でも実行できることを確認できます。
- クラスター管理者だけがファイルクラスターリソースの共有フォルダへのアクセス権(フルアクセス権限)を持つことを確認します。
- Data Protectorは、すべてのクラスターノード上で同じ場所(ドライブとパス名)にインストールされます。これらのインストール場所に空きがあることを確認してください。
- クラスター対応Cell Managerのインストールをネットワーク共有から開始する場合、すべてのクラスターノードからこの共有にアクセスする必要があります。
- あらゆるクラスターノードで、その他のMicrosoftインストーラーベースのインストールが実行されていないことを確認してください。
- クラスターの各システム(ノード)が適切に稼動していること。
- Windows Server 2008上でMicrosoft Cluster Service (MSCS)が実行されているサーバークラスターに、クラスター対応のData Protector Cell Managerをインストールできるようにするには、「Data Protectorインストールのための Windows Server 2008上で実行するMicrosoftサーバークラスターの準備」(390ページ)で説明されている手順を実行します。

留意事項

- ファイルクラスターリソースの共有フォルダに直接アクセスできるように、ファイルクラスターリソースがアクティブになっているシステム(ノード)上のクラスターサービスアカウ

ントでセットアップを起動すること。リソースのオーナー(リソースがアクティブになっているシステム)は、クラスター管理ユーティリティを使うと確認できます。

- クラスター対応Data Protector Cell Managerをインストールおよび構成するために、インストール時に以下のユーザー権限のドメインアカウントを用意すること。
  - Cell Managerシステムに対する管理者権限を付与します。
  - クラスター内でのクラスター管理者権限を付与します。
  - [パスワードを無期限にする]オプションを選択します。
  - [サービスとしてログオン]オプションを選択します。
  - [ユーザーはパスワードを変更できない]オプションを選択します。
  - ログオン時間をすべて可能に設定します。

重要:

Microsoft Cluster Serverをインストールするには、すべてのクラスターシステム(ノード)に対する管理者権限を付与されたアカウントが必要です。Data Protectorのインストールにも、このアカウントを使用する必要があります。そうしなかった場合は、Data Protectorのサービスが、クラスター対応モードではなく通常のモードで稼動することになります。

ローカルインストール手順

クラスター対応Data Protector Cell Managerは、DVD-ROMからローカルにインストールする必要があります。この場合、以下の手順を実行します。

1. WindowsインストールDVD-ROM

   Windows Server 2008の場合は、[ユーザーアカウント制御]ダイアログボックスが表示されます。**[続行]**をクリックしてインストールを続けます。

2. HP Data Protectorウィンドウで**[インストールData Protector]**を選択し、Data Protectorのセットアップ用ウィザードを開始します。

3. セットアップ用ウィザードの指示に従って操作を行い、ライセンス契約を十分にお読みください。記載内容に同意する場合は、**[Next]**をクリックして次に進みます。

4. [Installation Type]ページで、[Cell Manager]を選択します。[Next]をクリックすると、選択したData Protector Cell Managerソフトウェアがインストールされます。

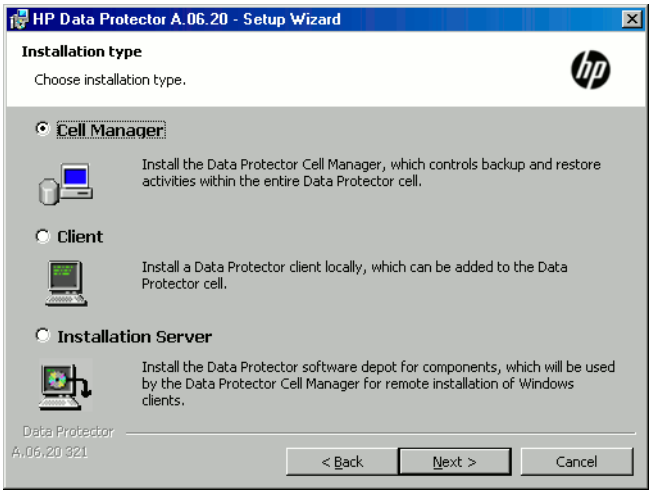


図 25 インストールの種類の選択

5. セットアップはクラスター環境で実行していることを自動的に検出します。[Install cluster-aware Cell Manager]を選択して、クラスターセットアップを有効にします。

   クラスターグループ、仮想ホスト名と、Data Protectorの共有ファイルおよびデータベースのインストール先となるファイルクラスターリソースを選択します。

注記:

[Install Cell Manager on this node only]を選択した場合、Cell Managerはクラスター対応にはなりません。詳細については、「Windows用Cell Managerのインストール」(55ページ)を参照してください。

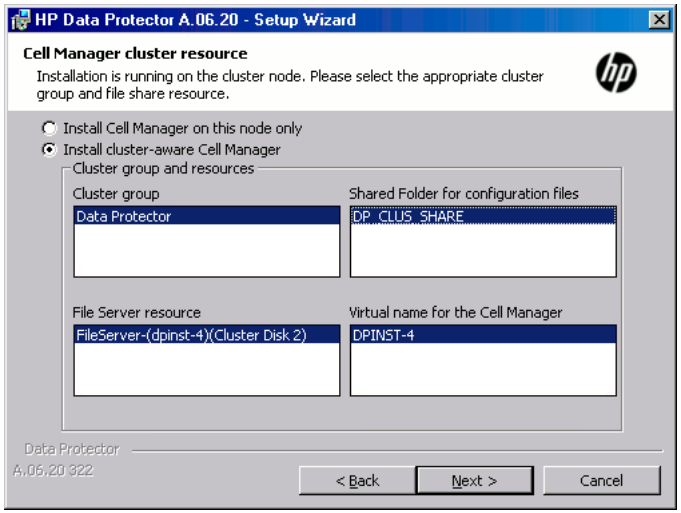


図 26 SWindows Server 2008でのクラスターリソースの選択

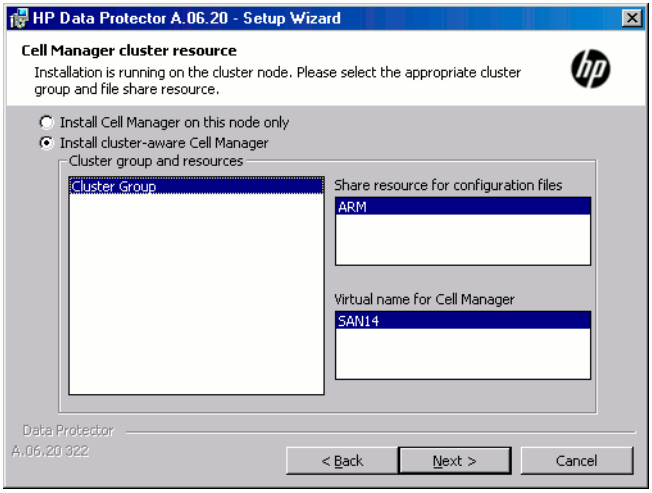


図 27 Windowsシステムでのクラスターリソースの選択

6. Data Protectorサービスの起動に使用されるアカウントのユーザー名とパスワードを入力します。

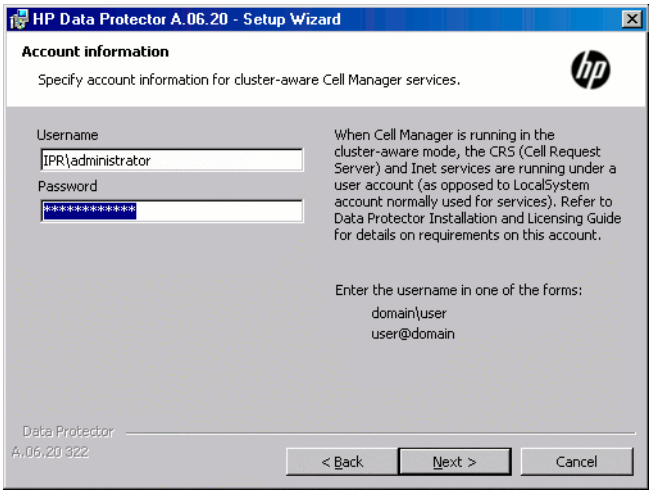


図 28 アカウント情報の入力

7. Data Protectorをデフォルトフォルダにインストールする場合には、[Next]をクリックします。

   それ以外の場合は、[Change]をクリックして[Change Current Destination Folder]ウィンドウを開き、別のパスを入力します。

8. [Component Selection]ウィンドウで、すべてのクラスターノードおよびクラスター仮想サーバーにインストールするコンポーネントを選択します。[Next]をクリックします。

   MS Cluster Supportファイルは自動的にインストールされます。

   選択されたコンポーネントは、クラスター内のすべてのノードにインストールされます。

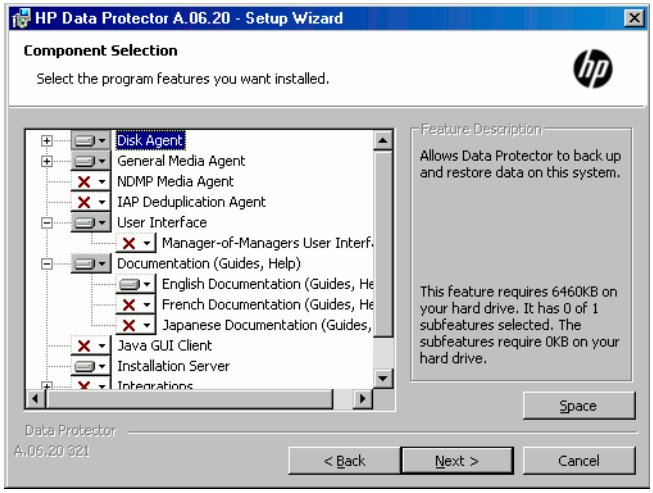


図 29 コンポーネント選択ページ

9. *Data Protectorによってシステムに*Windows*ファイアウォールが検出されると、*[Windows Firewall configuration]ページが表示されます。Data Protectorのセットアッププログラムによって、必要なすべてのData Protector実行可能ファイルが登録されます。デフォルトでは、[Initially, enable newly registered Data Protector binaries to open ports as needed]オプションが選択されています。この時点で、Data Protectorによってポートがオープンされないようにするには、オプションを選択解除します。ただし、Data Protectorを適切に機能させるには、実行可能ファイルを有効にする必要があります。

   [次へ]をクリックします。

10. コンポーネント選択サマリーページが表示されます。[インストール]をクリックします。

11. [Installation setup]ページが表示されます。[Next]をクリックします。

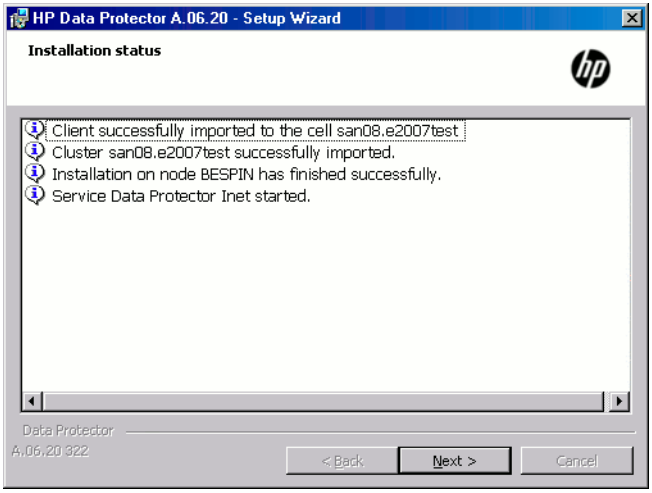


図 30 [Installation Status]ページ

12. Install後すぐにData Protectorを起動するには、[Start the Data Protector Manager]を選択します。

『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を表示するには、[Open the Product Announcements]を選択します。

Windows Server 2003 x64およびWindows Server 2008 x64以外のオペレーティングシステムで、HP AutoPassユーティリティをインストールまたはアップグレードするには、[Start AutoPass installation]オプションまたは[Upgrade AutoPass installation]オプションを選択します。

HP AutoPassユーティリティは、すべてのノードではなく1つのノードにのみインストールされるため、HP AutoPassユーティリティをMicrosoftサーバークラスターにインストールすることはお勧めしません。ただし、AutoPassをインストールする場合は、Data Protectorをシステムから削除するために、インストールされているノードと同じノードからData Protectorをアンインストールする必要があります。

Windows Server 2003 x64およびWindows Server 2008 x64システムでは、HP AutoPassはインストールされません。

13. [Finish]をクリックしてインストールを完了します。

インストールのチェック

セットアップ手順が完了したら、Data Protectorソフトウェアが正しくインストールされているかどうかチェックできます。以下の手順に従ってください。

1. クラスターサービスアカウントが各クラスターノードのData Protector Inetサービスに割り当てられていることを確認します。さらに、同じユーザーがData Protector adminユーザーグループに割り当てられていることを確認します。ログオンアカウントの種類は、図31(203ページ)とに示すように、[アカウント]に設定する必要があります。

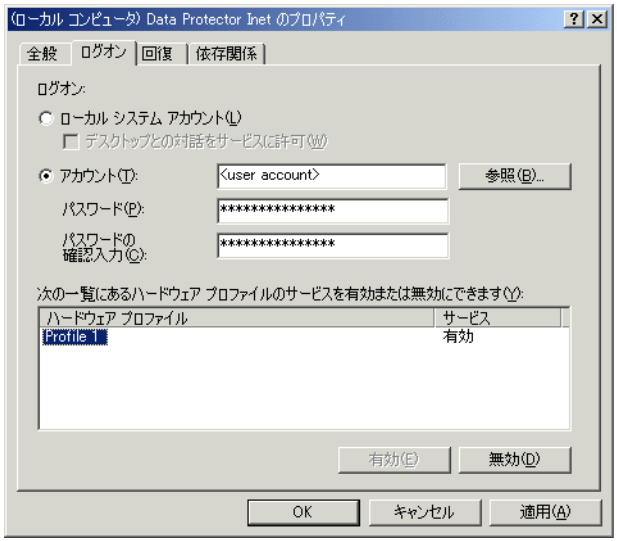


図 31 Data Protectorユーザーアカウント

2. Data_Protector_home¥binディレクトリへ移動し、以下のコマンドを実行します。

   omnirsh *host* INFO_CLUS

   *host*には、クラスター仮想サーバーの名前を指定します。このコマンドを実行すると、クラスター内のシステムの名前のリストと仮想サーバーの名前が表示されます。0 “NONE” のような出力が表示された場合は、Data Protectorがクラスター対応モードでインストールされていません。

3. Data Protector GUIを起動し、[**クライアント**]コンテキストを選択して、[**MS Cluster**]をクリックします。新たにインストールしたシステムが結果エリアに表示されていることを確認してください。

Data Protector InetサービスとCRSサービス

必要に応じて、Data Protector InetサービスとCRSサービスを実行しているアカウントを変更してください。

クラスター対応クライアントのインストール

前提条件

クラスター対応のData Protectorクライアントをインストールするには、次の前提条件を満たす必要があります。

- すべてのクラスターノード上にクラスター機能が正しくインストールされていること。たとえば、ディスク共有の問題なしに、グループをノード間で必要な回数だけ移動できる必要があります。
- クラスターの各システムが適切に稼動していること。
- Windows Server 2008上でMicrosoft Cluster Service (MSCS)が実行されているサーバークラスターに、クラスター対応のData Protectorクライアントをインストールできるようにするには、「Data Protectorインストールのための Windows Server 2008上で実行するMicrosoftサーバークラスターの準備」(390ページ)で説明されている手順を実行します。

ローカルインストール手順

Data Protectorのクラスター対応クライアントは、DVD-ROMを使用して各クラスターノードにローカルにインストールする必要があります。クラスターノード(Data Protectorクラスタークライアント)は、インストールプロセス中に指定したセルにインポートされます。その後、仮想サーバー名をインポートする必要があります。

Installを実行する際には、クラスター管理者のアカウントが必要です。この点を除けば、クラスタークライアントのセットアップは、通常のWindowsクライアントのセットアップと同じです。MS Cluster Supportファイルは自動的にインストールされます。

Data Protector Windowsクライアントシステムをローカルにインストールする方法は、「Windows用クライアントのインストール」(92ページ)を参照してください。

Data Protectorインストールでは、クラスターが検出されたことが通知されます。[**クラスター対応モードでクライアントをインストールする**]を選択します。

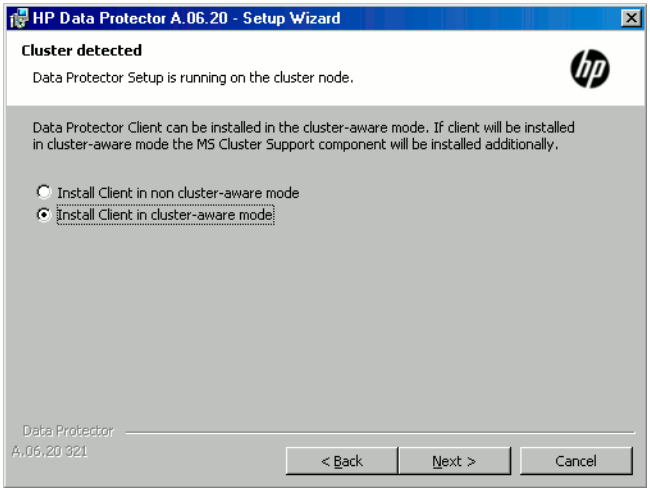


図 32 クラスター対応インストールモードの選択

Data ProtectorのOracle用統合ソフトウェアをインストールする場合、セットアップ手順は、Oracleリソースグループのすべてのクラスターノード上と仮想サーバー上で実行する必要があります。

注記：

クラスター対応クライアントは、標準のCell Managerが管理するData Protectorセル、またはクラスター対応のCell Managerが管理するData Protectorセルのどちらにでもインポートできます。

インストールのチェック

セットアップ手順が完了したら、Data Protectorソフトウェアが正しくインストールされているかどうかチェックできます。以下の手順に従ってください。

1. クラスターサービスアカウントが各クラスターノードのData Protector Inetサービスに割り当てられていることを確認します。さらに、同じユーザーがData Protectoradminユーザーグループに割り当てられていることを確認します。ログオンアカウントタイプは、図33(206ページ)に示すように、[**アカウント**]に設定する必要があります。

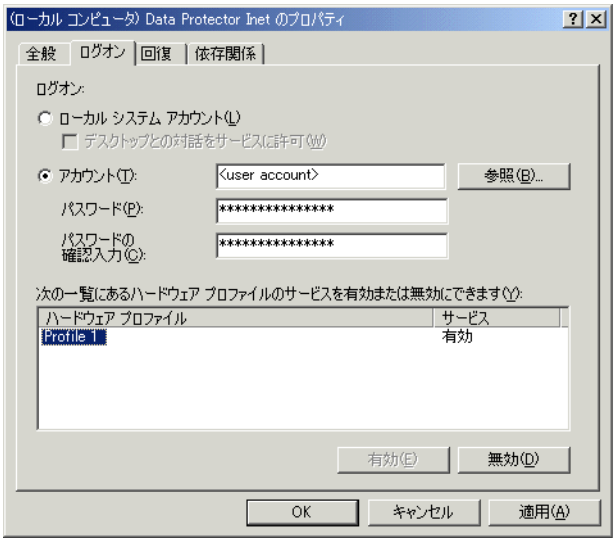


図 33 Data Protectorユーザーアカウント

2. Data_Protector_home¥binディレクトリに移動します。

3. 次のコマンドを実行します。

   omnirsh host INFO_CLUS

   *host*には、クラスタークライアントシステムの名前を指定します。クラスター対応のクライアントシステムのリストが出力されます。0 “NONE” のような出力が表示された場合は、Data Protectorがクラスター対応モードでインストールされていません。

Veritas Volume Manager

クラスター上にVeritas Volume Managerがインストールされている場合は、Microsoft Cluster ServerへのData Protectorのインストールが完了した後に、追加作業が必要になります。追加作業の手順は「Veritas Volume ManagerがインストールされたMicrosoft Cluster ServerへのData Protectorのインストール」(393ページ)を参照してください。

この次に行う作業

Installが完了したら、仮想サーバーのホスト名(クラスター対応アプリケーション)をData Protectorセルにインポートする必要があります。「セルへのクラスター対応クライアントのインポート」(217ページ)を参照してください。

オンラインヘルプの索引「構成」を参照して、バックアップデバイスおよびメディアプールの作成方法、またはData Protectorのその他の構成タスクの詳細をご確認ください。

InetアカウントとCRSアカウントの変更

必要に応じて、Data Protector InetサービスとCRSサービスを実行しているアカウントを変更してください。

Veritas ClusterへのData Protectorクライアントのインストール

Data Protectorクライアントは、クラスター外にあるCell Managerを使用して、Veritas Clusterノード上にインストールできます。この構成では、ローカルディスクのバックアップがサポートされます。

共有ディスクまたはクラスター対応アプリケーションをバックアップする必要がある場合は、仮想サーバーのIPアドレスをライセンスに使用する必要がある点に注意してください。

重要:

Data Protectorの場合、フェイルオーバー時のクラスター対応バックアップは サポートされていません。

クラスター対応クライアントのインストール

Install手順は、Data Protectorを標準構成のSolarisクライアントシステムにインストールする場合と同じです。詳細な手順については、「Solaris用クライアントのインストール」(102ページ)を参照してください。

この次に行う作業

Installが完了したら、以下の作業を行います。

- 仮想サーバーをバックアップする必要がある場合は、仮想サーバーをセルにインポートしてください。

- 物理ノードをバックアップする必要がある場合は、物理ノードをセルにインポートしてください。

「セルへのクラスター対応クライアントのインポート」(217ページ)を参照してください。オンラインヘルプの索引「構成」を参照して、バックアップデバイスおよびメディアプールの作成方法、またはData Protectorのその他の構成タスクの詳細をご確認ください。

Novell NetWare ClusterへのData Protectorクライアントのインストール

Data Protectorクライアントは、クラスター外にあるCell Managerを使用して、Novell NetWare 6.0 Cluster Servicesクラスターノード上にインストールすることができます。この構成を使用して、ローカルディスクのバックアップと仮想サーバーを使用した共有クラスタープールのバックアップが行えます。Novell NetWare Clusterで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、『HP Data Protector製品案内、ソフトウェアノート、リファレンス』を参照してください。

共有ディスクまたはクラスター対応アプリケーションをバックアップする必要がある場合は、仮想サーバーのIPアドレスをライセンスに使用する必要がある点に注意してください。

重要:

フェイルオーバー時のクラスター対応バックアップは、サポートされていません。フェイルオーバーが発生した場合は、バックアップまたは復元セッションを、手動で再起動する必要があります。

バックアップデバイスは、仮想サーバーではなくクラスターノード上で構成されている必要があります。これは、クラスターノードがデバイスを制御するためです。

クラスター対応クライアントのインストール

インストール前

Novell NetWare Cluster Servicesクラスターノード上にData Protectorクライアントをインストールする前に、クラスター内のすべての仮想サーバーのアンロードスクリプトを編集することをお勧めします。そうすることにより、仮想サーバーから他のノードへの移行中でも、セカンダリIPアドレスはアクティブのままになります。アンロードスクリプトを編集するには、Novell Console Oneユーティリティ、またはNetWare Remote Managerを使用します。使用方法はNovell NetWareのマニュアルを参照してください。

例

すべての仮想サーバーに対するデフォルトのアンロードスクリプトは、以下のとおりです。

```
del secondary ipaddress 10.81.1.173 CLUSTER CVSBIND DEL TREENW6_CLUSTER_FIRST_SERVER
10.81.1.173 NUDP DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173 nss
/pooldeactivate=FIRST /overridetype=question
```

すべての仮想サーバーに対する変更済みのアンロードスクリプトは、以下のとおりです。

```
nss /pooldeactivate=FIRST
/overridetype=question del secondary ipaddress 10.81.1.173 CLUSTER CVSBIND DEL
TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173 NUDP DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
```

変更済みのアンロードスクリプトでは、最初に仮想サーバー上のすべてのクラスター共有プールをディスマウントおよび非アクティブ化し、その後セカンダリIPアドレスを削除します。これにより、セカンダリIPアドレスは移行中もアクティブのままとなります。

変更済みのアンロードスクリプトをアクティブにするには、優先ノード上で仮想サーバーをオフラインにし、再びオンラインに戻します。

smsrun.basスクリプトの編集

アンロードスクリプトの編集後、クラスターのサポートを無効にするパラメータを使用してTSA600.NLMモジュールまたはTSAFS.NLMモジュール(使用するモジュールによって異なる)をロードするように、smsrun basスクリプトを編集する必要があります。詳細は、「Known Backup/Restore Issues for NetWare 6.x」の「Novell Support Knowledge database」を参照してください。

smsrun.basスクリプトの編集は、以下の手順で行います。

1. SYS:NSN/user/smsrun.basスクリプトの書き込み保護を読み込み専用から読み込み/書き込みに変更して、標準のコンソールエディタで開きます。
2. Sub Main()セクションのnlmArray = Array(“SMDR”, “TSA600”, “TSAPROXY”)(またはnlmArray = Array(“SMDR”, “TSAFS /NoCluster”))行を次のように変更します。
   - nlmArray = Array(“SMDR”, “TSA600 /cluster=off”, “TSAPROXY”)(TSA600がインストールされている場合)
   - nlmArray = Array(“SMDR”, “TSAFS /NoCluster”)(TSAFSがインストールされている場合)

   変更した内容を保存します。
3. ファイルサーバーのコンソールで、SMSSTOPと入力します。
4. ファイルサーバーのコンソールで、SMSSTARTと入力します。

クラスター共有ボリュームがTSA600.NLM(TSAFS.NLM)モジュールにより表示されます。

インストール

Install手順は、Data Protectorを標準構成のNovell NetWareクライアントにローカルインストールする場合と同じです。詳細な手順については、「Novell NetWareクライアントのローカルインストール」(131ページ)を参照してください。

この次に行う作業

Installが完了したら、以下の作業を行います。

- 物理ノードをバックアップする必要がある場合は、物理ノードをセルにインポートしてください。
- 仮想サーバー(共有クラスターボリューム)をバックアップする必要がある場合は、仮想サーバーをセルにインポートしてください。

「セルへのクラスター対応クライアントのインポート」(217ページ)を参照してください。オンラインヘルプの索引「構成」を参照して、バックアップデバイスおよびメディアプールの作成方法、またはData Protectorのその他の構成タスクの詳細をご確認ください。

Data ProtectorのIBM HACMP Clusterへのインストール

Data Protectorは、IBM High Availability Cluster Multi-processing for AIXをサポートしています。

重要:

Data Protector Disk Agentコンポーネントをすべてのクラスターノードにインストールします。

クラスター対応クライアントのインストール

Data Protectorコンポーネントをクラスターノードにインストールするには、Data Protectorを標準構成のUNIXシステムにインストールする場合と同じ手順を使用します。詳細については、「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)または「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

この次に行う作業

Installが終了したら、クラスターノードと仮想サーバー(仮想環境パッケージのIPアドレス)をData Protectorセルにインポートします。「セルへのクラスター対応クライアントのインポート」(217ページ)を参照してください。

バックアップデバイス、メディアプール、または追加Data Protector構成タスクの構成方法については、オンラインヘルプの索引「構成」を参照してください。

3 インストールの保守

この章の内容

この章では、バックアップ環境の構成を変更するために最も頻繁に実行される手順について説明します。以降の項では、以下の情報を提供します。

- グラフィカルユーザーインタフェースを使用してクライアントをセルにインポートする方法。詳細は、「セルへのクライアントのインポート」(213ページ)を参照してください。
- グラフィカルユーザーインタフェースを使用してインストールサーバーをセルにインポートする方法。詳細は、「セルへのインストールサーバーのインポート」(216ページ)を参照してください。
- グラフィカルユーザーインタフェースを使用してクラスターや仮想サーバーをインポートする方法。詳細は、「セルへのクラスター対応クライアントのインポート」(217ページ)を参照してください。
- グラフィカルユーザーインタフェースを使用してクライアントをエクスポートする方法。詳細は、「Data Protectorソフトウェアのアンインストール」(242ページ)を参照してください。
- グラフィカルユーザーインタフェースを使用して保護を設定する方法。詳細は、「保護について」(223ページ)を参照してください。
- インストール済みのData Protectorパッチを確認する方法。詳細は、「どのData Protectorパッチがインストールされているかを確認する」(240ページ)を参照してください。
- Data Protectorソフトウェアをアンインストールする方法。詳細は、「Data Protectorソフトウェアのアンインストール」(242ページ)を参照してください。
- Data Protectorソフトウェアコンポーネントを追加または削除する方法。詳細は、「Data Protectorソフトウェアコンポーネントの変更」(257ページ)を参照してください。

セルへのクライアントのインポート

インストールサーバーを使用してソフトウェアコンポーネントをクライアントに配布すると、クライアントシステムが自動的にセルに追加されます。リモートインストールが完了すると、クライアントはセルのメンバーになります。

いつインポートを行うか

インストールCD-ROMからローカルにインストールされたNovell NetWare、HP OpenVMS、およびWindows XP Home Editionなどの一部のクライアントは、インストール後にセルにインポートする必要があります。**インポート** とは、Data Protectorソフトウェアのインストール後にセルにコンピュータを追加することを意味します。Data Protectorセルに追加されると、システムはData Protectorクライアントになります。システムがセルのメンバーになると、この新しいクライアントに関する情報は、Cell Manager上のIDBに書き込まれます。

クライアントがメンバーになれるのは、1つのセルだけです。クライアントを他のセルに移動する場合は、まずクライアントを現在のセルからエクスポートしてから、新しいセルにインポートします。クライアントをエクスポートする手順は、「セルからのクライアントのエクスポート」(220ページ)を参照してください。

重要:

Data Protectorクライアントのインストール、およびクライアントのセルへのインポートが完了したら、不要なセル権限によるアクセスからクライアントを保護することを、強くお勧めします。詳細は、「クライアントの保護設定」(227ページ)を参照してください。

インポート方法

グラフィカルユーザーインタフェースを使ってクライアントシステムをインポートするには、以下の手順に従ってください。

1. コンテキストリストで[**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。詳細は、図34(215ページ)を参照してください。

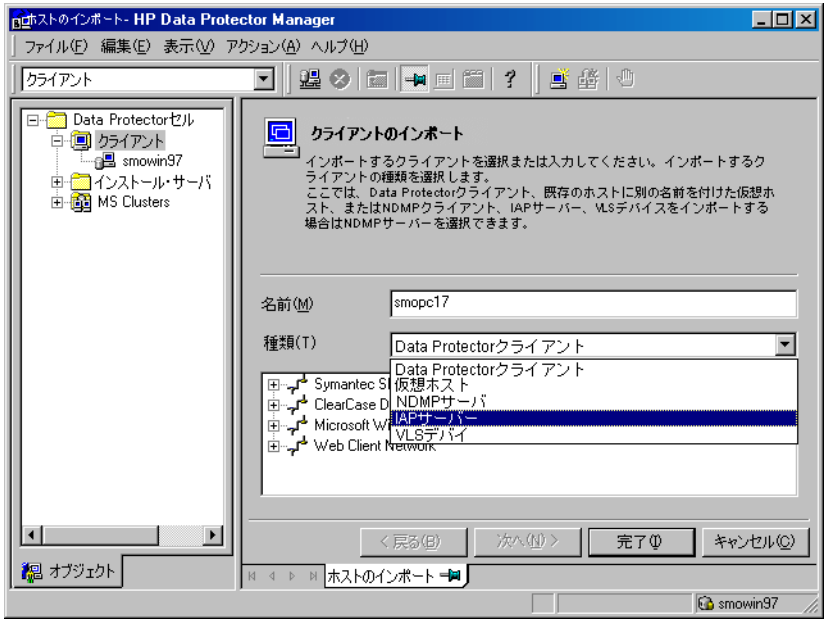


図 34 セルへのクライアントのインポート

複数のLANカードが構成されたクライアントをインポートする場合は、[**仮想ホスト**]オプションを選択します。このオプションにより、同一システムに割り当てられている複数のホスト名をすべてインポートします。

NDMPクライアントをインポートする場合は、[**NDMPサーバー**]オプションを選択し、[**次へ**]をクリックします。NDMP Serverに関する情報を指定します。

HP OpenVMSクライアントをインポートする場合は、OpenVMSクライアントのTCP/IP名を、[名前]テキストボックスに入力します。

VLSデバイスをインポートする場合は、**VLSデバイス**オプションを選択して、[**次へ**]をクリックします。VLSデバイスの情報を指定します。

Data ProtectorのMicrosoft Exchange Server 2010用統合ソフトウェアで使用するMicrosoft Exchange Server 2010 DAG仮想ホストをインポートする場合は、[**仮想ホスト**]を選択します。

Data Protectorの仮想環境統合ソフトウェアで使用するクライアントをインポートする場合は、[**VMware ESX(i)**](スタンドアロンのESX(i) Serverシステムの場合)、[**VMware vCenter**](VMware vCenter Serverシステムの場合)、[**Hyper-V**](Microsoft Hyper-V

システムの場合)のいずれかを選択します。[**次へ**]をクリックし、ログイン資格情報を入力します。

[Finish]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。

セルへのインストールサーバーのインポート

いつ追加を行うか

以下の状況では、インストールサーバーをセルに追加する必要があります。

- 独立した形で、たとえばCell Managerとは別のシステム上にUNIXインストールサーバーをインストールした場合。

  この場合、インストールサーバーをセルに追加するまでは、セル内のクライアントに対するリモートインストールは実行できません。

- Cell Managerにインストールしているが、他のセルでもリモートインストールを実行する場合。この場合は、他のセルのCell Managerに接続されたGUIを使用して、他のセルにも追加する必要があります。

クライアントとは異なり、インストールサーバーは複数のセルのメンバーにすることができます。したがって、インストールサーバーは、いずれかのセルから削除(エクスポート)しなくても、他のセルに追加(インポート)できます。

追加方法

インストールサーバーのインポートプロセスは、クライアントのインポートプロセスに似ています。この作業は、インストールサーバーを追加するセルのCell Managerに接続されたData ProtectorGUIを使用して、以下の手順に従って実行します。

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、[**インストールサーバー**]を右クリックし、[**インストールサーバーの追加**]をクリックして、ウィザードを起動します。詳細は、図34(215ページ)を参照してください。
3. インポートするシステムの名前を入力または選択します。[**完了**]をクリックしてインストールサーバーをインポートします。

セルへのクラスター対応クライアントのインポート

Data Protectorソフトウェアをクラスター対応クライアント上にローカルにインストールした後、そのクラスター対応クライアントを表す仮想サーバーをData Protectorセルにインポートします。

前提条件

- すべてのクラスターノード上にData Protectorがインストールされていること。
- クラスター内ですべてのクラスターパッケージが実行されていること。

Microsoft Cluster Server

Microsoft Cluster ServerクライアントをData Protectorセルにインポートするには、以下の手順に従ってください。

1. [Data Protector]で、[クライアント]コンテキストを選択します。
2. Scopingペインの**[MS Cluster]**を右クリックし、**[クラスターのインポート]**をクリックします。

3. インポート対象のクラスタークライアントを表す仮想サーバーの名前を入力するか、ネットワークをブラウズして仮想サーバーを選択します。詳細は、図35(218ページ)を参照してください。

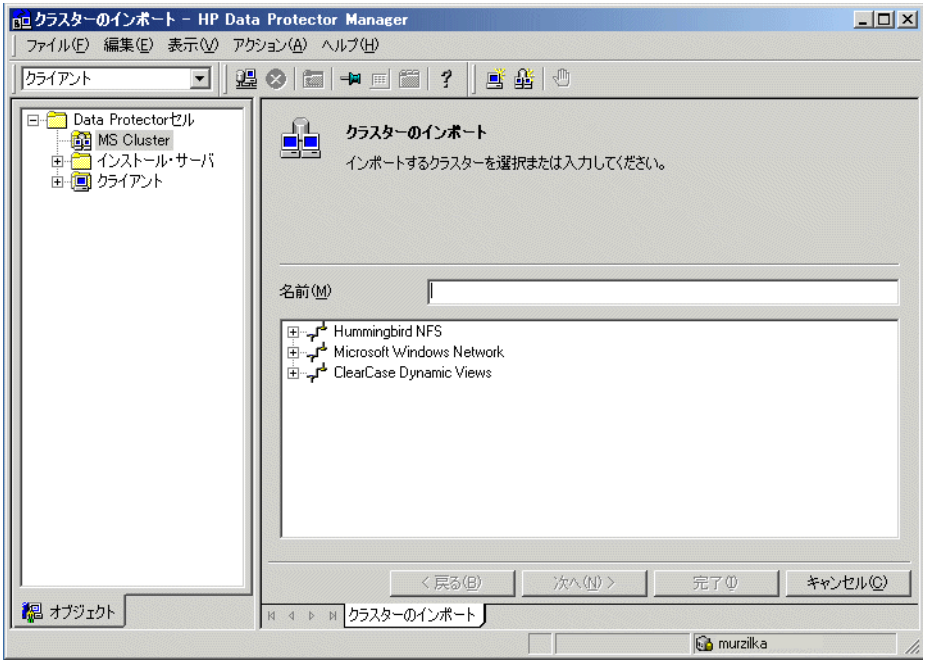


図 35 セルへのMicrosoft Cluster Serverクライアントのインポート

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。

ヒント:

特定のクラスターノードまたは仮想サーバーをインポートするには、Scopingペインでそのクラスターを右クリックし、[クラスターノードのインポート]または[クラスター仮想サーバーのインポート]をクリックします。

その他のクラスター

Tru64 Clusterの前提条件

クラスターのホスト名をインポートする前に、以下の点を確認してください。

- クラスター内の共有ディスク上にData Protectorがインストールされていること。

- Tru64 Cluster内ですべてのTru64 Clusterノードが実行されていること。
- Data Protector 各ノード上でinetdプロセスが実行されていること。

手順

MC/ServiceGuard、Veritas、Tru64 Cluster、IBM HACMP Cluster、Novell NetWare Cluster Servicesのいずれかのクライアントを Data Protectorセルにインポートするには、以下の手順に従ってください。

1. [Data Protector Manager]で、[クライアント]コンテキストを開きます。
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. 仮想サーバーのホスト名をアプリケーションクラスターパッケージで指定されているとおりに入力します。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仮想サーバーを選択することもできます。

   [仮想ホスト]オプションを選択し、これがクラスター仮想サーバーであることを示します。詳細は、図36(220ページ)を参照してください。
4. **[完了]**をクリックして仮想サーバーをインポートします。

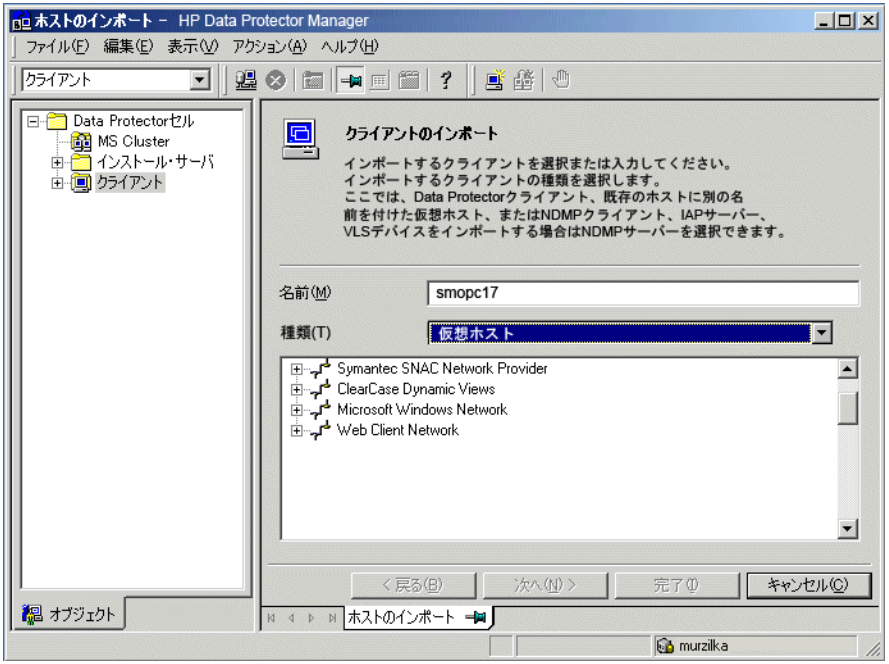


図 36 MC/ServiceGuardクライアント、Veritasクライアント、またはNovell NetWare Cluster Servicesクライアントのセルへのインポート

ヒント:

クラスターノードのローカルディスク上にあるデータのバックアップも構成できるようにするには、Data Protectorクライアントを表すクラスターノードをインポートする必要があります。インポート手順は、「セルへのクライアントのインポート」(213ページ)を参照してください。

セルからのクライアントのエクスポート

Data Protectorセルからのクライアントの**エクスポート**は、クライアントからソフトウェアをアンインストールすることなく、Cell ManagerのIDBからその参照を削除することを意味します。この作業は、Data Protector GUIを使用して行います。

エクスポート機能を使うと、以下のような作業を実施できます。

- クライアントを他のセルに移動できます。

- ネットワークに現在含まれていないクライアントを、Data Protectorセルから削除できます。
- ライセンスの不足によって発生した問題を解決できます。

  セルからクライアントをエクスポートすると、そのシステムで使用していたライセンスを他のシステムで使用できるようになります。

前提条件

クライアントをエクスポートする前に、以下の条件が満たされていることを確認してください。

- 存在するすべてのクライアントがバックアップ仕様から削除されていること。削除されていない場合、Data Protectorは不明なクライアントのバックアップを実行しようとするため、バックアップ仕様のこのシステムに対応する部分が正常に実行されません。オンラインヘルプの索引「変更、バックアップ仕様」を参照して、バックアップ仕様を変更する手順を確認してください。
- クライアントに接続済みおよび構成済みのバックアップデバイスが存在しないこと。システムがエクスポートされると、Data Protectorは元のセルのバックアップデバイスを使用できなくなります。

エクスポート方法

Data Protector GUIを使用してクライアントをセルからエクスポートするには、以下の手順に従ってください。

1. コンテキストリストで[**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**]をクリックします。次に、エクスポート対象のクライアントシステムを右クリックし、[**削除**]をクリックします。詳細は、図37(222ページ)を参照してください。

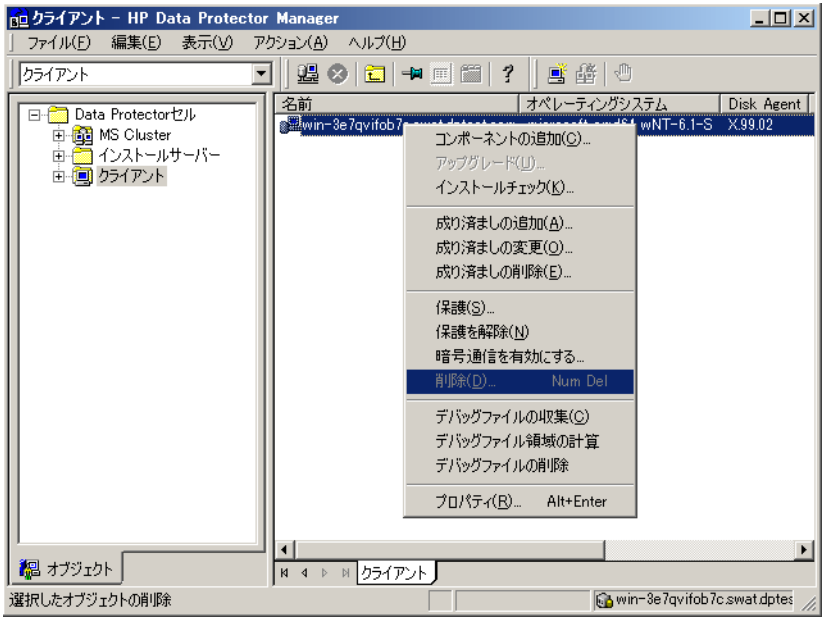


図 37 クライアントシステムのエクスポート

3. Data Protectorソフトウェアをアンインストールするかどうかを尋ねるメッセージが表示されます。クライアントをエクスポートする場合は、[**いいえ**]をクリックし、[**完了**]をクリックします。

選択したクライアントが[結果エリア]のリストから削除されます。

注記:

エクスポートするクライアントと同じシステムにCell Managerがインストールされている場合は、Data Protectorクライアントをエクスポートまたは削除することはできません。ただし、クライアントとインストールサーバーのみがインストールされているシステムからクライアントをエクスポートすることはできます。この場合は、インストールサーバーはセルからも削除されます。

Microsoft Cluster Serverクライアント

Microsoft Cluster ServerクライアントをData Protectorセルからエクスポートするには、以下の手順に従ってください。

1. コンテキストリストで[**クライアント**]をクリックします。
2. Scopingペインで[**MS Clusters**]を展開し、エクスポートするクライアントを右クリックして、[**削除**]をクリックします。
3. Data Protectorソフトウェアをアンインストールするかどうかを尋ねるメッセージが表示されます。[**いいえ**]をクリックして、クラスタークライアントのみエクスポートします。

選択したクラスタークライアントが[結果エリア]のリストから削除されます。

ヒント：

特定のクラスターノードまたは仮想サーバーをエクスポートするには、Scopingペインでクラスターノードまたは仮想サーバーを右クリックし、[削除]をクリックします。

保護について

ここでは、Data Protectorの保護について説明します。Data Protectorの保護を強化するために使用できる高度な設定、およびその前提条件や留意事項について説明します。

環境全体での保護の強化には、さらなる作業も必要となるため、多くの保護機能は、デフォルトでは有効になっていません。

この章で説明する内容は、保護設定を変更する場合だけではなく、新しいユーザーを構成する場合、クライアントを追する場合、Application Agentを構成する場合、または留意事項の対象となるその他の変更を加える場合にも従う必要があります。保護設定の変更は、セル全体に影響を及ぼす可能性があるため、慎重に計画する必要があります。

セキュリティ層

Data Protectorを安全に運用するためには、セキュリティが重要な以下の層に対して、セキュリティ対策を計画、テスト、および実現する必要があります。セキュリティ対策が必要な層は、Data Protectorクライアント、Cell Manager、およびユーザーです。ここでは、これらの各層の保護の構成方法について説明します。

クライアントの保護

セル内のクライアントにインストールされているData Protectorエージェントは、システム上のすべてのデータへのアクセスなど、多数の強力な機能を備えています。これらの機能は、**セル権限**(Cell Managerおよびインストールサーバー)で実行されるプロセスにのみ使用できるようにし、それ以外の要求はすべて拒否することが重要です。

クライアントを保護する前に、信頼されるホストのリストを確認することが重要です。このリストには、以下が含まれます。

- Cell Manager
- 対応するインストールサーバー
- クライアントによっては、ロボティクスにリモートでアクセスするクライアントのリスト

重要:

リストには、接続元になる可能性のあるすべてのホスト名(またはIPアドレス)が含まれている必要があります。上記のホストのいずれかがマルチホーム(複数のネットワークアダプタや複数のIPアドレスを持つ)またはクラスターの場合は、複数のクライアント名が必要になることがあります。

セル内のDNS構成が一律でない場合は、他にも考慮すべき事項が存在することがあります。詳細は、「クライアントの保護設定」(227ページ)を参照してください。

セル内のすべてのクライアントを常に保護する必要があるわけではありませんが、他のクライアントに信頼される以下のようなコンピュータについては、保護設定が重要です。

- Cell Manager / MoM
- インストールサーバー
- Media Agent(MA)クライアント

注記:

ユーザーインタフェースクライアントを信頼されるクライアントのリストに追加する必要はありません。ユーザー権限によっては、GUIを使用してData Protectorの全機能、または一部のコンテキストのみにアクセスできます。

Data Protectorユーザー

Data Protectorユーザーの構成時には、以下の点について十分に考慮してください。

- 一部のユーザー権限は非常に強力です。たとえば、User configurationおよびClients configurationユーザー権限を持つユーザーは保護設定を変更できます。Restore to other clientsユーザー権限も非常に強力です。Back up as rootまたはRestore as rootユーザー権限のいずれかと組み合わせた場合は、特に強力です。
- それほど強力ではないユーザー権限にも、常にリスクは伴います。Data Protectorを構成して一定のユーザー権限を制限し、これらのリスクを削減できます。これらの設定については、本章で後述します。「[バックアップ仕様を開始]ユーザー権限」(238ページ)も参照してください。
- Data Protectorでは、少数のユーザーグループが事前に定義されています。Data Protector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、最小限の権限だけをユーザーに割り当てることをお勧めします。
- ユーザーグループのメンバーシップによるユーザー権限の割り当てに加えて、さらに特定のユーザーグループの操作をData Protectorセルの特定のシステムのみに制限することもできます。このポリシーは、user_restrictions ファイルを構成することによって実装できます。詳細は、オンラインヘルプを参照してください。
- 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(「ホスト名厳密チェック」(233ページ)を参照)。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なく、逆に、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機能しない可能性があります。
- 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。

注記:

ユーザー仕様のホスト部分は、(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を管理する際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、そのユーザーをユーザー、グループ、<*任意*>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ー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。

ユーザーを構成する方法の詳細については、オンラインヘルプの索引「構成、ユーザー」を参照してください。

Cell Managerの保護

Cell Managerは、セル内のすべてのクライアントとデータにアクセスできるため、その保護は重要です。

Cell Managerの保護は、ホスト名厳密チェック機能によって強化できます。ただし、Cell Managerがクライアントとしても保護され、Data Protectorユーザーが十分に検討された上構成されていることが重要です。

必ずしもセル内のすべてのクライアントのセキュリティを強化する必要はありませんが、ほかのクライアントから信頼されるコンピュータについては、セキュリティの強化が重要です。この点は、Cell Managerだけではなく、インストールサーバーやMedia Agentのクライアントについても同様です。

Cell ManagerおよびData Protectorセル内のすべてのクライアントのセキュリティは、暗号制御通信を有効化することにより、さらに強化することができます。

詳細は、「ホスト名厳密チェック」(233ページ)、「クライアントの保護設定」(227ページ)、および「セキュアな通信の有効化」(235ページ)を参照してください。

その他のセキュリティ保護について

他に考慮すべきセキュリティ保護は、以下のとおりです。

- ユーザーが信頼されるクライアント(Cell Manager、インストールサーバー、MA、ロボティクスクライアント)にアクセスできないようにする必要があります。匿名ログオンやFTPアクセスも、全体的なセキュリティに重大なリスクをもたらす可能性があります。
- メディアおよびテープライブラリ(および接続先クライアント)を、許可されていないユーザーや信頼されていないユーザーから物理的に保護する必要があります。
- バックアップ、復元、オブジェクトまたはメディアのコピー、オブジェクト集約、またはオブジェクト検証の最中に、データがネットワーク経由で転送されます。ネットワークのセグメント化によって信頼されていないネットワークから完全に分離されていない場合は、ローカルに割り当てられたデバイス、Data Protector暗号化テクニック、またはカスタムエンコードライブラリを使用します。エンコードライブラリを変更した後は、フルバックアップを実行する必要があります。
- さらに、Data Protectorセル内で暗号制御通信を有効にすると、システムへの不正なアクセスを防止し、セキュリティを強化できます。

その他のセキュリティ関連事項は、オンラインヘルプおよび『*HP Data Protectorコンセプトガイド*』を参照してください。

クライアントの保護設定

Data Protectorクライアントのインストール、およびクライアントのセルへのインポートが完了したら、権限のない他のクライアントによるアクセスからクライアントを保護することを、強くお勧めします。

Data Protectorでは、クライアントがどのセル権限(Cell Manager、MoM、、およびインストールサーバー)からData Protectorポート5555で要求を受け付けるかを指定できます。その結果、他のコンピュータからそのクライアントにアクセスできなくなります。「クライアントの保護」(224ページ)も参照してください。

注記:

ライブラリロボティクスに対してリモートアクセスを行うクライアントは、ライブラリロボティクスクライアントのセル権限リストに追加する必要があります。

バックアップや復元、実行前または実行後スクリプトの起動、クライアントのインポートやエクスポートなどの作業について、クライアントは、Data Protectorポート(デフォルト5555)を介してこれらの作業を開始するコンピュータが、その作業を許可されているかどうかをチェックします。この保護メカニズムによって、クライアントは、指定されたセル権限からのみアクションを受け付けるよう指示されます。

例外的状況に対する考慮

クライアントへのアクセスを制限する前に、問題を引き起こす可能性がある以下の状況について 考慮してください。

- セル権限に、複数のLANカードや複数のIPアドレス/クライアント名がある場合。
- クラスター対応のCell Managerを使用する場合。
- テープライブラリのロボティクスが別個の(または専用の)システム上で構成されている場合。

Data Protectorでは、クライアントに接続するためのセル権限が明示的に認められたシステムを、1つだけではなく、リストで指定することができます。障害を回避するために、事前にすべての適したクライアント名のリストを代わりのセル権限として用意しておきます。

リストには、以下の情報を含めるようにしてください。

- セル権限で使用している、追加分を含めた(すべてのLANカードに対応する)クライアント名。
- Cell Managerがフェイルオーバーする可能性のあるすべてのクラスターノードのクライアント名およびクラスター仮想サーバーのホスト名。

- セル権限の全ハードウェアがダウンした場合に、セル権限の移動先となるターゲットシステムの名前。このターゲットシステムは、ディザスタリカバリ対象として事前に定義されている必要があります。
- ライブラリのロボティクスを制御するクライアントへのアクセスが許可されているクライアントについては、そのライブラリのドライブを使用するすべてのクライアント名。

アクセスの許可および拒否は、Data Protectorがインストールされているすべてのシステムに適用できます。たとえば、Cell ManagerからクライアントCell Manager、Cell ManagerからCell Manager、インストールサーバーからクライアント、またはクライアントからクライアントへのアクセスを許可または拒否できます。

注記:

Cell Manager以外のシステムにあるインストールサーバーが許可されたクライアントのリストに追加されていない場合は、保護されたクライアントにアクセスできません。この場合は、インストールサーバーに依存している操作(インストールのチェック、コンポーネントの追加、クライアントの削除など)は失敗します。保護されているクライアント上でこれらの操作を実行できるようにするには、インストールサーバーを許可されているクライアントのリストに追加してください。

クライアントの保護方法

クライアント側でセル権限を確認できるようにする(クライアントを保護する)には、Data Protector GUIで以下の手順を行ってください。

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]を展開し、保護対象のクライアントを右クリックした後、[**保護**]をクリックします。図38(229ページ)を参照してください。

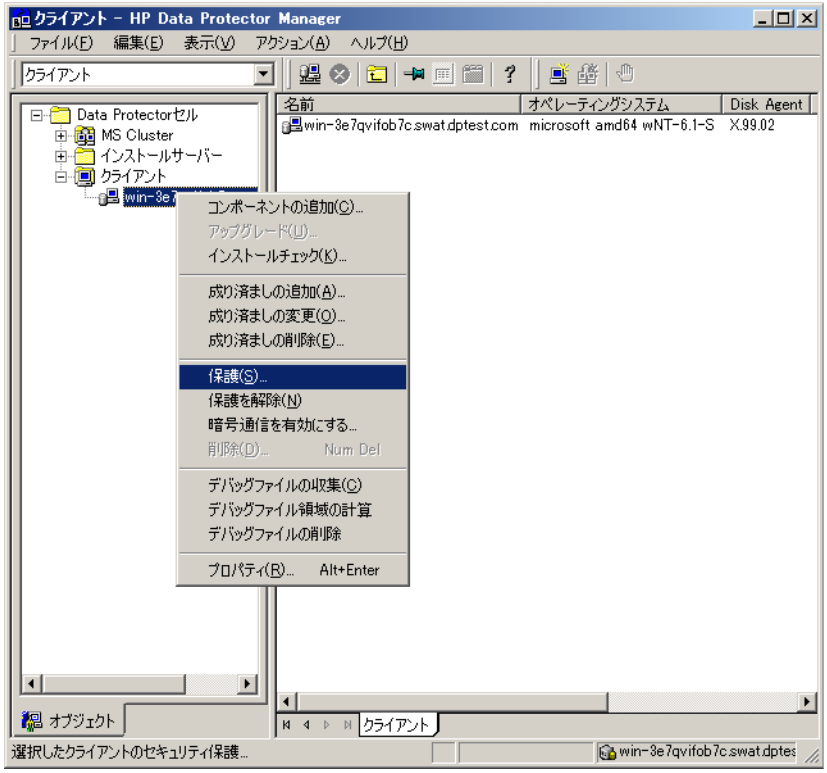


図 38 クライアントの保護設定

3. 選択されたクライアントへのアクセスを許可するシステムの名前を入力するか、[ネットワーク]または[検索]タブを使用してシステムを検索します。**[追加]**をクリックして、リストに各システムを追加します。図39(230ページ)を参照してください。

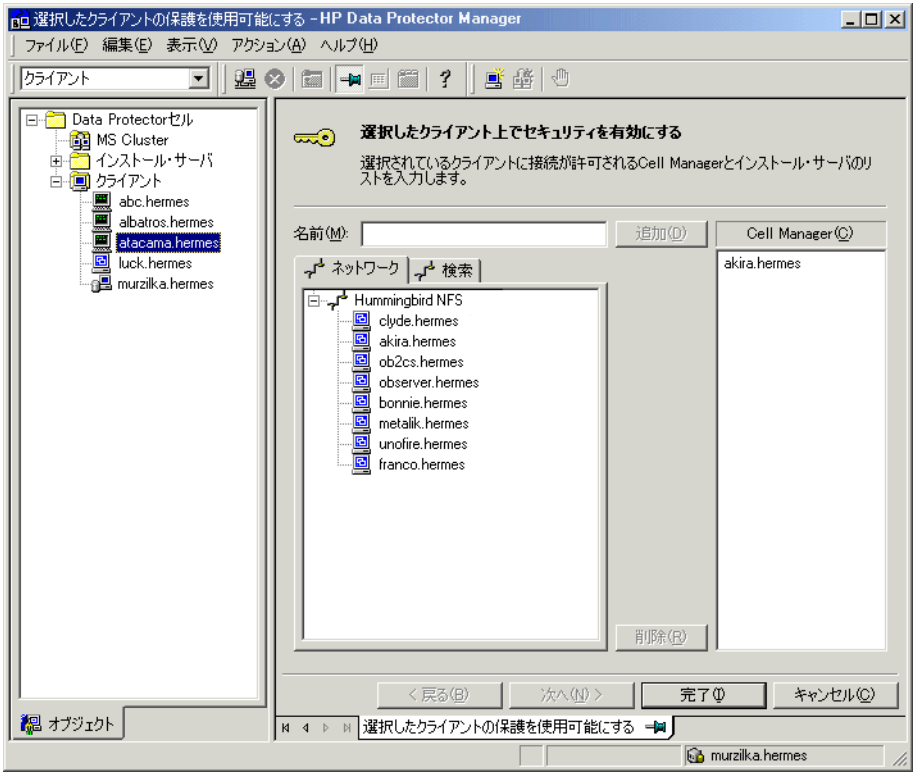


図 39 選択したクライアントの保護を使用可能にする

Cell Managerは、自動的にアクセスが許可され、信頼されるクライアントのリストに追加されます。リストからCell Managerを削除することはできません。

4. **[完了]**をクリックして、選択したシステムをallow_hostsファイルに追加します。

どのような処理が行われるか

クライアントは、各要求に対してソースを確認し、[選択したクライアント上でセキュリティを有効にする]ウィンドウで選択されているクライアントからの要求だけを受信します。これらのクライアントは、allow_hostsallow_hostsファイルセキュリティallow_hostsファイルファイル allow_hostsファイルにリストされています。要求が拒否されると、イベントは、以下のディレクトリのinet.log ファイルに記録されます。

- Windows Vista、Windows 7、Windows Server 2008の場合:*Data_Protector_program_data*¥log
- その他のWindowsシステムの場合: *Data_Protector_home*¥log
- HP-UX、Solaris、およびLinuxの場合: /var/opt/omni/log
- その他のUNIXシステムおよびMac OS Xシステムの場合:/usr/omni/log

セル内のすべてのクライアントに保護を設定する場合は、Data Protector GUI上で以下の手順に従ってください。

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. セル内のすべてのクライアントへのアクセスを許可するシステムの名前を入力するか、[ネットワーク] (Windows GUIの場合)または[検索]タブで検索します。[**追加**]をクリックして、リストに各システムを追加します。図40(231ページ)を参照してください。

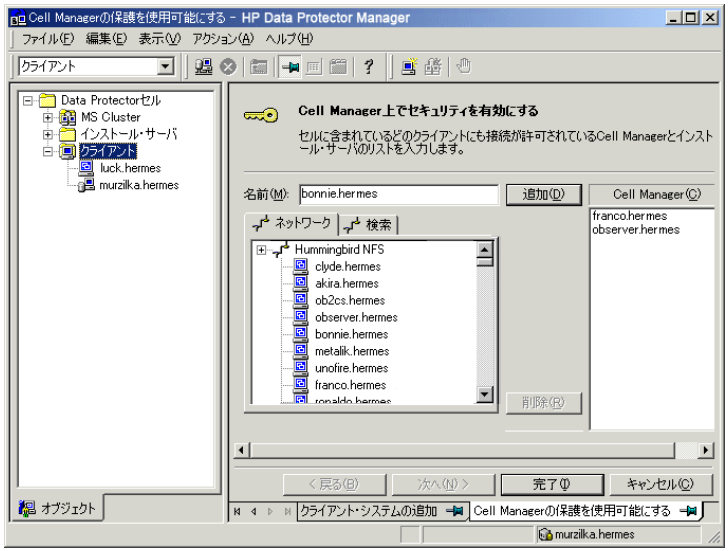


図 40 セル内のすべてのクライアントに対する保護の設定

3. [**完了**]をクリックして、選択したシステムをallow_hostsファイルに追加します。

どのような処理が行われるか

クライアントは、各要求に対してソースを確認し、[Cell Manager上でセキュリティを有効にする]ウィンドウで選択されているクライアントからの要求だけを受信します。これらのクライアントは、allow_hostsallow_hostsファイルセキュリティallow_hostsファイルファイルallow_hostsファイルにリストされています。要求が拒否されると、イベントは、以下のディレクトリのinet.logファイルに記録されます。

- Windows Vista、Windows 7、Windows Server 2008の場合:Data_Protector_program_data¥log
- その他のWindowsシステムの場合: Data_Protector_home¥log
- HP-UX、Solaris、およびLinuxの場合: /var/opt/omni/log
- その他のUNIXシステムおよびMac OS Xシステムの場合:/usr/omni/log

セル全体を保護すると、そのセル内に存在するすべてのクライアントが同時に保護されます。セルに新しいクライアントを追加する場合は、追加したクライアントも保護する必要があります。

保護の解除方法

選択したシステムの保護を解除する場合は、Data Protector GUI上で以下の手順に従ってください。

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、保護を解除するクライアント(複数選択可能)を右クリックし、[**保護を解除**]をクリックします。
3. [**はい**]をクリックして、選択したクライアント(複数選択可能)に対するアクセスを許可することを確認します。

セル内のすべてのクライアントの保護を解除する場合は、以下の手順に従ってください。

1. コンテキストリストで[**クライアント**]をクリックします。
2. Scopingペインの[**クライアント**]をマウスの右ボタンでクリックし、[**セルの保護解除**]を選択します。
3. [**はい**]をクリックして、セル内のすべてのクライアントへのアクセスを許可することを確認します。

allow_hostsファイルとdeny_hostsファイル

クライアントに保護を設定すると、クライアントへのアクセスが許可されているシステムのクライアント名がallow_hostsファイルに書き込まれます。特定のコンピュータからのクライアントへのアクセスを明示的に拒否することもできます。拒否するには、拒否するホスト名をdeny_hostsファイルに追加します。これらのファイルは、次のディレクトリに配置されます

- Windows Vista、Windows 7、およびWindows Server 2008の場合:Data_Protector_program_data¥Config¥client
- その他のWindowsシステムの場合: Data_Protector_home¥Config¥client
- HP-UX、Solaris、およびLinuxシステムの場合: /etc/opt/omni/client

- その他のUNIXシステムおよびMac OS Xシステムの場合:/usr/omni/config/client

各クライアント名は行を分けて指定してください。

注記:

クライアントへのアクセスが誤って拒否されるようになった場合は、そのクライアント上のallow_hostsファイルを 手動で編集(または削除)できます。

これらのファイルは、Windowsシステムでは2バイトのUNICODE形式で保存され、HP-UXシステム、Solarisシステム、およびLinuxシステムでは1バイト形式またはマルチバイト形式(Shift-JISなど)で保存されます。

inet.logファイルに大量のログが記録される

クライアントに保護が設定されず、Cell ManagerがMC/ServiceGuard環境に構成されるか、複数の名前またはIP番号が割り当てられている場合に、inet.logファイルに以下のようなエントリーが多数含まれていることがあります。

```
A request 0 came from host name.company.com which is not a Cell Manager
of this client
```

これは、保護されていないクライアントがCell Managerのプライマリホスト名しか認識しないために発生します。その他のクライアントからの要求もすべて許可されますが、要求はinet.logファイルに記録されます。

クライアントに保護が設定されている場合は、allow_hostsファイルに記載されているクライアントからの要求は承認されるため、ログに記録されることはありません。その他のクライアントからの要求は拒否されます。

クライアントの保護は、inet.logファイルへの不要なエントリーを回避する方法として使用できます。ただし、Cell Managerのすべてのクライアント名は、各クライアントのallow_hostsファイルにリストされている必要があります。これによってフェイルオーバー時もクライアントへのアクセスが可能になります。

何らかの理由でユーザー環境でこの回避策を使用できない場合は、クライアントを保護し、アクセスを許可するシステムのIPアドレスの範囲として*を指定します。これによって、クライアントは、すべてのシステム(任意のIPアドレス)からの要求を受け付け、事実上保護されていない状態となりますが、大量のログが記録される問題は解決します。

ホスト名厳密チェック

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。ユーザーインタフェースまたはApplication Agent が開始されるクライアン

ト上で認識されているホスト名が使用されます。この方法は、セキュリティが“推奨”される(たとえば、悪意のある攻撃の可能性があまり高くない)環境で、中レベルのセキュリティをより簡単に構成および実現する場合に適しています。

一方、ホスト名による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逆引き参照を行ってホスト名を解決し、そのホスト名を使用します。この方法には、以下の制限事項および留意事項があります。

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追加できます。
- 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。高レベルのセキュリティ環境では、標準ユーザーと強力な権限を持つユーザーが同じクライアント上で混在しないようにしてください。
- ユーザー仕様に含まれるホストは、DHCPを使用するように構成してはいけません(固定IPを割り当てるように設定し、DNSに登録しているホストを除きます)。

ホスト名厳密チェックを使用することで達成できる安全度を正しく判断するためには、これらの制限に留意する必要があります。

ホスト名の解決

以下の状況では、Data Protectorで検証に使用されるホスト名が、デフォルトのユーザー検証を行う場合とホスト名厳密チェックを行う場合で異なることがあります。

- DNS逆引き参照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逆引き参照用テーブルの不正な設定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の場合。

この設定で有効になるチェックの特性によっては、Data Protectorユーザーを再構成する必要があります。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により影響され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、ホスト名による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逆引き参照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を使用してユーザーを構成すると、DNSに関連する検証上の問題の一部を回避することができます。ただし、このように構成すると保守が困難になります。

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、以下のそれぞれについて、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)。Windowsクライアントの場合、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。詳細は、オンラインヘルプの索引「厳密なホスト名の確認」を参照してください。
- Webレポートを使用する場合は、Webレポートの提供元になる各ホスト名について、java、applet、*hostname*を追加する必要があります。Webレポートの全機能を使用するためには、ユーザーがadminグループに属している必要があります。したがって、これらのクライアントは信頼済みクライアントである必要があります。また、(Webサーバー経由などで)Webレポートの機能を他のユーザーが使用できるようにする前に、全般的に使用可能にするデータのセキュリティについても検討してください。

ユーザー構成の詳細は、オンラインヘルプの索引「構成、ユーザー」を参照してください。

機能を使用可能にする

ホスト名厳密チェックを有効に設定するには、グローバルオプションファイルで、StrictSecurityFlagsフラグを0x0001に設定します。

グローバルオプションファイルの詳細は、『*HP Data Protectorトラブルシューティングガイド*』を参照してください。

セキュアな通信の有効化

Data Protectorの暗号制御通信により、Data Protectorセル内の不正なアクセスを防止できます。Data Protector GUIまたはCLIを使用して、Data Protectorセル内のすべてのクライアントの暗号制御通信をリモートで有効化できます。

CLIで暗号制御通信を有効化するには、以下のコマンドを実行します。

```
omnicc -encryption -enable
```

詳細は、omniccのマンページまたは『*HP Data Protector Command Line Interface Reference*』を参照してください。

重要:

暗号制御通信は、Cell Managerまたはセル内で暗号制御通信がすでに有効になっているクライアントからのみ、有効にすることができます。

暗号制御通信を有効化する方法

暗号制御通信を有効化するには、Data Protector GUI上以下の手順を実行してください。

注記:

最初にCell Manager上で暗号制御通信を有効化し、その後にセル内のクライアント上で有効化します。

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[**Data Protectorセル**]と[**クライアント**]を順に展開します。すべてのクライアントが表示されます。
3. 変更するクライアントをクリックします。
4. [接続]プロパティページで、[**暗号制御通信**]オプションを選択します。
5. [**証明書チェーン**]ドロップダウンリストで、証明書を選択します。
6. [**秘密キー**]ドロップダウンリストで、秘密キーを選択します。
7. [**信頼済み証明書**]ドロップダウンリストで、信頼済み証明書を選択します。
8. [**適用**]をクリックして変更内容を保存します。

複数のクライアントで暗号制御通信を有効化するには、Data Protector GUIで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[**クライアント**]をクリックします。
2. Scopingペインで[**Data Protectorセル**]と[**クライアント**]を順に展開します。すべてのクライアントが表示されます。

3. 暗号制御通信の有効化の実行元となるクライアントを右クリックし、[**暗号通信を有効にする**]をクリックします。
4. 暗号制御通信を有効化するクライアントを 1 つ以上選択します。[**次へ**]をクリックします。
5. [**証明書チェーン**]ドロップダウンリストで、証明書を選択します。
6. [**秘密キー**]ドロップダウンリストで、秘密キーを選択します。
7. [**信頼済み証明書**]ドロップダウンリストで、信頼済み証明書を選択します。
8. [**完了**]をクリックして変更内容を保存します。

どのような処理が行われるか

暗号化はクライアントごとに有効化されます。つまり、選択したクライアントのすべての制御通信の暗号化が有効化または無効化されます。

セキュリティの例外リストにクライアントを追加する方法

何らかの理由により保護された通信がサポートされていないクライアントは、Cell Manager例外リストに追加し、特定のクライアントの非暗号化モードによる通信を許可することができます。

セキュリティの例外リストにクライアントを追加するには、Data Protector GUIで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[**クライアント**]をクリックします。
2. Scopingペインで[**Data Protectorセル**]と[**クライアント**]を順に展開します。すべてのクライアントが表示されます。
3. 変更するCell Managerをクリックします。
4. セル内のセキュリティの例外リストに追加するシステムの名前を入力するか、[**ネットワーク**](Windows GUIのみ)または[**検索**]タブでシステムを検索します。
5. [**追加**]をクリックしてシステムをリストに追加し、[**適用**]をクリックして変更内容を保存します。

server configurationファイル

プレーンテキストモードで許可されるクライアントは、Cell Manager上の以下のディレクトリにあるserver configurationファイルに書き込まれます。

- Windows Vista、Windows Server 2008の場合:Data_Protector_program_data¥Config¥server¥config
- 他のWindowsシステムの場合:Data_Protector_home¥Config¥server¥config

- HP-UX、Solaris、およびLinuxの場合:/etc/opt/omni/server/config

システムをセキュリティの例外リストから削除するには、手順1～4を実行して**[削除]**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。

制限事項

- 非暗号化通信を使用するクライアントと暗号制御通信が有効化されたクライアントの間の通信はサポートされていません。つまり、Data Protectorの操作は実行されません(たとえば、インストールサーバーからのリモートインストールは暗号制御通信が有効化されたクライアントに対して非暗号化通信を使用するため成功しません)。

  ただし、Cell ManagerはData Protectorセル内の両方の種類のクライアントと通信できます。

[バックアップ仕様を開始]ユーザー権限

Data Protectorのユーザーおよびユーザー権限の一般的な情報は、オンラインヘルプの索引「ユーザー」を参照してください。

[バックアップ仕様を開始]ユーザー権限だけでは、GUIの[バックアップ]コンテキストを使用することができません。ユーザーは、omnibの-datalistオプションを使用してコマンドラインからバックアップ仕様を起動できます。

注記:

[バックアップ仕様を開始]**を**[バックアップ開始]**ユーザー権限と組み合わせることにより、ユーザーは、GUIに構成されたバックアップ仕様を参照することができるようになり、バックアップ仕様や会話型バックアップを起動できます。**

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。バックアップ使用を保存する権限を持つユーザーのみに対話式バックアップを許可するには、グローバルオプションファイルでStrictSecurityFlagsフラグを0x0200に設定します。

グローバルオプションファイルに関する詳細は、『*HP Data Protectorトラブルシューティングガイド*』を参照してください。

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

高レベルのセキュリティ環境では、保存されたバックアップ仕様の内容が慎重に取り扱うべき情報、または秘密情報として認識される場合があります。Data Protectorを構成して、*Save backup specification*ユーザー権限を持つユーザー以外のユーザーのバックアッ

プ仕様を隠すことができます。仕様を隠すには、グローバルオプションファイルのStrictSecurityFlagsフラグを0x0400に設定します。

グローバルオプションファイルに関する詳細は、『*HP Data Protectorトラブルシューティングガイド*』を参照してください。

ホストの信頼

ホスト信頼機能を使用すると、一定数以下のクライアントの間で1つの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だけのユーザーに対して「別のクライアントへ復元」ユーザー権限を割り当てる手間を減らすことができます。このためには、相互に信頼してデータをやり取りできるホストのグループを定義します。データのやり取りにおいて相互に信頼し合うホストのグループを定義することができます。

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の問題が原因で、クライアントのホスト名とバックアップオブジェクトの間に不適合がある場合。
- 複数のクライアントを所有していて、1つのクライアントのデータを別のクライアントに復元する必要がある場合。
- 1つのホストのデータを別のホストに移行する場合。

構成

トラストホストを構成するには、Cell Manager上にファイルData_Protector_program_data¥Config¥Server¥cell¥host_trusts(Windows Server 2008の場合)、Data_Protector_home¥Config¥Server¥cell¥host_trusts (その他のWindowsシステムの場合)、または/etc/opt/omni/server/cell/host_trusts(UNIXシステムの場合)を作成します。

相互に信頼し合うホストのグループを定義するには、ホスト名のリストを中括弧で囲みます。以下に例を示します。

例

```
GROUP="cluster.domain.com" {
cluster.domain.com node1.domain.com node2.domain.com } GROUP="Bajo" {
computer.domain.com anothercomputer.domain.com }
```

保護イベントのモニター

Data Protectorの使用時に問題が発生した場合は、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

クライアントの保護イベントは、セル内の各クライアントのinet.logファイルに記録されます。

- Windows Vista、Windows 7、およびWindows Server 2008の場合: Data_Protector_program_data¥log
- その他のWindowsシステムの場合: Data_Protector_home¥log
- HP-UX、Solaris、およびLinuxの場合: /var/opt/omni/log
- その他のUNIXシステムおよびMac OS Xシステムの場合:/usr/omni/log

Cell Manager保護イベント

Cell Managerの保護イベントは、Cell Managerのsecurity.logファイルに記録されます。

- Windows Server 2008の場合: *Data_Protector_program_data*¥log¥server
- その他のWindowsシステムの場合: *Data_Protector_home*¥log¥server
- UNIXシステムの場合: /var/opt/omni/server/log

どのData Protectorパッチがインストールされているかを確認する

セル内の各システムにどのData Protectorパッチがインストールされているかについては、確認が可能です。

前提条件

この機能を使用するには、ユーザーインタフェースコンポーネントまたはJava GUIクライアント コンポーネントがインストールされている必要があります。

注記:

サイト特定パッチのインストール後は、それが以降のパッチに含まれていたとしても、常にパッチレポートに表示されます。

セル内の特定のシステムにインストール済みのData Protectorパッチを確認するには、Data Protector GUIまたはCLIを使用します。

制限事項

パッチの確認には、以下の制限があります。

- このコマンドは、同じセル内のメンバーに対してのみ、インストール済みのパッチの確認を行います。

GUIを使用したData Protectorパッチの確認

Data Protector GUIを使用して、特定のクライアントにインストールされたパッチを確認するには、以下の手順に従ってください。

1. コンテキストリストで、[**クライアント**]を選択します。
2. Scopingペインで、[**クライアント**]を展開し、インストール済みのパッチを確認するセル内のシステムを選択します。
3. [結果エリア]で[**パッチ**]をクリックすると、[**パッチ**]ウィンドウが開きます。

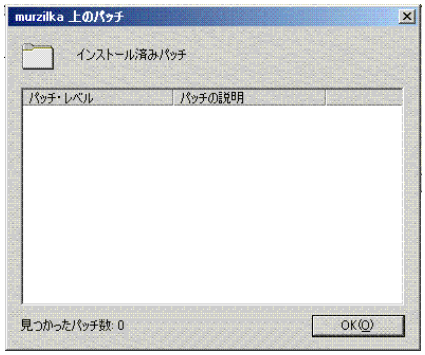


図 41 インストール済みパッチの確認

システム上でパッチが見つかった場合、各パッチのレベルと説明、インストール済みのパッチ数が表示されます。

システム上にData Protectorパッチがない場合は、空のリストが返されます。

確認対象のシステムがセルのメンバーでない場合や利用不能な場合、またはエラーが発生した場合は、エラーメッセージが表示されます。

4. [OK]をクリックしてウィンドウを閉じます。

CLIを使用したData Protectorパッチの確認

Data Protector CLIを使用して、特定のクライアントにインストールしてあるパッチを確認するには、以下のディレクトリからomnicheck -patches -host *hostname*コマンドを実行します。

- Windowsの場合: *Data_Protector_home*¥bin
- UNIXの場合: /opt/omni/bin

ここで、*hostname*は、確認対象システムの名前を表します。

omnicheckコマンドの詳細は、omnicheckマンページを参照してください。

Data Protectorソフトウェアのアンインストール

システム構成を変更した場合は、Data Protectorソフトウェアをシステムからアンインストールしたり、一部のソフトウェアコンポーネントを削除したりすることが必要になる場合があります。

アンインストールすると、システムからすべてのData Protectorソフトウェアコンポーネントが削除され、さらに、Cell Manager上のIDBからそのシステムへのすべての参照が削除されます。ただし、デフォルトでは、以降のData Protectorのアップグレードに必要になることがあるため、Data Protector構成データはシステム上に残されます。Data Protectorソフトウェアのアンインストール後に構成データを削除する場合は、Data Protectorがインストールされていたディレクトリを削除してください。

Data Protectorがインストールされているディレクトリに他のデータが含まれる場合は、Data Protectorをアンインストールする前にそのデータを別の場所にコピーしてください。この作業を行わなければ、アンインストール処理中にデータが削除されます。

Data Protectorソフトウェアをセルからアンインストールするには、以下の手順に従ってください。

1. GUIを使用してData Protectorクライアントソフトウェアをアンインストールします。詳細は、「Data Protectorクライアントのアンインストール」(243ページ)を参照してください。
2. Data Protector Cell Managerおよびインストールサーバーをアンインストールします。詳細は、「Cell Managerとインストールサーバーのアンインストール」(245ページ)を参照してください。

Cell Managerやクライアントをアンインストールせずに、Data Protectorソフトウェアコンポーネントをアンインストールすることも可能です。「Data Protectorソフトウェアコンポーネントの変更」(257ページ)を参照してください。

UNIXの場合は、Data Protectorソフトウェアを手作業で削除することも可能です。詳細は、「UNIXでのData Protectorソフトウェアの手動による削除」(255ページ)を参照してください。

前提条件

Data Protectorソフトウェアをコンピュータからアンインストールする前に、以下の条件が満たされていることを確認してください。

- コンピュータへのすべての参照がバックアップ仕様から削除されていることを確認します。削除されていない場合、Data Protectorは不明なシステムのバックアップを実行しようとするため、バックアップ仕様のこのシステムに対応する部分が正常に実行されません。オンラインヘルプの索引「変更、バックアップ仕様」を参照して、バックアップ仕様を変更する手順を確認してください。
- アンインストールを行うシステム上で接続および構成されているバックアップデバイスが存在しないことを確認します。システムがエクスポートされると、Data Protectorは元のセルのバックアップデバイスを使用できなくなります。

Data Protectorクライアントのアンインストール

注記:

リモートでアンインストールを行う場合は、Data Protectorソフトウェアのアンインストールを実行するプラットフォームにインストールサーバーがインストールされている必要があります。

Data Protector GUIで以下の手順を実行すると、クライアントをリモートでアンインストールできます。

1. コンテキストリストで、[**クライアント**]コンテキストに切り替えます。
2. Scopingペインで[**クライアント**]を展開し、アンインストール対象のクライアントを右クリックした後、[**削除**]をクリックします。Data Protectorソフトウェアをアンインストールするかどうかを尋ねるメッセージが表示されます。
3. [**はい**]をクリックして、クライアントからすべてのソフトウェアコンポーネントをアンインストールするように指定し、[**完了**]をクリックします。

選択したクライアントが[結果エリア]のリストから削除され、Data Protectorソフトウェアがそのシステムのハードディスクから物理的に削除されます。

Data Protector構成データはクライアントシステムに残ります。構成データを削除する場合は、Data Protectorがインストールされていたディレクトリを削除してください。

Data Protectorをアンインストールすると、Java GUIクライアントも削除されます。Data Protectorのアンインストール時に[Permanently delete configuration data]チェックボックスが選択されていない限り、Java GUI構成データはシステムに残ります。

クラスタークライアント

Data Protector環境内にクラスター対応クライアントがあり、それらをアンインストールする場合は、アンインストールをローカルに実行する必要があります。アンインストール手順は、Cell Managerおよびインストールサーバーのアンインストール手順と同じです。詳細は、「Cell Managerとインストールサーバーのアンインストール」(245ページ)を参照してください。

選択したクラスタークライアントが[結果エリア]のリストから削除され、Data Protectorソフトウェアがそのシステムのハードディスクから物理的に削除されます。

TruCluster

TruClusterクライアントをアンインストールするには、まず仮想ノードをエクスポートします。エクスポート後にData Protectorクライアントをノードからアンインストールします。

HP OpenVMSクライアント

Data Protector OpenVMSクライアントは、インストールサーバーを使用してリモートで削除することはできません。ローカルにアンインストールする必要があります。

OpenVMSシステムからData Protectorクライアントをアンインストールするには、以下の手順に従ってください。

1. まず、「セルからのクライアントのエクスポート」(220ページ)の説明に従って、Data Protector GUIを使用してData Protectorセルから対象クライアントをエクスポートします。

   Data Protectorソフトウェアもアンインストールするかどうかを確認するメッセージが表示されたら、[**いいえ**]を選択します。

2. 実際のData Protectorクライアントソフトウェアを削除するには、OpenVMSクライアントのSYSTEMアカウントにログインし、以下のコマンドを実行します。`$ PRODUCT REMOVE DP`.プロンプトに対してYESを選択します。

重要:

これでData Protectorサービスが停止され、OpenVMSシステムのData Protectorに関連付けられたすべてのディレクトリ、ファイル、およびアカウントが削除されます。

Cell Managerとインストールサーバーのアンインストール

ここではData Protector Cell Managerとインストールサーバーソフトウェアを Windows、HP-UX、Solaris、およびLinuxシステムからアンインストールする方法について説明します。

Windowsシステムからのアンインストール

Microsoftサーバークラスターからのアンインストール

HP AutoPassユーティリティと共にData ProtectorをMicrosoftサーバークラスターノードにインストールしている場合は、Data Protectorを同じノードからアンインストールする必要があります。アンインストールしない場合は、AutoPassがアンインストールされません。

Data ProtectorソフトウェアをWindowsシステムからアンインストールするには、以下の手順に従ってください。

1. すべてのData Protectorセッションが終了され、GUIが閉じていることを確認します。
2. Windowsの[コントロールパネル]で**[プログラムの追加と削除]**をクリックします。

3. HP AutoPassをインストールしたかどうか、またはData Protectorの構成データを削除するかどうかによって、アクションが異なります。

重要:

Data Protectorのアンインストール後も構成データをシステム上に残しておき、後からそのシステムに、アンインストールしたバージョンよりも古いData Protector Cell Managerをインストールすると、構成データが使用できなくなることに注意してください。

古いバージョンを適切にインストールするには、構成データを削除するオプションをインストール中に選択する必要があります。

以下の手順を実行します。

- AutoPassユーティリティがData Protectorとともにインストールされている場合

  [HP Data Protector 6.20]を選択し、**[変更]**、**[次へ]**の順にクリックします。[プログラムの保守]ダイアログボックスで、**[削除]**を選択します。Data Protectorの構成データを完全に削除するには、**[環境設定を削除]**を選択します。削除しない場合は、**[次へ]**をクリックします。

  Data Protectorと共にAutoPassがインストールされていて、Data Protectorでのみ使用している場合は、AutoPassが削除されます。他のアプリケーションでも使用されている場合は、Data Protectorへの登録のみ解除され、AutoPassはインストールされたままになります。AutoPassを手動で削除するには、以下のコマンドを実行します。

  ```
  msiexec.exe /X Package_GUI_ID /qr INSTALLSTANDALONE=1
  ```

  You can obtain the GUI ID by reading the registry entry HKEY_LOCAL_MACHINE¥SOFTWARE¥Hewlett-Packard¥HpOvLic.

- AutoPassがインストールされていない場合
  - Data Protectorをアンインストールして、Data Protectorの構成データをシステム上に残しておく場合は、**[HP Data Protector 6.20]**を選択し、**[削除]**をクリックします。
  - Data Protectorをアンインストールし、Data Protector構成データを削除するには、**[HP Data Protector 6.20]**を選択して、**[変更]**、**[次へ]**の順にクリックします。[プログラムの保守]ダイアログボックスで、**[削除]**を選択します。**[環境設定を削除]**を選択し、**[次へ]**をクリックします。

4. アンインストールが完了したら、**[完了]**をクリックして、ウィザードを終了します。

Cell Managerのアンインストールの際にAutoPassが削除された場合は、[プログラムの追加と削除]ウィンドウで**[F5]**キーを押すと、インストールされているプログラムとコンポーネントのリストが更新されます。

HP-UXシステムからのアンインストール

重要:

Data Protectorのアンインストール後も構成データをシステム上に残しておき、後からそのシステムに、アンインストールしたバージョンよりも古いData Protector Cell Managerをインストールすると、構成データが使用できなくなることに注意してください。

古いバージョンを適切にインストールするには、アンインストールの終了後に、残っているData Protectorディレクトリをシステムから削除する必要があります。

Data Protectorソフトウェアをアンインストールする前に、Cell Managerシステムおよびインストールサーバーシステム上で実行されているData Protectorプロセスをシャットダウンする必要があります。

1. rootユーザーとしてログインし、/opt/omni/sbinディレクトリからomnisv -stopコマンドを実行します。
2. ps -ef | grep omniコマンドを実行して、すべてのプロセスがシャットダウンされているかどうかをチェックします。ps -ef | grep omniの実行後は、Data Protectorプロセスがリストされていてはなりません。

   実行中のData Protectorプロセスがある場合は、アンインストールを開始する前に、kill *process_ID*コマンドを実行して、そのプロセスを停止してください。
3. /usr/sbin/swremove DATA-PROTECTORコマンドを実行して、Data Protectorソフトウェアをアンインストールします。
4. HP AutoPassユーティリティは、Data Protectorのアンインストール処理中は削除されません。AutoPassユーティリティは、/usr/sbin/swremove HPOVLICコマンドをrootユーザーとして実行することにより、手動で削除できます。

残っているData Protectorディレクトリをシステムから削除する方法は、「UNIXでのData Protectorソフトウェアの手動による削除」(255ページ)を参照してください。

MC/ServiceGuard上に構成されているCell ManagerおよびインストールサーバーのアンインストールMC/ServiceGuard上に構成されているCell Managerおよびインストールサーバーのアンインストール

MC/ServiceGuardクラスター上にCell Managerやインストールサーバーを構成している場合は、以下の手順に従ってソフトウェアをアンインストールしてください。

一次ノード

一次ノードにログオンし、以下の手順に従ってください。

1. Data Protectorパッケージを停止します。

   cmhaltpkg pkg_name

   pkg_nameには、クラスターパッケージの名前を指定します。

   例:

   cmhaltpkg ob2cl

2. ボリュームグループのクラスターモードを非アクティブ化します。

   vgchange -c n *vg_name*

   (vg_nameには、/devディレクトリのサブディレクトリ内に存在するボリュームグループのパス名を指定します)。

   例:

   vgchange -c n /dev/vg_ob2cm

3. ボリュームグループをアクティブ化します。

   vgchange -a y -q y *vg_name*

   例:

   vgchange -a y -q y /dev/vg_ob2cm

4. 論理ボリュームを共有ディスクにマウントします。

   mount *lv_path shared_disk*

   (lv_pathには論理ボリュームのパス名、shared_diskにはマウントポイントまたは共有ディレクトリを指定します。)

   例:

   mount /dev/vg_ob2cm/lv_ob2cm /omni_shared

5. swremoveユーティリティを使用して、Data Protectorを削除します。

6. ソフトリンクを削除します。

   rm /etc/opt/omni

   rm /var/opt/omni

7. バックアップディレクトリを削除します。

   rm -rf /etc/opt/omni.save

   rm -rf /var/opt/omni.save

8. Data Protectorディレクトリを、その内容とともに削除します。

   rm -rf /opt/omni

9. ユーザールートとして/usr/sbin/swremove HPOVLICコマンドを実行すると、HP AutoPassユーティリティを削除できます。

10. 共有ディスクのマウントを解除します。

    umount *shared_disk*

    例:

    umount /omni_shared

11. ボリュームグループを非アクティブ化します。

    vgchange -a n *vg_name*

    例:

    vgchange -a n /dev/vg_ob2cm

二次ノード

二次ノードにログオンし、以下の手順に従ってください。

1. ボリュームグループをアクティブ化します。

   vgchange -a y *vg_name*

2. 共有ディスクをマウントします。

   mount *lv_path shared_disk*

3. swremoveユーティリティを使用して、Data Protectorを削除します。

4. ソフトリンクを削除します。

   rm /etc/opt/omni

   rm /var/opt/omni

5. バックアップディレクトリを削除します。

   rm -rf /etc/opt/omni.save

   rm -rf /var/opt/omni.save

6. Data Protectorディレクトリを、その内容とともに削除します。

   rm -rf /opt/omni

7. 共有ファイルシステム内のディレクトリを削除します。

   rm -rf shared_disk/etc_opt_omni

   rm -rf shared_disk/var_opt_omni

   例:

   rm -rf /omni_shared/etc_opt_omni

   rm -rf /omni_shared/etc_opt_omni

8. ユーザールートとして/usr/sbin/swremove HPOVLICコマンドを実行すると、HP AutoPassユーティリティを削除できます。

9. 共有ディスクのマウントを解除します。

   umount *shared_disk*

10. ボリュームグループを非アクティブ化します。

    vgchange -a n *vg_name*

以上でData Protectorがシステムから完全に削除されました。

Solarisシステムからのアンインストール

Cell Manager

Solaris用のCell Managerは、omnisetup.shコマンドを使用して、常にローカルにインストールされています。したがって、pkgrmユーティリティを使用して、ローカルにアンインストールする必要があります。

重要:

Data Protectorのアンインストール後も構成データをシステム上に残しておき、後からそのシステムに、アンインストールしたバージョンよりも古いData Protector Cell Managerをインストールすると、構成データが使用できなくなることに注意してください。

古いバージョンを適切にインストールするには、アンインストールの終了後に、残っているData Protectorディレクトリをシステムから削除する必要があります。

Data Protector Cell Managerをアンインストールするには、以下の手順に従ってください。

1. すべてのData Protectorセッションを終了し、グラフィカルユーザーインタフェースを閉じておきます。

2. pkginfo | grep OB2コマンドを入力して、Cell Manager上にインストールされているすべてのパッケージを一覧表示します。

   Cell Managerに関連するパッケージは以下のとおりです。

OB2-CORE	Data Protectorのコアソフトウェア
OB2-C-IS	インストールサーバーソフトウェア
OB2-CS	Cell Managerソフトウェア
OB2-CC	Cell Consoleソフトウェアには、グラフィカルユーザーインタフェースとコマンドラインインタフェースが含まれます。

   システム上にData Protectorクライアントやインストールサーバーがインストールされている場合は、一覧内にその他のパッケージも表示されます。

   注記:

   インストールされているData Protectorコンポーネントの中に残しておきたいものがある場合は、OB2-COREパッケージを削除しないでください。これは、他のパッケージとの関連性を保つためです。

3. インストールとは逆の順番で、ステップ 2 (251ページ)で挙げたパッケージを削除します。pkgrm package nameコマンドを実行し、プロンプトに従ってください。
4. HP AutoPassユーティリティは、Data Protectorのアンインストール処理中は削除されません。ユーティリティは、rootユーザーとして以下のコマンドを実行することによって手動で削除できます。

   ```
   swremove HPOvLic
   ```

インストールサーバー

UNIX用のインストールサーバーはSolarisで、omnisetup.shコマンドを使用して、常にローカルにインストールされています。. したがって、pkgrmユーティリティを使用して、ローカルにアンインストールする必要があります。.

Data Protector インストールサーバーをアンインストールするには、以下の手順に従ってください。

1. すべてのData Protectorセッションが終了され、GUIが閉じていることを確認します。

2. pkginfo | grep OB2コマンドを実行して、すべてのインストール済みData Protectorパッケージのリストを表示します。

   インストールサーバーに関連するパッケージは以下のとおりです。

OB2-CORE	Data Protectorのコアソフトウェア
OB2-C-IS	インストールサーバーのコアソフトウェア
OB2-CFP	すべてのUNIXシステム用の共通インストールサーバーパケット
OB2-CCP	すべてのUNIXプラットフォーム用のCell Consoleリモートインストールパケット
OB2-DAP	すべてのUNIXプラットフォーム用のDisk Agentリモートインストールパケット
OB2-MAP	すべてのUNIXプラットフォーム用のMedia Agentリモートインストールパケット

   システム上にその他のData Protectorコンポーネントもインストールされている場合は、一覧内にその他のコンポーネントも示されます。

   全コンポーネントのリストおよびそれぞれの依存関係については、表9(259ページ)を参照してください。

注記:

インストールされているData Protectorコンポーネントの中に残しておきたいものがある場合は、OB2-COREパッケージを削除しないでください。これは、他のパッケージとの関連性を保つためです。

3. インストールとは逆の順番で、前述の手順で挙げたパッケージを削除します。pkgrm *package name*コマンドを実行し、プロンプトに従ってください。

Linuxシステムからのアンインストール

Cell Manager

Linux用のCell Managerは、omnisetup.shコマンドを使用して、常にローカルにインストールされています。したがって、rpmユーティリティを使用して、ローカルにアンインストールする必要があります。

重要:

Data Protectorのアンインストール後も構成データをシステム上に残しておき、後からそのシステムに、アンインストールしたバージョンよりも古いData Protector Cell Managerをインストールすると、構成データが使用できなくなることに注意してください。

古いバージョンを適切にインストールするには、アンインストールの終了後に、残っているData Protectorディレクトリをシステムから削除する必要があります。

Data Protector Cell Managerをアンインストールするには、以下の手順に従ってください。

1. すべてのData Protectorセッションを終了し、グラフィカルユーザーインタフェースを閉じておきます。

2. rpm -qa | grep OB2コマンドを入力して、Cell Manager上にインストールされているすべてのData Protectorパッケージを一覧表示します。

   Cell Managerに関連するパッケージは以下のとおりです。

OB2-CORE	Data Protectorのコアソフトウェア
OB2-CORE-IS	インストールサーバーソフトウェア
OB2-CS	Cell Managerソフトウェア
OB2-CC	Cell Consoleソフトウェア(コマンドラインインタフェースを含む)

   システム上にData Protectorクライアントやインストールサーバーがインストールされている場合は、一覧内にその他のパッケージも表示されます。

注記:

InstallされているData Protectorコンポーネントの中に残しておきたいものがある場合は、OB2-COREパッケージを削除しないでください。これは、他のパッケージとの関連性を保つためです。

3. Installとは逆の順番で、前述の手順で挙げたパッケージを削除します。rpm -e *package name*コマンドを実行し、プロンプトに従ってください。

インストールサーバー

UNIX用のインストールサーバーはLinuxで、omnisetup.shコマンドを使用して、常にローカルにインストールされています。. したがって、rpmユーティリティを使用して、ローカルにアンインストールする必要があります。.

Data Protector インストールサーバーをアンインストールするには、以下の手順に従ってください。

1. すべてのData Protectorセッションが終了され、GUIが閉じられていることを確認します。

2. `rpm -qa | grep OB2`コマンドを入力して、インストールサーバーシステムにインストールされているすべてのData Protectorパッケージを一覧表示します。

   インストールサーバーに関連するパッケージは以下のとおりです。

OB2-CORE	Data Protectorのコアソフトウェア
OB2-CORE-IS	インストールサーバーのコアソフトウェア
OB2-CFP	すべてのUNIXシステム用の共通インストールサーバーパケット
OB2-CCP	すべてのUNIXプラットフォーム用のCell Consoleリモートインストールパケット
OB2-DAP	すべてのUNIXプラットフォーム用のDisk Agentリモートインストールパケット
OB2-MAP	すべてのUNIXプラットフォーム用のMedia Agentリモートインストールパケット

   システム上にその他のData Protectorコンポーネントもインストールされている場合は、一覧内にその他のコンポーネントも示されます。

   全コンポーネントのリストおよびそれぞれの依存関係については、表10（260ページ）を参照してください。

注記：

InstallされているData Protectorコンポーネントの中に残しておきたいものがある場合は、OB2-COREパッケージを削除しないでください。これは、他のパッケージとの関連性を保つためです。

3. Installとは逆の順番で、前述の手順で挙げたパッケージを削除します。`rpm -e` *`package name`*コマンドを実行し、プロンプトに従ってください。

UNIXでのData Protectorソフトウェアの手動による削除

UNIXクライアントのアンインストールを開始する前に、そのクライアントをセルからエクスポートする必要があります。詳細は、「セルからのクライアントのエクスポート」（220ページ）を参照してください。

HP-UXシステム

HP-UXシステムからファイルを手作業で削除するには、以下の手順に従ってください。

1. /usr/sbin/swremove DATA-PROTECTORコマンドを実行して、Data Protectorソフトウェアを削除します。
2. rmコマンドを使って、以下のディレクトリを削除します。

   ```
   rm -fr /var/opt/omni
   rm -fr /etc/opt/omni
   rm -fr /opt/omni
   ```

   この時点で、Data Protectorへの参照がシステム内に残っていないことを確認してください。

Solarisシステム

Solarisシステムからファイルを手作業で削除するには、これらのファイルを以下のディレクトリから削除し、次にrmコマンドを使用してディレクトリを削除してください。

```
rm -fr /var/opt/omni
rm -fr /etc/opt/omni
rm -fr /opt/omni
```

Linuxシステム

Linuxシステムからファイルを手作業で削除するには、これらのファイルを以下のディレクトリから削除し、次にrmコマンドを使用してディレクトリを削除してください。

```
rm -fr /var/opt/omni
rm -fr /etc/opt/omni
rm -fr /opt/omni
```

その他のUNIXシステムおよびMac OS Xシステム

以下のディレクトリからファイルを削除し、次にrmコマンドを使用してディレクトリを削除してください。

```
rm -fr /usr/omni
```

Data Protectorソフトウェアコンポーネントの変更

ここでは、Data Protectorソフトウェアコンポーネントを Windows、HP-UX、Solaris、および Linuxシステムに対して削除および追加する方法について説明します。各オペレーティングシステムでサポートされているData Protectorコンポーネントの一覧は、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。

Data Protectorソフトウェアコンポーネントは、Data Protector GUIを使用して、Cell Manager またはクライアント上で追加できます。インストールサーバー機能を使用して、選択されたコンポーネントをリモートでインストールします。手順の詳細は、「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

Data Protectorコンポーネントは、Cell Managerまたはクライアントからローカルに削除できます。

Windowsシステムの場合

Windowsシステム上でData Protectorソフトウェアコンポーネントを追加または削除するには、以下の手順を行います。

1. Windowsの[コントロールパネル]で、**[プログラムの追加と削除]**を開きます。
2. **[HP Data Protector 6.20]**を選択し、**[変更]**をクリックします。
3. **[次へ]**をクリックします。
4. [プログラムの保守]ウィンドウで**[変更]**をクリックして**[次へ]**をクリックします。
5. [カスタムセットアップ]ウィンドウで、追加するソフトウェアコンポーネントを選択、または削除するコンポーネントを選択解除します。**[次へ]**をクリックします。
6. **[インストール]**をクリックして、ソフトウェアコンポーネントのインストールまたは削除を開始します。
7. Installが完了したら、**[完了]**をクリックします。

クラスター対応クライアント

クラスター対応クライアント上でData Protectorソフトウェアコンポーネントを変更する場合は、各クラストノードで、DVD-ROMからローカルに変更する必要があります。変更後、GUIを使用して、Data Protectorセルに仮想サーバーホスト名を手動でインポートする必要があります。

HP-UXシステムの場合

インストールサーバー機能を使用して新しいコンポーネントを追加できます。HP-UXシステムでは、Data Protectorソフトウェアコンポーネントが相互に依存しているため、コンポーネントを削除すると他のコンポーネントが正常に動作しなくなる可能性があります。コンポーネントとその依存関係を、次の表に示します。

表 8 HP-UX上のData Protectorソフトウェアコンポーネントの依存関係

コンポーネント	依存関係
Cell Manager	
OMNI-CC	OMNI-CORE
OMNI-CS	OMNI-CORE、OMNI-CC
OMNI-DA、OMNI-MA、OMNI-JAVAGUI、OMNI-DOCS	OMNI-CORE
インストールサーバー	
OMNI-CORE-IS	OMNI-CORE
OMNI-CF-P	OMNI-CORE-IS
OMNI-CC-P、OMNI-JGUI-P、OMNI-DA-P、OMNI-MA-P、OMNI-NDMP-P、OMNI-AUTODR-P、OMNI-DOCS-P、OMNI-CHS-LS-P、OMNI-FRA-LS-P、OMNI-JPN-LS-P、OMNI-PEGASUS-P、OMNI-INTEG-P、OMNI-VMW-P	OMNI-CORE-IS、OMNI-CF-P
OMNI-DB2-P、OMNI-EMC-P、OMNI-INF-P、OMNI-LOTUS-P、OMNI-OR8-P、OMNI-OV-P、OMNI-SAPDB-P、OMNI-SAP-P、OMNI-SSEA-P、OMNI-SYB-P	OMNI-INTEG-P、OMNI-CORE-IS、OMNI-CF-P
OMNI-SMISA-P、OMNI-VLSAM-P	OMNI-CORE-IS、OMNI-CF-P、OMNI-PEGASUS-P

手順

Data Protectorソフトウェアコンポーネントを削除するには、以下の手順を行います

1. rootユーザーとしてログインし、swremoveコマンドを実行します。
2. [B6960MA]、[DATA-PROTECTOR]、および[OB2-CM]を順にダブルクリックして、Data Protectorコンポーネントのリストを表示します。
3. 削除対象のコンポーネントを選択します。
4. [Actions]メニューで[Mark for Remove]をクリックして、削除対象のコンポーネントをマークします。
5. 削除対象のコンポーネントをマークした後、[Actions]メニューで[Remove]をクリックし、[OK]をクリックします。

注記:

削除するData Protectorコンポーネントをマークしたときに、そのコンポーネントを削除すると他のコンポーネントが正常に動作しなくなる場合は、[Dependency Message Dialog]ボックスが表示されて、依存するコンポーネントのリストが示されます。

Oracle固有の問題

Oracleサーバー上のData ProtectorOracle用統合ソフトウェアをアンインストールしても、Oracleサーバーソフトウェアの Data Protectorデータベースライブラリへのリンクはそのまま残ります。このリンクを削除しなければ、Oracle用統合ソフトウェアを削除した後にOracleサーバーを起動できません。詳細は、『*HP Data Protectorインテグレーションガイド*』の「Data Protector Oracle用統合ソフトウェア削除後のOracleの使用」を参照してください。

Solarisシステムの場合

インストールサーバー機能を使用して新しいコンポーネントを追加できます。Solarisシステムでは、Data Protectorソフトウェアコンポーネントが相互に依存しているため、コンポーネントを削除すると他のコンポーネントが正常に動作しなくなる可能性があります。コンポーネントとその依存関係を、次の表に示します。

表 9 Solaris上のData Protectorソフトウェアコンポーネントの依存関係

コンポーネント	依存関係
Cell Manager	
OB2-CC、OB2-DA、OB2-MA、OB2-JAVAGUI、OB2-DOCS	OB2-CORE

コンポーネント	依存関係
OB2-CS	OB2-CORE、OB2-CC
インストールサーバー	
OB2-C-IS	OB2-CORE
OB2-CF-P	OB2-C-IS
OB2-CCP、OB2-JGUIP、OB2-DAP、OB2-MAP、OB2-NDMPP、OB2-AUTODRP、OB2-DOCSP、OB2-CHSP、OB2-FRAP、OB2-JPNP、OB2-INTGP、OB2-VMWP	OB2-C-IS、OB2-CF-P
OB2-DB2P OB2-EMCP OB2-INFP OB2-LOTP OB2-OR8P OB2-OVP OB2-SAPDP OB2-SAPP OB2-SSEAP OB2-SYBP	OB2-INTGP、OB2-C-IS、OB2-CF-P
OB2-SMISP OB2-VLSAMP	OB2-C-IS、OB2-CF-P、OB2-PEG-P

Linuxシステムの場合

インストールサーバー機能を使用して新しいコンポーネントを追加できます。Linuxシステムでは、Data Protectorソフトウェアコンポーネントが相互に依存しているため、コンポーネントを削除すると他のコンポーネントが正常に動作しなくなる可能性があります。コンポーネントとその依存関係を、次の表に示します。

表 10 Linux上のData Protectorソフトウェアコンポーネントの依存関係

コンポーネント	依存関係
Cell Manager	
OB2-CC、OB2-DA、OB2-MA、OB2-JAVAGUI、OB2-DOCS	OB2-CORE
OB2-CS	OB2-CORE、OB2-CC
インストールサーバー	
OB2-CORE-IS	OB2-CORE
OB2-CF-P	OB2-CORE-IS

コンポーネント	依存関係
OB2-CCP、OB2-JGUIP、OB2-DAP、OB2-MAP、OB2-NDMPP、OB2-AUTODRP、OB2-DOCSP、OB2-CHSP、OB2-FRAP、OB2-JPNP、OB2-INTEGP、OB2-VMWP	OB2-CORE-IS、OB2-CF-P
OB2-DB2P OB2-EMCP OB2-INFP OB2-LOTP OB2-OR8P OB2-OVP OB2-SAPDP OB2-SAPP OB2-SSEAP OB2-SYBP	OB2-INTEGP、OB2-CORE-IS、OB2-CF-P
OB2-SMISP OB2-VLSAMP	OB2-CORE-IS、OB2-CF-P、OB2-PEG-P

手順

LinuxシステムからData Protectorソフトウェアコンポーネントを削除するには、以下の手順を実行します。

1. すべてのData Protectorセッションが終了され、GUIが閉じていることを確認します。
2. `rpm | grep OB2`コマンドを入力して、インストールされているすべてのData Protectorパッケージを一覧表示します。
3. Installとは逆の順番で、ステップ 2(261ページ)で挙げたパッケージを削除します。`rpm -e package name`コマンドを実行し、プロンプトに従ってください。

その他のUNIXシステムの場合

SolarisまたはHP-UX以外のUNIXシステムでData Protectorクライアントからコンポーネントを手動で削除する場合は、`/usr/omni/bin/install/omni_info`の`omni_info`ファイルを 更新します。

アンインストールした各コンポーネントについて、対応するコンポーネントバージョン文字列を`omni_info`ファイルから削除してください。

コンポーネントをData Protectorクライアントから削除し、クライアントがセルからエクスポートされていない場合は、`cell_info``cell_info`ファイル構成ファイル`cell_info`ファイル(Cell Manager上)のセル構成を更新する必要があります。セル構成を更新するには、セル内のCell Consoleがインストールされているシステムで以下のコマンドを実行します。

```
/opt/omni/bin/omnicc -update_host HostName
```

4 Data Protector 6.20へのアップグレード

この章の内容

この章では、Data Protectorのアップグレードと移行の手順について説明します。

アップグレードの概要

作業を開始する前に

既存のプロダクトバージョンをData Protector 6.20にアップグレードする前に、以下の点を考慮してください。

- サポート対象およびサポート対象外のプラットフォームおよびバージョンについては、http://www.hp.com/support/manualsにある最新のサポート一覧を参照してください。
- アップグレード後は、Cell Manager、およびインストールサーバーに同じバージョンのData Protectorがインストールされていなければなりません。Data ProtectorのDisk AgentおよびMedia Agentの古いバージョンは同一セル内ではサポートされていますが、Data Protectorコンポーネントのバージョンが同じクライアントをインストールすることを強くお勧めします。

  アップグレード後の古いバージョンのDisk AgentおよびMedia Agentによる制限事項については、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。
- マルチセル(MoM)環境のアップグレード後は、すべてのCell Managerに同じバージョンのData Protectorがインストールされていなければなりません。
- Data Protector A.06.00、Data Protector A.06.10、または Data Protector A.06.11の恒久ライセンスを取得している場合は、その恒久ライセンスをData Protector 6.20でも使用できます。

  上記のいずれにも当てはまらない場合は、暫定ライセンスを使用することになります。この場合、ライセンスの有効期間は、最初のインストール後60日間です。

ライセンスの詳細は、第5章（309ページ）を参照してください。

前提条件

- 既存のCell Managerシステムと内部データベース(IDB)をバックアップしてください。
- Cell ManagerをData Protector A.06.00、Data Protector A.06.10、またはData Protector A.06.11のシステムからData Protector 6.20のシステムに移行する場合は、まず既存のCell ManagerをData Protector 6.20にアップグレードする必要があります。

制限事項

- Data Protector 6.20へのアップグレードは、Data Protector A.06.00、Data Protector A.06.10、Data Protector A.06.11、およびApplication Recovery Manager A.06.00のみサポートされています。
- 以前のバージョンのData Protectorで作成した内部データベースのバックアップをData Protector 6.20で復元することはできません。Cell Managerのアップグレードが終了したら、Data Protectorの使用を継続する前に、内部データベースを必ずバックアップしてください。
- Cell Managerプラットフォームの変更は、Data Protectorの6.20 リリースでサポートされていません。アップグレードは同一のCell Managerプラットフォーム上でのみ可能です（HP-UXからHP-UXへ、SolarisからSolarisへ、LinuxからLinuxへ、および Windowsから Windowsへ）。
- Windows上でData Protector 6.20へのアップグレードを実行し、Microsoft Installer (MSI) 2.0 以前のバージョンを使用している場合は、Data Protectorセットアッププログラムにより、自動的にバージョン2.0にアップグレードされます。この場合、Data Protectorによって、アップグレードの最後の段階でMSIがアップグレードされたことが通知されます。MSIがアップグレードされた場合は、システムを再起動することを強く推奨します。個々のWindows オペレーティングシステムに対するMSI 2.0の前提条件については、Microsoft Supportにお問い合わせください。

  お使いのシステム上のMSIのバージョンを調べる場合は、エクスプローラでc:¥winnt¥system32¥msi.dllファイルを右クリックし、**[プロパティ]**を選択します。[プロパティ]ダイアログボックスで、**[バージョン]**を選択します。

アップグレードの手順

旧バージョンからData Protector 6.20にセルをアップグレードするには、以下の手順で行います。

1. Cell ManagerおよびインストールサーバーをData Protector 6.20にアップグレードします。手順は、UNIXプラットフォームとWindowsプラットフォームで異なります。

   インストールサーバーをアップグレードする前に、まず、現在のセルのCell Managerをアップグレードする必要があることに注意してください。

2. GUIクライアントをアップグレードします。
3. オンラインアプリケーション統合ソフトウェア(Oracle、SAP R/3、Informix Server、Microsoft SQL Server、Microsoft Exchange Serverなど)がインストールされているクライアントをアップグレードします。
4. Media Agent (MA)がインストールされているクライアントをアップグレードします。Cell Managerと同一のプラットフォームを使用するすべてのMAクライアントでMAがアップグレードされると、バックアップを実行できるようになります。
5. ファイルシステムDisk Agent (DA)がインストールされているクライアントを、2週間以内にアップグレードすることをお勧めします。

MoM環境でのアップグレード

MoM環境をData Protector 6.20にアップグレードするには、まずMoM Managerシステムをアップグレードする必要があります。アップグレード完了後は、アップグレードされていないすべての以前のバージョンのCell Managerで、Central MMDBおよびライセンスの集中管理にアクセスして、バックアップを実行できるようになります。ただし、その他のMoM機能は使用できません。Data Protector 6.20 MoMセルと製品の旧バージョンがインストールされたセル間のデバイスの共有はサポートされていません。MoM環境でのアップグレード処理中は、MoM環境のCell Managerがすべて非稼動状態になっている必要があります。

暗号化キーの自動移行

Cell Manager、インストールサーバー、およびすべてのクライアントをData Protector 6.20にアップグレードすると、omnikeymigrateコマンドにより、セル内のすべてのクライアントシステムから既存のkeystoreファイルがすべて移行され、Data Protector 6.20 Cell Managerの中央keystoreファイルにインポートされます。指定されたクライアントシステムからアクティブになっている暗号化キーが移行されると、この暗号化キーと共にこのクライアントシステムに関連付けられたすべてのバックアップ仕様が自動的に移行されます。インポート後は、移行されたすべての暗号化キーが無効になります。

何らかの理由で、自動移行が機能していない場合は、手動で暗号化キーを移行できます。詳細は、omnikeymigrateマンページまたは*HP Data Protector Command Line Interface Reference*を参照してください。

Data Protector A.06.00、A.06.10、およびA.06.11からのアップグレード

Data Protector A.06.00、A.06.10、およびA.06.11リリースバージョンは、UNIXおよびWindowsプラットフォームのData Protectorに直接アップグレードできます。

ライセンス

既存のData Protector A.06.00、A.06.10、A.06.11ライセンスは、Data Protector 6.20との互換性を完全に確保し、Data Protector 6.20の使用に有効です。ライセンスの詳細は、第5章(309ページ)を参照してください。

作業を開始する前に

アップグレード開始前に、アップグレード手順の制限の詳細について、「アップグレードの概要」(263ページ)を参照してください。

UNIX用Cell Managerとインストールサーバーのアップグレード

前提条件

- /opt/omni/sbin/omnisv -stopコマンドを実行して、Data Protectorサービスを停止します。
- Solairs上で古いパッチがインストールされている場合は、アップグレード前にそれらをアンインストールします。
- Installには、POSIXシェル(sh)が必要です。
- アップグレードを実行するにはroot パーミッションが必要です。

HP-UX、Solaris、またはLinux インストールサーバーが Cell Managerとともにインストールされている場合は、omnisetup. shコマンドの実行時に自動的にアップグレードされます。

HP-UX、Solaris、またはLinux インストールサーバーが 別のシステムにインストールされている場合は、「インストールサーバーのアップグレード」(270ページ)を参照してください。

Cell Managerのアップグレード

HP-UX、Solaris、またはLinux Cell Managerは、omnisetup. shコマンドの実行時に自動的にアップグレード されます。

HP-UXでは、このコマンドによって既存のパッケージセットがswinstallユーティリティを使用して直接アップグレードされます。Solarisでは、このコマンドによって、既存のパッケー

ジセットがpkgrmユーティリティを使用して削除され、pkgaddユーティリティを使用して新しいパッケージがインストールされます。Linuxでは、このコマンドによって、既存のパッケージセットがrpmを使用して直接アップグレードされます。

インストールサーバーがクライアントコンポーネントとともにインストールされている場合は、omnisetup.shコマンドによって削除されます。この場合は、omnisetup.sh -ISコマンドを使用して新しいインストールサーバーデポをインストールしてから、アップグレードしたインストールサーバーを再度インポートします。詳細は、「セルへのインストールサーバーのインポート」(216ページ)を参照してください。

MC/ServiceGuard

MC/SGで構成されているCell Managerのアップグレード手順は、MC/SG環境で実行されていないCell Managerのアップグレード手順とは異なります。手順の詳細は、「MC/ServiceGuard上で構成されているCell Managerのアップグレード」(301ページ)を参照してください。

カーネルパラメータの設定

HP-UXシステムでは、カーネルパラメータmaxdsiz(最大データセグメントサイズ)またはmaxdsiz_64 (64ビットシステムの場合)を134217728バイト(128MB)以上に、また、カーネルパラメータsemmnu (セマフォ取り消し構造体の数)を256以上に、それぞれ設定することをお勧めします。パラメータを変更したときは、カーネルを再コンパイルし、マシンを再起動してください。

Solarisの場合、/etc/system内のカーネルパラメータshmsys:shminfo_shmmax(最大共有メモリーセグメントサイズ(SHMMAX))を67108864バイト(64MB)以上に設定することをお勧めします。この変更を実行したら、マシンを再起動してください。

アップグレード手順

HP-UX用、Solaris用またはLinux用のCell ManagerをData Protector 6.20にアップグレードするには、以下の手順に従います。

1. UNIXインストールDVD-ROMをドライブに挿入し、マウントポイントにマウントします。

   例:

   ```
   mkdir /dvdrom mount /dev/c0d0t0 /dvdrom
   ```

   オプションで、ディスク上のデポからData Protectorをインストールする場合は、以下の手順を実行します。

   - Installファイルが格納されているDP_DEPOTディレクトリ、AUTOPASSディレクトリ、およびLOCAL_INSTALLディレクトリをローカルディスクにコピーする場合は、以下のコマンドを実行します。

     ```
     mkdir directory
     cp -r /dvdrom/platform_dir/DP_DEPOT directory
     cp -r /dvdrom/platform_dir/AUTOPASS directory
     cp -r /dvdrom/LOCAL_INSTALL directory
     ```

     ここで、*platform_dir*には、以下のいずれかの値を指定します。

hpux	IA-64およびPA-RISCシステム上のHP-UX
solaris	Solarisシステム
linux	Linuxシステム

   - DVD-ROM全体をローカルディスクにコピーする場合は、以下のコマンドを実行します。

     ```
     cp -r /dvdrom dvd_image_dir
     ```

2. omnisetup.shコマンドを実行します。

   このコマンドをDVD-ROMから実行するには、以下のようにして実行します。

   cd /dvdrom/LOCAL_INSTALL ./omnisetup.sh

   ディスクからインストールを開始する場合は、以下の手順を実行します。

   - DP_DEPOTディレクトリ、AUTOPASSディレクトリ、およびLOCAL_INSTALLディレクトリをローカルディスク上の*directory*にコピーした場合は、omnisetup.shコマンドが格納されているこのディレクトリに移動して以下を実行します。

     cd directory/LOCAL_INSTALL

     ./omnisetup.sh

   - DVD-ROM全体を*dvd_image_dir*にコピーした場合は、omnisetup.shコマンドをパラメータなしで実行します。

     cd dvd_image_dir/LOCAL_INSTALL

     ./omnisetup.sh

3. HPパスワードセンターのWebサーバーからインターネットを介して直接購入したライセンスのパスワードをダウンロードしてインストールする場合は、omnisetup.shにより、HP AutoPassユーティリティをインストールまたはアップグレードするためのプロンプトが表示されます。AutoPassユーティリティの詳細は、HP AutoPassのオンラインヘルプを参照してください。AutoPassをインストールすることをお勧めします。

   AutoPassをMC/ServiceGuardにインストールする場合は、すべてのノードでインストールまたはアップグレードしなければなりません。

   メッセージが表示されたら、[Return]キーを押してAutoPassをインストールまたはアップグレードします。AutoPassをインストールまたはアップグレードしない場合は、nと入力します。

   Data ProtectorのA.06.00、A.06.10、またはA.06.11バージョンの検出後に、アップグレード手順が自動的に開始されます。クリーンインストール(以前のバージョンのデータベースは削除されます)を実行するには、旧バージョンをアンインストールし、インストールを初めからやり直します。

   Installの詳細は、「UNIX用Cell Managerのインストール」(45ページ)および「UNIX用のインストールサーバーのインストール」(63ページ)を参照してください。

アップグレード完了後、Data Protectorが使用できるようになります。

omnisetup.shコマンドの説明については、DVD-ROMのMount_point/LOCAL_INSTALLディレクトリにあるREADMEファイルか、DVD-ROMのMount_point/DOCS/C/MANディレクトリにある『*HP Data Protector Command Line Interface Reference*』を参照してください。

この次に行う作業

- Cell Managerシステムとインストールサーバーシステムのアップグレードが完了したら、構成ファイルの変更が必要かどうかを確認します。「構成の変更のチェック」(276ページ)を参照してください。
- 以前のバージョンのData Protectorで作成され、Data Protector 6.20へのアップグレード後にデフォルトで1 TBに設定されている仮想テープライブラリのライブラリ容量(VTLCAPACITY)を、手動で調整する必要があります。「構成の変更のチェック」(276ページ)を参照してください。
- HP-UX 11.23および11.31 (Itanium)およびSuSE Linux (x86-64)でデータベースファイルの最大サイズがデフォルトの最大サイズの2 GBを超える場合があります。その結果、Data Protector 6.20へのアップグレード時に、データベースファイルの最大サイズを調整するように勧める警告メッセージが表示されます。この調整は、データベースのサイズによってはかなり時間がかかるため、アップグレード処理後に行ってください。(『「アップグレードのトラブルシューティング」(353ページ)』を参照)。

インストールサーバーのアップグレード

HP-UX、Solaris、またはLinux インストールサーバーは、omnisetup.shコマンドの実行時に自動的にアップグレード されます。

HP-UXでは、このコマンドによって既存のパッケージセットがswinstallユーティリティを使用して直接アップグレードされます。Solarisでは、このコマンドによって、既存のパッケージセットがpkgrmユーティリティを使用して削除され、pkgaddユーティリティを使用して新しいパッケージがインストールされます。Linuxでは、このコマンドによって、既存のパッケージセットがrpmを使用して直接アップグレードされます。

インストールサーバーがクライアントコンポーネントとともにインストールされている場合は、omnisetup.shコマンドによって削除されます。この場合は、omnisetup.sh -ISコマンドを使用して新しいインストールサーバーデポをインストールしてから、アップグレードしたインストールサーバーを再度インストールします。詳細は、「セルへのインストールサーバーのインポート」(216ページ)を参照してください。

重要:

まずCell Managerをアップグレードしなければ、インストールサーバーをアップグレードすることはできません。

アップグレード手順

HP-UX用またはSolaris用のインストールサーバーをData Protector 6.20にアップグレードするには、以下の手順に従います。

1. UNIXインストールDVD-ROMをドライブに挿入し、マウントポイントにマウントします。

   例:

   ```
   mkdir /dvdrom mount /dev/c0d0t0 /dvdrom
   ```

   オプションで、ディスク上のデポからData Protectorをインストールする場合は、以下の手順を実行します。

   - Installファイルが格納されているDP_DEPOTディレクトリおよびLOCAL_INSTALLディレクトリをローカルディスクにコピーする場合は、以下のコマンドを実行します。

     ```
     mkdir directory
     cp -r /dvdrom/platform_dir/DP_DEPOT directory
     cp -r /dvdrom/platform_dir/AUTOPASS directory
     cp -r /dvdrom/LOCAL_INSTALL directory
     ```

     *platform_dir*は、Data Protectorのアップグレードを実行するオペレーティングシステムおよびプロセッサからなるプラットフォームに応じて、以下のようになります。

hpux_ia	IA-64システム上のHP-UX
hpux_pa	PA-RISCシステム上のHP-UX
solaris	Solarisシステム
linux	Linuxシステム

   - DVD-ROM 全体をローカルディスクにコピーするには、以下を実行します。

     ```
     cp -r /dvdrom dvd_image_dir
     ```

2. omnisetup.shコマンドを実行します。

   このコマンドをDVD-ROMから実行するには、以下のようにして実行します。

   cd /dvdrom/LOCAL_INSTALL ./omnisetup.sh

   ディスクからインストールを開始するには、以下のいずれかの操作を行います。

   - DP_DEPOTディレクトリおよびLOCAL_INSTALLディレクトリをローカルディスク上の*directory*にコピーした場合は、omnisetup.shコマンドが格納されているこのディレクトリに移動して以下を実行します。

     cd directory/LOCAL_INSTALL ./omnisetup.sh

   - DVD-ROM全体を*dvd_image_dir*にコピーした場合は、omnisetup.shコマンドをパラメータなしで実行します。

     cd *dvd_image_dir*/LOCAL_INSTALL ./omnisetup.sh

アップグレード完了後、Data Protectorが使用できるようになります。

omnisetup.shコマンドの説明については、DVD-ROMのMount_point/LOCAL_INSTALLディレクトリにあるREADMEファイルか、DVD-ROMのMount_point/DOCS/C/MANディレクトリにある『*HP Data Protector Command Line Interface Reference*』を参照してください。

この次に行う作業

インストールサーバーシステムのアップグレードが完了したら、構成ファイルの変更が必要かどうかを確認します。「構成の変更のチェック」(276ページ)を参照してください。

Windows Cell Managerとインストールサーバーのアップグレード

Data Protectorの以前のバージョンが検出されると、オペレーティングシステムでは、インストール済みのものと同じコンポーネントセットが想定されます(削除されるコンポーネントなし)。既存のパッケージセットは削除され、新しい(クリーン)インストールとして新しいパッケージセットがインストールされます。

Windows インストールサーバーが Cell Managerと同じシステム上にインストールされている場合は、Windows インストールサーバーはアップグレード手順によって自動的にアップグレードされます。古いインストールサーバーデポは削除され、インストール時にインストールサーバーコンポーネントが選択されている場合は、新しいインストールサーバーデポがその場所にコピーされます。

インストールサーバーがData Protectorクライアントとともにインストールされており、このクライアントが(Data Protector GUIを使用して)リモートでアップグレードされた場合は、インストールサーバーも同時にアップグレードされます。

重要：

Install手順の終了後にアップグレード済みのインストールサーバーを再度インポートします。詳細は、「セルへのインストールサーバーのインポート」（216ページ）を参照してください。

Microsoft Cluster Server

Microsoft Cluster Server環境で実行されているCell Managerのアップグレード手順は、Microsoft Cluster Serverでの使用向けに構成されていないCell Managerのアップグレード手順とは異なります。手順の詳細は、「Microsoft Cluster Server上で構成されているCell Managerのアップグレード」（305ページ）を参照してください。

アップグレード手順

Windows用のCell ManagerとインストールサーバーをData Protector 6.20にアップグレードするには、以下の手順に従います。

1. WindowsインストールDVD-ROMをドライブに挿入し、`Windows_other¥i386¥setup.exe`コマンドを実行します。以前行ったData Protectorインストールが検出されます。[Next]をクリックして、アップグレードを開始します。
2. [Component Selection]ページで、以前にシステムにインストールされたコンポーネントが選択されています。コンポーネントは、追加のコンポーネントを選択または選択解除することによって変更できます。選択済みのコンポーネントの説明については、ウィザードの次の手順を参照してください。[Next]をクリックします。
3. *Data Protectorによってシステムに*Windows*ファイアウォールが検出されると、*[Windows Firewall configuration]ページが表示されます。Data Protectorのセットアッププログラムによって、必要なすべてのData Protector実行可能ファイルが登録されます。デフォルトでは、[Initially, enable newly registered Data Protector binaries to open ports as needed]オプションが選択されています。この時点で、Data Protectorによってポートがオープンされないようにするには、オプションを選択解除します。ただし、Data Protectorを適切に機能させるには、実行可能ファイルを有効にする必要があります。

   [Next]をクリックします。

4. コンポーネントのサマリーリストが表示されます。[Install]をクリックして、アップグレードを開始します。

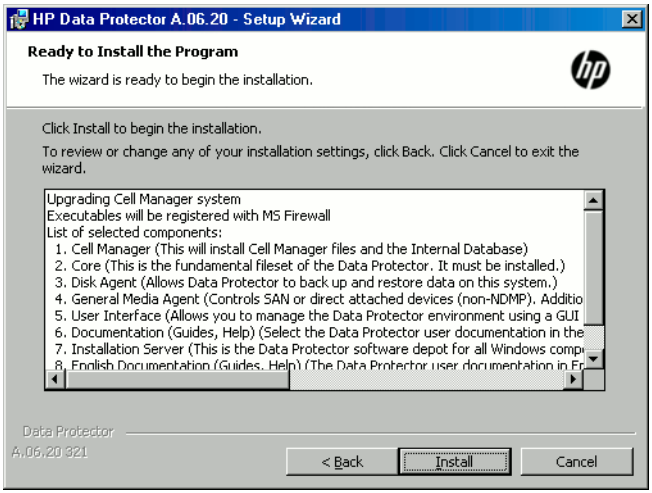


図 42 コンポーネント選択サマリーページ

5. [Installation status]ページが表示されます。[Next]をクリックします。

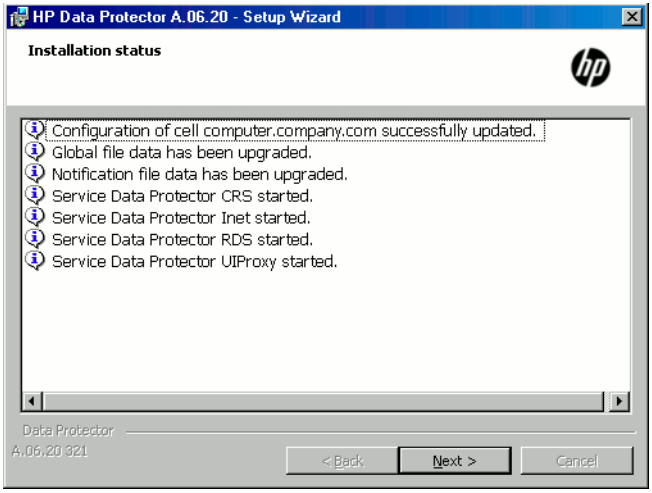


図 43 [Installation status]ページ

6. この手順はCell Managerのアップグレード時にのみ実行されます。Cell Manager 以外のクライアントにインストールされているインストールサーバーをアップグレードする場合は、この手順は発生しません。

   HPパスワードセンタのWebサーバーからインターネットを介して直接購入したライセンスのパスワードをダウンロードしてインストールする場合は、セットアップ用ウィザードでHP AutoPassユーティリティをインストールまたはアップグレードできます。AutoPassユーティリティの詳細は、「HP AutoPassユーティリティを使用した恒久パスワードの取得とインストール」(328ページ)を参照してください。

   デフォルトでは、[Start AutoPass installation]オプションまたは[Upgrade AutoPass installation]オプションが選択されています。HP AutoPassユーティリティをインストールすることをお勧めします。AutoPassをインストールまたはアップグレードしない場合は、オプションを選択解除します。

   セットアップ後すぐにData Protectorを起動するには、[Start the Data Protector Manager GUI]を選択します。

   『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を表示するには、[Open the Product Announcements]を選択します。

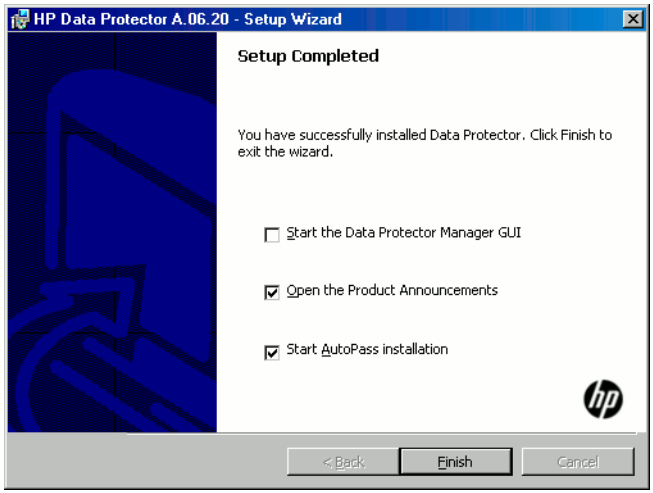


図 44 AutoPassをインストール対象として選択する場合

7. [完了]をクリックします。

アップグレード完了後、Data Protectorが使用できるようになります。

この次に行う作業

- Cell Managerシステムとインストールサーバーシステムのアップグレードが完了したら、構成ファイルの変更が必要かどうかを確認します。「構成の変更のチェック」(276ページ)を参照してください。
- 以前のバージョンのData Protectorで作成され、Data Protector 6.20へのアップグレード後にデフォルトで1 TBに設定されている仮想テープライブラリのライブラリ容量(VTLCAPACITY)を、手動で調整する必要があります。「構成の変更のチェック」(276ページ)を参照してください。

構成の変更のチェック

グローバルオプションファイル

アップグレード時には、UNIX Cell Managerでは/etc/opt/omni/server/optionsディレクトリまたはWindows Cell ManagerではData_Protector_home¥Config¥server¥Optionsディレクトリに存在する*古い*グローバルオプションファイルのコンテンツがCell Manager上の*新しい(デフォルト)*グローバルオプションファイルのコンテンツとマージされます。

- /opt/omni/newconfig/etc/opt/omni/server/options (UNIX Cell Managerの場合)
- Data_Protector_home¥NewConfig¥Server¥Options (Windows Cell Managerの場合)

globalという名前が付けられたマージ*後*のファイルは、古いファイルと同じ場所である/etc/opt/omni/server/optionsディレクトリ(UNIX Cell Managerの場合)、またはData_Protector_home¥Config¥server¥Options (Windows Cell Managerの場合)に置かれ、アップグレードされたバージョンの製品によって使用されます。*古い*グローバルオプションファイルの名前は、実行されたアップグレード数に応じてglobal.1、global.2...に変更されます。

マージファイルの作成時には、以下が適用されます。

- 古いファイルでアクティブ(コメント解除)だったグローバルオプションファイル変数は、マージファイルでもアクティブなままとなります。古いファイルから変数の値がコピーされたことを示す以下のコメントがマージファイルに付加されます。

  variable=*value* # Data Protector 6.20 # This value was automatically copied from previous version.
- 使用されなくなったグローバルオプションファイル変数は、マージ後のファイルではコメント化(非アクティブ化)され、その変数がもう使用されないことを示す以下のコメントが付加されます。

  #*variable*=*value* # Data Protector 6.20 # This value is no longer in use.

- サポート対象外となった値を持つ変数については、マージファイルにコメント(非アクティブ化)が付加されます。テンプレート(*variable_template*)を含み、この変数の以前の値を示す以下のコメントが付加されます。

  # *variable*=*variable_template* # Data Protector 6.20 # This variable cannot be transferred automatically.# The previous setting was:# *variable*=*value*

- 古いファイルのコメントは、マージ後の新しいファイルには移されません。

Windowsシステムでは、グローバルオプションファイルはUnicode形式で、メモ帳などを使用して編集できます。このファイルを編集した後は、必ずUnicode形式で保存してください。

新しいオプションについての説明は、マージ後のグローバルオプションファイルに含まれています。場所は、/etc/opt/omni/server/options/global (UNIX Cell Managerの場合)、または*Data_Protector_home*¥Config¥server¥options¥global (Windows Cell Managerの場合)です。グローバルオプションの使用方法については、『*HP Data Protectorトラブルシューティングガイド*』を参照してください。

手動で行う作業

以下に示す一覧は、アップグレードが正常に完了した後に手動で行う必要がある作業をまとめたものです。

- Omnirc ファイル

  Cell Managerおよびインストールサーバーシステムのアップグレード後は、omnircファイルを編集することもできます。ファイルの編集方法については、『*HP Data Protectorトラブルシューティングガイド*』の「Omnircオプションの使用方法」を参照してください。

- コマンドライン

  変更されたコマンドや機能が拡張されたコマンドのリストについては、付録D (437ページ)を参照してください。古いコマンドを使用しているスクリプトを確認および変更する必要があります。使用法については、該当するマンページまたは*HP Data Protector Command Line Interface Reference*を参照してください。

- DCBFディレクトリのデフォルトの最大サイズ

  すでに存在するDCBFディレクトリのデフォルト設定は、アップグレード後は変更されません。新しく作成されたディレクトリのデフォルトの最大サイズのみが16GBに設定されます。デフォルトの最大サイズを増やすときには、DCBFバイナリファイルに必要なディスクの空き容量(最大サイズの10～25%を推奨)も調整する必要があります。DCディレクトリの最大サイズを手動で変更するには、以下のコマンドを実行します。

  omnidbutil -modify_dcdir *directory* -maxsize *size_MB* -spacelow *size_MB*

  サイズの大きなドライブ(LTO 4など)を使用してテープに1000万個以上のファイルをバックアップする場合は、設定を変更する必要があります。また、DCディレクトリの存

在するファイルシステムがサイズの大きなファイルをサポートしていることを確認します。

- hostsファイルに、computer.company.com形式の完全修飾ドメイン名(FQDN)が含まれていることを確認します。この形式でない場合は、ホストのファイルをFQDNで構成します。ファイルの場所は、オペレーティングシステムによって異なります。

  Windowsシステム: %SystemRoot%¥system32¥drivers¥etc¥

  UNIXシステム: /etc/hosts

- アドバンストバックアップ使用権

  以前のバージョンのData Protectorで作成された仮想テープライブラリのライブラリ容量(VTLCAPACITY)は、Data Protector 6.20へのアップグレード後にデフォルトで1 TBに設定されます。そのため、グラフィカルユーザーインタフェース(GUI)またはコマンドラインインタフェース(CLI)を使用して、手動でライブラリ容量の推定値を入力する必要があります。

例

Data Protector 6.20へのアップグレード前は、「VTL」という名前の構成済み仮想テープライブラリについての情報は以下のようになります。

```
#omnidownload -library VTL NAME "VTL" DESCRIPTION
"" HOST computer.company.com POLICY SCSI-II TYPE DDS REPOSITORY "SCSI
repository" MGMTCONSOLEURL ""
```

Data Protector 6.20へのアップグレード後に、新しい文字列VTLCAPACITYが追加され、ライブラリ容量はデフォルトで1 TBに設定されます。

```
#omnidownload -library VTL NAME "VTL" DESCRIPTION
"" HOST computer.company.com POLICY SCSI-II TYPE DDS LIBVIRTUAL VTLCAPACITY 1
IOCTLSERIAL "" CONTROL "SCSI address" REPOSITORY "SCSI repository"
MGMTCONSOLEURL ""
```

「C:¥Temp」ディレクトリにある「libVTL.txt」というASCIIファイル内の、「VTL」という名前の仮想テープライブラリのライブラリ容量(VTLCAPACITY)を変更するには、次のコマンドを実行します。

```
omnidownload -library VTL -file C:¥Temp¥libVTL.txt
```

ライブラリ容量の推定値として、たとえば163と入力し、次のコマンドを実行します。

```
omniupload -modify_library VTL -file C:¥Temp¥libVTL.txt
```

注記:

推定仮想ライブラリ容量消費量の値(VTLCAPACITY)**は、**指定したVTL容量は無効です**というエラーメッセージを避けるために、テラバイト(TB)単位で整数で指定する必要があります。**

構成を確認するには、次のコマンドを実行します。

omnidownload -library VTL

```
#omnidownload -library VTL NAME "VTL" DESCRIPTION
"" HOST computer.company.com POLICY SCSI-II TYPE DDS LIBVIRTUAL VTLCAPACITY 163
IOCTLSERIAL "" CONTROL "SCSI address" REPOSITORY "SCSI repository"
MGMTCONSOLEURL ""
```

この次に行う作業

Cell Managerおよびインストールサーバーをインストールし、必要な変更をすべて実施したら、ソフトウェアをクライアントに配布します。「クライアントのアップグレード」(279ページ)を参照してください。

クライアントのアップグレード

アップグレード手順

クライアントのアップグレード手順は「アップグレードの概要」(263ページ)を参照してください。

クライアントのリモートアップグレード

インストールサーバーを使用してクライアントをアップグレードする手順は、「Data Protector クライアントのリモートインストール」(82ページ)を参照してください。UNIXシステムでは、新しいコンポーネントを追加する前に、既存のコンポーネントをアップグレードする必要があります。新しいコンポーネントを追加すると、以前のバージョンのコンポーネントはData Protectorに表示されません。この場合は、再度インストールする必要があります。

クライアントのローカルアップグレード

ネットワーク上にインストールサーバーがない場合、または何らかの理由によりData Protectorソフトウェアをクライアントシステムに配布できない場合は、Data Protectorクライアントをローカルにアップグレードできます。

Windowsクライアントのローカルアップグレード方法は、「Windows用クライアントのインストール」(92ページ)を参照してください。

UNIXクライアントのローカルアップグレード方法は、「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)を参照してください。

制限事項

Windows、HP-UX、およびLinuxシステムでData Protector 6.20にアップグレードする場合、拡張増分バックアップデータベースは新しいバージョンに移行されません。古い拡張増分バックアップレポジトリはData_Protector_home¥enhincrdb¥mount_pointディレクトリから削除されます。クライアントアップグレード後の最初のフルバックアップ時に、同じ場所に新しいレポジトリが作成されます。アップグレード後の最初のバックアップは、フルバックアップを実行する必要があります。

Novell NetWare

アップグレードしたシステムにNovell NetWareクライアントが含まれている場合は、NDS/eDirectoryデータベースのバックアップと復元を可能にするための追加手順が必要になります。詳細は、「Novell NetWareクライアントのローカルインストール」(131ページ)を参照してください。

Linuxクライアント

inetdサービスではなくxinetdサービスを使用している場合は、/etc/xinetd.d/omniファイルは*置き換えられない*ため、設定は変更されません。xinetdサービスが実行されているかどうかを確認するには、以下のコマンドを実行します。

```
ps -e | grep xinetd
```

設定をデフォルト設定に戻す、または破損したファイルを置き換えるには、ファイルを削除し、任意のData Protectorソフトウェアコンポーネントを Data Protector GUIからリモートでアップグレードします。/etc/xinetd.d/omniファイルがデフォルトの設定でインストールされます。

重要:

/etc/xinetd.d/omniファイルを置き換えると、変更内容は失われます。変更内容を保持するには、バックアップコピーを事前に作成しておき、アップグレードの完了後に、新しくインストールしたファイルに設定を手動で移動します。

MC/ServiceGuard上で構成されているクライアントのアップグレード

アップグレードされるData Protector用統合ソフトウェアコンポーネントがCell Managerと同じノードにインストールされる場合、MC/ServiceGuardを使用しているクライアントのアップグレードを行うには、最初に物理ノードをアップグレードしてから、以下の手順を行います。

1. 以下のコマンドを実行して仮想ホストをエクスポートします。

   omnicc -export_host *virtual_hostname*

2. 次のコマンドを実行して仮想ホストを再度インポートします。

   omnicc -import_host *virtual_hostname* -virtual

統合ソフトウェアがインストールされたクライアントのアップグレード

統合ソフトウェア(Oracle、SAP R/3、Microsoftボリュームシャドウコピーサービス、またはHP StorageWorks P6000 EVAディスクアレイファミリ用統合ソフトウェア、自動ディザスタリカバリモジュール、Microsoft Exchange Server、Microsoft SQL Server、HP StorageWorks P9000 XPディスクアレイファミリ、またはEMC Symmetrix用統合ソフトウェアなど)がインストールされたData Protectorクライアントのアップグレードを正常に行うには、以降の項に記述された手順に従ってください。

- Oracle用統合ソフトウェアのアップグレード方法の詳細は、「Oracle用統合ソフトウェアのアップグレード」(282ページ)を参照してください。
- SAP R/3用統合ソフトウェアのアップグレード方法の詳細は、「SAP R/3用統合ソフトウェアのアップグレード」(283ページ)を参照してください。
- Microsoftボリュームシャドウコピーサービス用統合ソフトウェアのアップグレード方法の詳細は、「Microsoftボリュームシャドウコピーサービス用統合ソフトウェアのアップグレード」(284ページ)を参照してください。
- HP StorageWorks P6000 EVAディスクアレイファミリ用統合ソフトウェアのアップグレード方法の詳細は、「HP StorageWorks P6000 EVAディスクアレイファミリ用統合ソフトウェアのアップグレード」(285ページ)を参照してください。
- 自動ディザスタリカバリモジュールのアップグレード方法の詳細は、「自動ディザスタリカバリモジュールのアップグレード」(285ページ)を参照してください。
- Microsoft Exchange Server、Microsoft SQL Server、HP StorageWorks P9000 XPディスクアレイファミリ、EMC Symmetrix用統合ソフトウェア、またはその他の統合ソフトウェエアのアップグレード方法の詳細は、「他の統合ソフトウェアのアップグレード」(286ページ)を参照してください。

Oracle用統合ソフトウェアのアップグレード

Oracle用統合ソフトウェアがインストールされているクライアントは、omnisetup. sh -install oracle8コマンド(UNIXシステムの場合)またはsetup. exeコマンド(Windowsシステムの場合)を実行してローカルにアップグレードするか、Data Protector GUIを使用してリモートからOracle用統合ソフトウェアエージェントをリモートでインストールしてアップグレードします。UNIXでは、Cell Managerにないクライアントをアップグレードする場合に-install oracle8オプションを指定する必要はありません。この場合、プロンプトは表示されず、アップグレード前にシステムにインストールされていたコンポーネントと同じコンポーネントが自動的に選択されます。

ユーザールートは必要ありません。

UNIXクライアントの場合、ユーザールートの下にData Protector Oracle Server用統合ソフトウェアを構成し、その構成を確認し、Oracleデータベースをブラウズする必要はありません。これらの操作は、バックアップ仕様で指定したオペレーティングシステムのユーザーアカウントの下で実行されます。したがって、ユーザールートをData Protectorユーザーグループから安全に削除できます。

注記:

ZDBおよびインスタントリカバリセッションの場合、ユーザールート**はこれまでどおり必要です。**

アップグレードした場合は、Data Protectorがオペレーティングシステムのユーザ アカウント(バックアップオーナー)を、バックアップ仕様から対応するData Protector Oracleデータベース構成ファイルへとコピー中に、各Oracleデータベースの構成チェックを実行することもお勧めします。

構成チェックを実行しないと、構成ファイルは更新されません。このような場合、復元処理の実行中、Data ProtectorはOracleデータベースを、直前のバックアップセッションのバックアップオーナーでブラウズします。過去3か月間にこのようなバック アップセッションが作成されなかった場合、最後のオプションとしてルートユーザーが使用されます。

Data Protector MML

Data Protector A.06.00 UNIXクライアントのアップグレード後は、Data Protector MMLへのシンボリックリンクは必要がなくなるため、削除します。

1. ディレクトリをORACLE_HOME/libに変更します。

2. ORACLE_HOME/libディレクトリにlibobk.sl.orig(libobk.so.orig)ファイルが存在する場合は、以下のコマンドを実行します。

   HP-UX:mv libobk.sl.orig libobk.sl

   その他のUNIXシステムの場合: mv libobk.so.orig libobk.so

   libobk.sl.orig(libobk.so.orig)は、統合ソフトウェアの構成前から存在していたOracleソフトリンクです。

インスタントリカバリのためのOracleインスタンスの構成

制御ファイル、リカバリカタログ、またはアーカイブREDOログファイルが、データベースファイルと同じボリュームグループ(LVM使用時)またはソースボリュームに置かれている場合は、Oracleインスタンスを再構成するか、またはZDB_ORA_INCLUDE_CF_OLF、ZDB_ORA_INCLUDE_SPF、ZDB_ORA_NO_CHECKCONF_IRの各omnirc変数を設定する必要があります。『*HP Data Protector Zero Downtime Backup Integration Guide*』を参照してください。

データストレージ用にHP StorageWorks P6000 EVAディスクアレイファミリを使用したOracle ASMの構成

自動ディザスタリカバリモジュール(ASM)を使用する構成のP6000 EVAアレイ上で、Oracle Serverデータの整合性のある複製の作成をサポートするためには、Oracle用統合ソフトウェアおよびHP StorageWorks P6000 EVA SMI-S Agentの両方のData Protectorコンポーネントを、アプリケーションシステムとバックアップシステムでアップグレードする必要があります。

SAP R/3用統合ソフトウェアのアップグレード

SAP R/3用統合ソフトウェアがインストールされているクライアントは、omnisetup.sh -install sapコマンド(UNIXシステムの場合)またはsetup.exeコマンド(Windowsシステムの場合)を実行してローカルにアップグレードするか、Data Protector GUIを使用してリモートからSAP R/3用統合ソフトウェアエージェントをリモートでインストールしてアップグレードします。UNIXでは、Cell Managerにないクライアントをアップグレードする場合は、-install sapオプションを指定する必要はありません。この場合、プロンプトは表示されず、アップグレード前にシステムにインストールされていたのと同じコンポーネントが自動的に選択されます。

Data Protector MML

Data Protector A.06.00 UNIX SAP R/3クライアントのアップグレード後は、Data Protector MMLへのシンボリックリンクは必要がなくなるため、削除します。詳細については、「Data Protector MML」(282ページ)を参照してください。

SAP対応ZDBセッション

SAP標準では、ZDBセッション(SAP対応ZDBセッション)処理中に、BRBACKUPをバックアップシステムで開始することをお勧めします。Data Protector 6.20を使用すると、これらの標準に対応できます。まず、バックアップシステムをOracle用のSAPガイドの説明に従って構成し(スプリットミラーバックアップ、ソフトウェア構成)、Data Protector SAP R/3 Integrationコンポーネントをバックアップシステムにインストールします。それから、『*HP Data Protector Zero Downtime Backup Integration Guide*』の説明に従ってSAP対応ZDBセッション用にData Protectorを構成します。

インスタントリカバリのためのOracleインスタンスの構成

制御ファイル、リカバリカタログ、またはアーカイブREDOログファイルが、データベースファイルと同じボリュームグループ(LVM使用時)またはソースボリュームに置かれている場合は、以下の3つのオプションがあります。

- Oracleインスタンスを再構成します。
- ZDB_ORA_INCLUDE_CF_OLF、ZDB_ORA_INCLUDE_SPF、および ZDB_ORA_NO_CHECKCONF_IR omnirc変数を設定します。
- BRBACKUPをバックアップシステム(SAP対応ZDBセッション)で開始するよう Data Protectorを構成します。

詳細は、『*HP Data Protector Zero Downtime backup Integration guide*』を参照してください。

Microsoftボリュームシャドウコピーサービス用統合ソフトウェアのアップグレード

HP Data Protector A.06.00からのアップグレード

アップグレード後は、HP Data Protector A.06.00 VSSバックアップ仕様は使用できなくなります。すべてのHP Data Protector A.06.00 VSSバックアップ仕様を再作成する必要があります。

インスタントリカバリが有効なバックアップセッションは、アップグレード後はインスタントリカバリに使用できなくなります。アップグレードを開始する前に、omnidbvssコマンドを使用してセッションを削除してください。

HP Data Protector A.06.10またはHP Data Protector A.06.11からのアップグレード後のインスタントリカバリが有効なバックアップセッション

VSS用統合ソフトウェアをData Protectorの古いバージョンからアップグレードした後、ディスクへのZDBセッションおよびディスク/テープへのZDBセッションを実行する場合は、ア

プリケーションシステム上のソースボリュームを解決する必要があります。この処理を実行しないと、ディスクへのZDBセッションは失敗し、ディスク/テープへのZDBセッションはディスクアレイに複製を維持しないテープへのバックアップでのみ完了します。セルのVSSクライアントからの解決操作は、以下のように実行します。

```
omnidbvss -resolve {-apphost ApplicationSystem | -all}
```

詳細は、『*HP Data Protector Zero Downtime backup Integration guide*』を参照してください。

HP StorageWorks P6000 EVAディスクアレイファミリ用統合ソフトウェアのアップグレード

留意事項

- Data Protector 6.20にアップグレードする場合、P6000 EVAアレイ上での複製作成の*緩和*スナップショットポリシーは、Data Protectorバージョン6.20ではサポートされていません。このディスクアレイに関するすべてのZDBセッションは、暗黙的に*厳格*スナップショットポリシーを使用します。アップグレード後に*緩和*スナップショットポリシーを使用するZDBセッションが実行された場合は、警告が報告され、*厳格*スナップショットポリシーが代わりに使用されますが、ZDBバックアップ仕様自体は更新されません。このような警告を回避するためには、上記のようなZDBバックアップ仕様を手動で更新する必要があります。

  ZDBバックアップ仕様を手動で更新して暗黙的に*厳格*スナップショットポリシーを使用するには、Data Protector GUIでバックアップ仕様を開き、そのオプションのいずれかを変更してから元に戻し、最後に**[適用]**をクリックしてバックアップ仕様を保存します。

  P6000 EVAアレイ上での複製作成のスナップショットポリシーについては、『*HP Data Protector Zero Downtime Backup Administrator's Guide*』およびオンラインヘルプを参照してください。

自動ディザスタリカバリモジュールのアップグレード

Data Protector 6.20の自動ディザスタリカバリモジュール(拡張自動ディザスタリカバリおよびワンボタンディザスタリカバリ機能)は、モジュールのA.06.00バージョン(DPWIN_00270パッチがインストールされていないバージョン)に完全には対応していません。

表11(286ページ)には、すべての組み合わせと互換性の問題が一覧表示されています。

表 11 アップグレード後のEADRおよびOBDRの互換性

Data Protectorのクライアントのバージョン		結果
バックアップ	イメージの作成	
A.06.00 (DPWIN_00270パッチなし)	A.06.00 (DPWIN_00270パッチなし)	イメージが作成されます。
A.06.00 (DPWIN_00270パッチなし)	A.06.00 (DPWIN_00270パッチあり)、A.06.10、A.06.11または6.20	エラー。
A.06.00 (DPWIN_00270パッチあり)、A.06.10、A.06.11または6.20	A.06.00 (DPWIN_00270パッチなし)	エラー。
A.06.00 (DPWIN_00270パッチあり)、A.06.10、A.06.11または6.20	A.06.00 (DPWIN_00270パッチあり)、A.06.10、A.06.11または6.20	イメージが作成されます。

EADRおよびOBDRの手順の変更点の詳細は、*HP Data Protectorディザスタリカバリガイド*を参照してください。

他の統合ソフトウェアのアップグレード

Data ProtectorクライアントにMicrosoft Exchange Server、Microsoft SQL Server、HP StorageWorks P9000 XPディスクアレイファミリ、EMC Symmetrix、またはその他の統合ソフトウェアがインストールされている場合は、omnisetup. sh -install *component_list* コマンド(UNIXシステム)、またはsetup. exeコマンド(Windowsシステム)を実行してローカルにクライアントをアップグレードするか、リモートからData Protector GUIを使用してクライアントをアップグレードします。Data Protectorコンポーネントコードの一覧は、「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)を参照してください。Cell Managerにないクライアントをアップグレードする場合は、-install *component_list*オプションを指定する必要はありません。この場合、プロンプトは表示されず、アップグレード前にシステムにインストールされていたコンポーネントと同じコンポーネントが自動的に選択されます。

MoM環境でのアップグレード

MoM環境は逐次的にアップグレードできます。ただし、以下の制限事項に注意してください。

- すべてのCell ManagerがData Protector 6.20にアップグレードされるまで、**分散ファイルメディア形式**をファイルライブラリで使用することはできません。

MoM環境をData Protector 6.20にアップグレードするには、以下の手順に従ってください。

1. MoM Manager/CMMDB ServerをData Protector 6.20にアップグレードします。

   アップグレード処理中は、MoM環境内のCell Managerが非稼動状態になければなりません。アップグレード後も、MoM Managerは古いCell Managerと連携可能です。

2. MoM環境内の各クライアントCell Managerをアップグレードします。

   アップグレード手順は、「UNIX用Cell Managerとインストールサーバーのアップグレード」(266ページ)および「Windows Cell Managerとインストールサーバーのアップグレード」(272ページ)を参照してください。

3. 構成したデバイスでクライアントをアップグレードします。

4. アプリケーション統合ソフトウェアでクライアントをアップグレードします。

   ここまでのアップグレード手順が完了すると、Data Protector 6.20 MoM GUIでファイルシステムと統合ソフトウェアをバックアップおよび復元することが可能になります。

シングルサーバー版からのアップグレード

以下のいずれかのアップグレードが可能です。

- 旧バージョンのシングルサーバー版(SSE)からData Protector 6.20シングルサーバー版へ。詳細は、「旧バージョンのSSEからData Protector 6.20 SSEへのアップグレード」(287ページ)を参照してください。
- Data Protector 6.20シングルサーバー版からData Protector 6.20へ。詳細は、「Data Protector 6.20 SSEからData Protector 6.20へのアップグレード」(288ページ)を参照してください。

旧バージョンのSSEからData Protector 6.20 SSEへのアップグレード

旧バージョンのSSEからData Protector 6.20 SSEへのアップグレード手順は、旧バージョンのData ProtectorからData Protector 6.20へのアップグレード手順と同じです。詳細は、「Data Protector A.06.00、A.06.10、およびA.06.11からのアップグレード」(266ページ)を参照してください。

Data Protector 6.20 SSEからData Protector 6.20へのアップグレード

ライセンス

Data Protector 6.20シングルサーバー版からData Protector 6.20にアップグレードするには、ライセンスが必要です。ライセンスの詳細は、第5章(309ページ)を参照してください。

Data Protector 6.20シングルサーバー版からData Protector 6.20へのアップグレードについては、次の2つの状況が考えられます。

- Data Protectorシングルサーバー版を1つのシステム(Cell Manager)にのみインストールしている場合。「Cell Managerのアップグレード」(288ページ)を参照してください。
- Data Protectorシングルサーバー版を複数のシステムにインストールしており、それらのセルをマージする場合。「複数のシステムからのアップグレード」(288ページ)を参照してください。

注記:

以前のバージョンのシングルサーバー版をData Protectorのフルインストール版にアップグレードする場合は、最初にシングルサーバー版を同じバージョンレベルのフルインストール版にアップグレードする必要があります。このフルインストール版をData Protector 6.20にアップグレードする方法は、「Data Protector A.06.00、A.06.10、およびA.06.11からのアップグレード」(266ページ)を参照してください。

Cell Managerのアップグレード

シングルサーバー版のCell Managerをアップグレードするには、以下の手順に従ってください。

1. 次のコマンドを実行して、シングルサーバー版のライセンスを削除します。
   - Windowsの場合: `del Data_Protector_home¥Config¥server¥Cell¥lic.dat`
   - UNIXの場合:`rm /etc/opt/omni/server/cell/lic.dat`
2. Data Protector GUIを起動し、恒久パスワードを追加します。

複数のシステムからのアップグレード

複数のシステムにインストールされているData Protectorシングルサーバー版をアップグレードするには、以下の手順に従ってください。

1. 既存のシングルサーバー版システムのうち、新しいCell Managerとなるシステムを1つ選択します。「Cell Managerシステムの選択」(38ページ)を参照してください。
2. 選択したCell Managerを以下のようにアップグレードします。
   a. 次のコマンドを実行して、シングルサーバー版のライセンスを削除します。

      del Data_Protector_home¥Config¥server¥Cell¥lic.dat (Windowsシステム)または

      rm /etc/opt/omni/server/cell/lic.dat (UNIXシステム)

   b. Data Protector GUIを起動し、恒久パスワードを追加します。
3. GUIを使用して、他のシングルサーバー版システムを新たに作成したCell Managerシステムに、クライアントとしてインポートします。
4. 他のシステムからData Protectorシングルサーバー版をアンインストールします。「Data Protectorソフトウェアのアンインストール」(242ページ)を参照してください。
5. 必要に応じて、新しいCell Managerにメディアをインポートします。

   他のシングルサーバー版システムで作成したメディアから頻繁に復元を実行する場合に、この手順を実行します。こうした復元を実行する可能性が比較的低い場合は、List from mediaによる復元方法を使用できます。オンラインヘルプの索引「インポート、メディア」を参照して、メディアのインポート方法およびList from mediaによる復元方法の詳細をご確認ください。

HP StorageWorks Application Recovery Manager A.06.00からのアップグレード

概要

Application Recovery Managerは、ExchangeおよびSQLアプリケーションデータの自動バックアップおよび復旧機能を提供し、数分単位のデータ復旧によってアプリケーションの可用性を高めるスケーラブルな復旧ソフトウェアソリューションです。

Data Protector 6.20では、Application Recovery Manager A.06.00からのアップグレードおよびすべてのApplication Recovery Manager A.06.00 機能がサポートされています。構成および内部データベースはアップグレード後も維持されます。

制限事項

- Cell Managerプラットフォームの変更は、Data Protectorの6.20リリースでサポートされていません。アップグレードは同一のCell Managerプラットフォーム上でのみ可能で

す(32ビットWindowsから32ビットWindowsへ、または64ビットWindowsから64ビットWindowsへ)。

アップグレード手順

Application Recovery Manager A.06.00からData Protector 6.20へのアップグレード手順は、旧バージョンのData ProtectorからData Protector 6.20へのアップグレード手順と同じです。Cell Managerのアップグレードおよびクライアントのアップグレードを参照してください。

アップグレード後の内部データベースのバックアップ

dbtool.plによって作成された内部データベースの古いバックアップは、Data Protectorで使用できません。内部データベースおよび構成をバックアップするには、新しいバックアップ仕様を構成する必要があります。オンラインヘルプの索引「IDB, configuring backups」を参照してください。

テープデバイスを使用する以外に、Data ProtectorでのIDBバックアップは、以下の点でApplication Recovery Managerと異なります。

- dbtool.plのように、バックアップ中にData Protectorサ ービスが停止されることはありません。
- VSSデータベースはバックアップされません

バックアップ仕様のアップグレード

Application Recovery Managerのバックアップ仕様には、テープデバイスが含まれていません。Data Protectorへのアップグレード後は、ディスクへのZDBのみにバックアップ仕様を使用できます。テープ機能(ディスク/テープへのZDB、テープへのZDB)を使用するには、テープデバイスを指定し、バックアップ仕様を再構成する必要があります。

omnib使用方法の変更点

オプションが指定されていない場合は、Data Protectorは、デフォルトでディスク/テープへのZDBに設定されます。omnibコマンドを使用してCLIから開始したApplication Recovery Managerのバックアップセッションは、テープデバイスが見つからないため失敗します。ディスク/テープへのZDB用に再構成せずに既存のバックアップ仕様を維持するには、-disk_onlyオプションを使用してディスクへのZDBを実行します。

Solaris 8からSolaris 9へのアップグレード

Solaris 8にData Protector 6.20 Disk Agent (DA)がインストールされ、オペレーティングシステムをSolaris 9にアップグレードする場合は、アップグレードがData Protectorに及ぼす影響を考慮してください。Data Protectorの適切な動作を確保し、拡張属性のバックアップなどの高度なバックアップオプションをSolaris 9で使用できるようにするには、システムにインストールされている汎用Solaris DAをSolaris 9 DAに置き換えることをお勧めします。

以下の順番でアップグレードしてください。

1. オペレーティングシステムをSolaris 8からSolaris 9にアップグレードします。詳細はSolarisのマニュアルを参照してください。
2. インストールサーバーを使用して、アップグレードしたシステムにDisk Agentをリモートインストールします。これにより、汎用のSolaris Disk AgentがSolaris 9 Disk Agentに置き換えられます。「Data Protectorクライアントのリモートインストール」(82ページ)を参照するか、またはob2installのマンページを参照してください。

HP-UX 11.x (PA-RISC)からHP-UX 11.23/11.31 (IA-64)への移行

ここでは、既存のCell ManagerをPA-RISC アーキテクチャベースのHP-UX 11.xシステムからIntel Itanium 2 (IA-64) アーキテクチャ対応のHP-UX 11.23/11.31に移行する手順を述べます。

制限事項

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、プラットフォーム、プロセッサのアーキテクチャ、およびData Protectorのコンポーネント、必要なパッチ、一般的な制限事項、およびインストールの前提条件の詳細は、*HP Data Protector製品案内*、*ソフトウェアノート*、*リファレンス*を参照してください。

- サポートされている移行は、PA-RISCベースのHP-UX 11.xシステム上のData Protector 6.20 Cell Managerからの移行だけです。
- サポートされているMoM構成の組み合わせについては、「MoM 固有の手順」(295ページ)を参照してください。

前提条件

- 移行を開始する前に、PA-RISCベースのHP-UX 11.xシステム上のData Protector Cell ManagerをData Protector 6.20にアップグレードする必要があります。

ライセンス

新しいCell Manager (IA-64 system)のIPアドレスは古いCell Managerとは異なるため、移行前にライセンスの移行を適用してください。一定期間は、両方のシステムでライセンスは有効になります。ライセンスがIPの範囲に基づいており、新しいCell ManagerのIPアドレスがこの範囲内にある場合は、ライセンスを再構成は必要ありません。詳細は、「Data Protector 6.20へのライセンス移行」(339ページ)を参照してください。

注記:

Cell Managerでは元のData Protector GUIがサポートされません。Data Protector Java GUIを使用するか、Data Protector GUIがサポートされているシステムにData Protector GUIをインストールしてください。omniusersコマンドを使用して、新しいCell Manager上にリモートユーザーアカウントを作成します。作成すると、Data Protector GUIをインストールした任意のシステム上でこのユーザーアカウントにより、GUIを起動して新しいCell Managerに接続できます。詳細は、omniusersのマンページを参照してください。

移行手順

以下の手順に従って移行してください。

1. IA-64システム上にData Protectorクライアントをインストールし、それを古いCell Managerのセルにインポートします。Data Protectorをクラスター内に構成する場合は、一次ノード上にクライアントをインストールします。「HP-UXクライアントのインストール」(99ページ)を参照してください。
2. *古い* Cell Manager上で以下のコマンドを実行し、保護が設定されたクライアントの信頼されるホスト一覧にIA-64システムのホスト名を追加します。

   omnimigrate.pl -prepare_clients *New_CM_Name* (ここで*New_CM_Name*は、前の手順のIA-64システムのクライアント名です。)

   信頼されるホストとData Protectorクライアントの保護設定の詳細は、「クライアントの保護設定」(227ページ)および「ホストの信頼」(239ページ)を参照してください。
3. IDBをバックアップします。新しいCell Managerシステム上で、以後も使用済みメディアにアクセスできることを確認してください。オンラインヘルプの索引「IDBバックアップ」を参照してください。
4. IDBをIA-64システム上の一時保存場所に復元します。オンラインヘルプの索引「IDB復元」を参照してください。
5. Data ProtectorクライアントをIA-64システムからアンインストールします。「Data Protectorクライアントのアンインストール」(243ページ)を参照してください。

6. IA-64システムにData Protector Cell Managerをインストールします。Data Protectorをクラスターに構成する場合は、Cell Managerを*スタンドアロン* Cell Manager (非クラスター対応)として一次ノードにインストールします。「Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール」(44ページ)を参照してください。

7. 古いCell Manager上のデフォルトのData Protector Inetポートを変更した場合は、新しいCell Manager上にも同じInetポートを設定します。「Data Protectorのデフォルトのポート番号の変更」(388ページ)を参照してください。

8. 新しいCell Managerの一時保存場所にある復元されたIDBと構成データを、新しいCell Manager上の、古いCell Managerと同じ場所に移動します。オンラインヘルプの索引「IDB復元」を参照してください。

   古いCell Managerがクラスター対応である場合は、/etc/opt/omni/server/sg/sg.confファイルのSHARED_DISK_ROOT 変数とCS_SERVICE_HOSTNAME変数をコメントアウトします。この作業は、新しいCell Managerがクラスター対応の場合も必要です。

9. IDBおよびクライアントを新しいCell Managerに移行し、Cell Managerの設定を再構成するには、*新しい* Cell Manager上で以下の手順を実行します。

   - スタンドアロンIA-64 Cell Managerを構成する場合は、omnimigrate.pl -configureコマンドを実行します。詳細は、omnimigrate.plのマンページを参照してください。
   - クラスター対応 IA-64 Cell Managerを構成する場合は、以下の手順に従ってください。

     a. omnimigrate -configure_idbコマンドを実行して、古いCell Managerからから移したIDBを、新しいCell Managerで使えるように構成します。詳細は、omnimigrate.plのマンページを参照してください。

     b. omnimigrate -configure_cmコマンドを実行して、古いCell Managerから移した構成データを、新しいCell Manager上で使えるように再構成します。詳細は、omnimigrate.plのマンページを参照してください。

     c. omnicc -export_host *Old_CM_Name*を実行して、古い仮想サーバーをセルからエクスポートします。

     d. 一次および二次Cell Managerを構成します。オンラインヘルプの索引「MC/ServiceGuard用統合ソフトウェアの構成」を参照してください。

     e. omnimigrate -configure_clientsコマンドを実行して、古いCell Managerから新しいCell Managerにクライアントを移行します。古いCell Managerの構成ファイルにはクライアントが残っていることに注意してください。そのクライアントのCell Managerは存在しません。

注記:

/etc/opt/omni/serverディレクトリが共有クラスターボリュームにある場合は、omnimigrate.plスクリプトによる構成の変更がクラスターのすべてのノードに影響します。

注記:

古いCell Managerは、自動的に新しいセルのクライアントとなります。古いCell Manager上ではCell Managerコンポーネントが不必要なため、アンインストールしても構いません。「Data Protectorソフトウェアコンポーネントの変更」(257ページ)を参照してください。

10. 新しいCell Manager上でライセンスを構成します。「Data Protector 6.20の製品構成とライセンス」(336ページ)を参照してください。

11. 新しいCell Managerでリモートユーザーアカウントを作成し、Data Protector GUIをインストールした他のシステム上で新しく作成したユーザーアカウントを使用して、GUIを起動して新しいCell Managerに接続します。詳細は、omniusersのマンページを参照してください。

12. 以下に該当する場合は、さらに手順を実行する必要があります。

    - セルがMoM環境の一部である場合。詳細は、「MoM 固有の手順」(295ページ)を参照してください。
    - セルがファイアウォールを越えて機能する場合。新しいCell Manager上にファイアウォールに関連するすべての設定を再構成します。オンラインヘルプの索引「ファイアウォール環境」を参照してください。
    - 新しいCell Manager上にインストールサーバーを配置する場合。「インストールサーバー 固有の手順」(296ページ)を参照してください。

MoM 固有の手順

新しいCell ManagerをMoM構成にする場合、基本的な移行手順が完了した後にさらに手順を実行する必要があります。必要な手順は、環境における新旧のCell Managerに対するMoM構成によって異なります。以下の組み合わせがサポートされています。

- 古いCell ManagerはMoMクライアントでした。新しいCell Managerは同じMoM ManagerのMoMクライアントになります。

  この場合、以下の手順を実行します。

  1. MoM Managerで、古いCell ManagerをMoM Managerセルからエクスポートし、新しいCell Managerをインポートします。オンラインヘルプの索引「クライアントシステムのエクスポート」を参照してください。
  2. MoM 管理者を新しいCell Managerのユーザーリストに追加します。オンラインヘルプの索引「MoM管理者、追加」を参照してください。

- 古いCell ManagerはMoM Managerでした。新しいCell ManagerはMoM Managerになります。

  古いMoM ManagerがMoMで唯一のクライアントである場合、処理は必要ありません。それ以外の場合、以下の手順を実行してください。

  1. 古いMoM Manager (古いCell Manager)で、すべてのMoMクライアントをエクスポートします。
  2. 新しいMoM Manager (新しいCell Manager)で、すべてのMoMクライアントをインポートします。
  3. すべてのMoMクライアントのユーザーリストにMoM 管理者を追加します。

注記：

Cell Managerでは元のData Protector GUIがサポートされません。Data Protector Java GUIを使用するか、Data Protector GUIがサポートされているシステムにData Protector GUIをインストールしてください。omniusersコマンドを使用して、新しいCell Manager上にリモートユーザーアカウントを作成します。作成すると、Data Protector GUIをインストールした任意のシステム上でこのユーザーアカウントにより、GUIを起動して新しいCell Managerに接続できます。詳細は、omniusersのマンページを参照してください。

インストールサーバー 固有の手順

インストールサーバーの移行はCell Managerの移行の一部として行われません。古いCell Manager上にインストールサーバーをインストールしている場合は、インストールサーバーが新しいCell Managerに移行されずにセルに残ります。

新しいCell Managerもインストールサーバーとしても使用する場合は、移行後に新しいCell Manager上にインストールサーバーコンポーネントをインストールし、セルにインポートします。オンラインヘルプの索引「インストールサーバー」を参照してください。

32ビット/64ビットWindowsから64ビットWindows/Windows Server 2008への移行

このセクションでは、既存のCell Managerを32ビットWindowsシステムから64ビットWindowsシステムに、または64ビットWindowsシステムから64ビットWindows Server 2008システムに移行する手順について説明します。

制限事項

サポートされているオペレーティングシステムバージョン、サポートされているプラットフォーム、サポートされているプロセッサ、サポートされているData Protectorコンポーネント、必要なパッチ、一般情報、およびインストールの前提条件については、『HP Data Protector製品案内、ソフトウェアノート、リファレンス』を参照してください。

前提条件

- 移行を開始する前に、32ビットWindowsシステム上のData Protector Cell ManagerをData Protector 6.20にアップグレードする必要があります。

ライセンス

新しいCell ManagerのIPアドレスは古いCell Managerとは異なるため、移行前にライセンスの移行を適用してください。一定期間は、両方のシステムでライセンスは有効になります。ライセンスがIPの範囲に基づいており、新しいCell ManagerのIPアドレスがこの範囲内にある場合は、ライセンスを再構成は必要ありません。詳細は、「Data Protector 6.20へのライセンス移行」(339ページ)を参照してください。

移行手順

以下の手順に従って移行してください。

1. 新しいCell Managerになる64ビットWindowsシステムまたは64ビットWindows Server 2008システムに、Data Protectorクライアントをインストールします。詳細は、「Windows用クライアントのインストール」(92ページ)を参照してください。
2. システムを古いCell Manager'のセルにインポートします。
3. *古い*Cell Manager上で、保護が設定されたクライアントの信頼されるホスト一覧に新しいCell Managerのホスト名を追加します。Data_Protector_home¥binディレクトリから以下のコマンドを実行してください。

   perl winomnimigrate.pl -prepare_clients *New_CM_Name*

   *New_CM_Name*には、前の手順の新しいCell Managerのクライアント名を指定します。winomnimigrate.plの詳細は、『*HP Data Protector Command Line Interface Reference*』を参照してください。

   信頼されるホストとData Protectorクライアントの保護設定の詳細は、「クライアントの保護設定」(227ページ)および「ホストの信頼」(239ページ)を参照してください。
4. IDBをバックアップします。新しいCell Managerシステム上で、以後も使用済みメディアにアクセスできることを確認してください。オンラインヘルプの索引「IDBバックアップ」を参照してください。
5. IDBを新しいCell Manager上の一時保存場所に復元します。IDBバックアップで選択するオプションによっては、デバイスを構成し、適切なメディアからカタログをインポートする必要があります。IDBバックアップオブジェクトがIDB内にあると、構成データを新しいシステムに移動させるためにIDBを復元することができます。オンラインヘルプの索引「IDB復元」を参照してください。
6. Data Protectorクライアントを新しいCell Managerからアンインストールします。「Data Protectorクライアントのアンインストール」(243ページ)を参照してください。
7. 新しいCell Manager上でのData Protector Cell Managerのインストール「Data Protector Cell Manager (CM)およびCell Manager (IS)のインストール」(44ページ)を参照してください。

8. 古いCell Manager上でデフォルトのData Protector Inetポートを変更していた場合は、新しいCell Manager上でも同じInetポートを設定します。「Data Protectorのデフォルトのポート番号の変更」(388ページ)を参照してください。

9. 新しいCell Managerの一時保存場所にある復元されたIDBと構成データを、新しいCell Manager上の、古いCell Managerと同じ場所に移動します。Data Protectorのサービスを再起動しないでください。オンラインヘルプの索引「IDB復元」を参照してください。

注記:

32ビット/64ビットのWindowsから64ビットのWindows/Windows Server 2008への移行時は、IDBファイルは新しいデフォルトのディレクトリに再配置されます。そのため、IDBファイルが移行前と同じディレクトリ(*Data_Protector_program_data*ではなく*Data_Protector_home*以下)にあるようにする必要があります。

10. IDBとクライアントを新しいCell Managerに移行し、Cell Managerの設定を再構成するため、*新しい* Cell Manager上で以下の手順を実行します。

- スタンドアロンCell Managerを構成するData_Protector_home¥binディレクトリから以下のコマンドを実行します。

  perl winomnimigrate.pl -configure

  Cell Managerを64ビットWindows Server 2008システムに移行する場合は、オプション-keep_dcdirsを指定して、移行したIDBの追加DCBFディレクトリに対する参照を無条件に維持することができます。

  perl winomnimigrate.pl -configure -keep_dcdirs

- クラスター対応のCell Managerを構成する場合は、以下の手順に従ってください。

  a. Data_Protector_home¥binディレクトリからperl winomnimigrate.pl -configure_idbコマンドを実行して、古いCell Managerから移したIDBを、新しいCell Manager上で使えるように構成します。

     Cell Managerを64ビットWindows Server 2008システムに移行する場合は、オプション-keep_dcdirsを指定して、移行したIDBの追加DCBFディレクトリに対する参照を無条件に維持することができます。perl winomnimigrate.pl -configure_idb -keep_dcdirs

  b. Data_Protector_home¥binディレクトリからperl winomnimigrate.pl -configure_cmコマンドを実行して、古いCell Managerから移した構成データを、新しいCell Manager上で使えるように再構成します。

  c. omnicc -export_host *Old_CM_Name*コマンドを実行して、古い仮想サーバーをセルからエクスポートします。

  d. Data_Protector_home¥binディレクトリからperl winomnimigrate.pl -configure_clientsコマンドを実行して、クライアントを古いCell Managerから新しいCell Managerに移行します。古いCell Managerの構成ファイルにはクライアントが残っていることに注意してください。そのクライアントのCell Managerは存在ません。

注記:

古いCell Managerは、自動的に新しいセルのクライアントとなります。古いCell Manager上ではCell Managerコンポーネントが不必要なため、アンインストールしても構いません。「Data Protectorソフトウェアコンポーネントの変更」(257ページ)を参照してください。

11. 古いCell Managerがインストールされていたディレクトリ以外のディレクトリに新しい64ビットCell Managerをインストールした場合も、IDBの内部リンクには古いCell Managerのパスが含まれます。新しいCell ManagerでData Protector GUIを使用して、Detail Catalog (DC)ディレクトリの新しいパスを手動で追加します。オンラインヘルプの索引「DCディレクトリの作成」を参照してください。

12. 新しいCell Manager上でライセンスを構成します。「Data Protector 6.20の製品構成とライセンス」(336ページ)を参照してください。

13. 以下の場合は追加の手順が必要になります。

    - セルがMoM環境の一部である場合。「MoM 固有の手順」(300ページ)を参照してください。
    - セルがファイアウォールを越えて機能する場合。新しいCell Manager上にファイアウォールに関連するすべての設定を再構成します。オンラインヘルプの索引「ファイアウォール環境」を参照してください。
    - 新しいCell Manager上にインストールサーバーを配置する場合。「インストールサーバー 固有の手順」(301ページ)を参照してください。

MoM 固有の手順

新しいCell ManagerをMoM構成にする場合、基本的な移行手順が完了後にさらに手順を実行する必要があります。必要な手順は、環境における新旧のCell Managerに対するMoM構成によって異なります。以下の組み合わせがサポートされています。

- 古いCell ManagerはMoMクライアントでした。新しいCell Managerは同じMoM ManagerのMoMクライアントになります。

  この場合、以下の手順を実行します。

  1. MoM Managerで、古いCell ManagerをMoM Managerセルからエクスポートし、新しいCell Managerをインポートします。オンラインヘルプの索引「クライアントシステム、エクスポート」を参照してください。
  2. MoM 管理者を新しいCell Managerのユーザーリストに追加します。オンラインヘルプの索引「MoM管理者、追加」を参照してください。

- 古いCell ManagerはMoM Managerでした。新しいCell ManagerはMoM Managerになります。

  古いMoM ManagerがMoMで唯一のクライアントである場合、処理は必要ありません。それ 以外の場合は、以下の手順を実行してください。

  1. 古いMoM Manager (古いCell Manager)で、すべてのMoMクライアントをエクスポートします。
  2. 新しいMoM Manager (新しいCell Manager)で、すべてのMoMクライアントをインポートします。

3. すべてのMoMクライアントのユーザーリストにMoM 管理者を追加します。

インストールサーバー 固有の手順

インストールサーバーの移行はCell Managerの移行の一部として行われません。古いCell Manager上にインストールサーバーをインストールしている場合は、インストールサーバーが新しいCell Managerに移行されません。

新しいCell Managerもインストールサーバーとしても使用する場合は、移行後に新しいCell Manager上にインストールサーバーコンポーネントをにインストールし、セルにインポートします。オンラインヘルプの索引「インストールサーバー」を参照してください。

MC/ServiceGuard上で構成されているCell Managerのアップグレード

アップグレード時には、データベースのみがアップグレードされて、古いバージョンの製品は削除されます。Data Protector 6.20はデフォルトで選択されるエージェントとともにインストールされ、その他のエージェントは削除されます。アップグレード前と同じ構成にしたい場合は、必要なエージェントをアップグレード時に手作業で選択するか、各物理ノード上に後から再インストールしなければなりません。

Data Protector A.06.00、A.06.10、または A.06.11からのアップグレードでは、一次ノードと二次ノードのアップグレードが必要です。以下の手順に従ってください。

一次ノード

一次ノードにログオンし、以下の手順に従ってください。

1. cmhaltpkg pkg_nameコマンドを実行して(pkg_nameにはクラスターパッケージの名前を指定)、古いData Protectorパッケージを停止します。例:

   ```
   cmhaltpkg ob2cl
   ```

2. 以下のようにボリュームグループを排他モードでアクティブ化します。

   ```
   vgchange -a e -q y vg_name
   ```

   例:

   ```
   vgchange -a e -q y /dev/vg_ob2cm
   ```

3. 論理ボリュームを共有ディスクにマウントします。

   mount *lv_path shared_disk*

   lv_pathパラメータには論理ボリュームのパス名を、shared_diskパラメータにはマウントポイントまたは共有ディレクトリを指定します。例:

   mount /dev/vg_ob2cm/lv_ob2cm /omni_shared

4. 以下の手順に従って、Cell Managerをアップグレードします。Data Protector 6.20にアップグレードする製品のバージョンによって、手順が一部異なります。「UNIX用Cell Managerとインストールサーバーのアップグレード」(266ページ)を参照してください。

5. 実行されているData Protectorサービスがあれば、停止します。

   /opt/omni/sbin/omnisv -stop

6. 共有ディスクのマウントを解除します。

   umount *shared_disk*

   例:

   umount /omni_shared

7. ボリュームグループを非アクティブ化します。

   vgchange -a n *vg_name*

   例:

   vgchange -a n /dev/vg_ob2cm

二次ノード

二次ノードにログオンし、以下の手順に従ってください。

1. 以下のようにボリュームグループを排他モードでアクティブ化します。

   vgchange -a e -q y *vg_name*

2. 論理ボリュームを共有ディスクにマウントします。

   mount *lv_path shared_disk*

3. Cell Managerをアップグレードします。Data Protector 6.20にアップグレードする製品のバージョンによって、手順が異なります。「UNIX用Cell Managerとインストールサーバーのアップグレード」(266ページ)で説明されている手順に従ってください。

4. /etc/opt/omni/server/sgディレクトリのcsfailover.sh起動スクリプトとmafailover.ksh起動スクリプトの名前をcsfailover_DP55.shやmafailover_DP55.kshに変更し、新しいcsfailover.shスクリプトとmafailover.kshスクリプトを/opt/omni/newconfig/etc/opt/omni/server/sgディレクトリから/etc/opt/omni/server/sgディレクトリにコピーします。

   古い起動スクリプトをカスタマイズしていた場合は、新しい起動スクリプトにも変更を再実装します。

5. 実行されているData Protectorサービスがあれば、停止します。

   /opt/omni/sbin/omnisv -stop

6. 共有ディスクのマウントを解除します。

   umount *shared_disk*

7. ボリュームグループを非アクティブ化します。

   vgchange -a n *vg_name*

一次ノード

一次ノードに再度ログインし、以下の手順に従ってください。

1. Data Protectorパッケージを再起動します。

   cmrunpkg pkg_name

   パッケージ切り替えおよびノード切り替えオプションが有効になっていることを確認します。

2. Cell Managerを構成します。スクリプトを実行するときに/etc/opt/omniディレクトリや/var/opt/omniディレクトリ、あるいはサブディレクトリに配置しないようにします。/etc/opt/omniまたは/var/opt/omniにサブディレクトリがマウントされていないことも確認してください。以下のコマンドを実行します。

   /opt/omni/sbin/install/omniforsg.ksh -primary -upgrade

3. 実行されているData Protectorサービスがあれば、停止します。

   /opt/omni/sbin/omnisv -stop

4. 共有ディスクのマウントを解除します。

   umount *shared_disk*

5. ボリュームグループを非アクティブ化します。

   vgchange -a n *vg_name*

二次ノード

二次ノードにもう一度ログオンし、以下の手順に従ってください。

1. Data Protectorパッケージを再起動します。

   cmrunpkg pkg_name

   パッケージ切り替えおよびノード切り替えオプションが有効になっていることを確認します。

2. Cell Managerを構成します。スクリプトを実行するときに/etc/opt/omniディレクトリや/var/opt/omniディレクトリ、あるいはサブディレクトリに配置しないようにします。/etc/opt/omniまたは/var/opt/omniにサブディレクトリがマウントされていないことも確認してください。以下のコマンドを実行します。

   /opt/omni/sbin/install/omniforsg.ksh -secondary /share -upgrade

3. 実行されているData Protectorサービスがあれば、停止します。

   /opt/omni/sbin/omnisv -stop

4. 共有ディスクのマウントを解除します。

   umount *shared_disk*

5. ボリュームグループを非アクティブ化します。

   vgchange -a n *vg_name*

一次ノード

一次ノードに再度ログインし、以下の手順に従ってください。

1. Data Protectorパッケージを再起動します。

   cmrunpkg pkg_name

   パッケージ切り替えおよびノード切り替えオプションが有効になっていることを確認します。

2. 仮想ホストを再度インポートします。

   omnicc -import_host *virtual_hostname* -virtual

3. IDB内のCell Managerの名前を変更します。

   omnidbutil -change_cell_name

4. インストールサーバーがCell Managerと同じパッケージにある場合は、以下のインストールサーバー 仮想ホスト名をインポートします。

   omnicc -import_is virtual_hostname

注記：

Cell Managerからのすべての要求は、クライアント上の/var/opt/omni/log/inet.log**ファイルに 記録されます。不要なログエントリーが書き込まれないようにするには、クライアントに保護を設定します。セルに保護を設定する方法については、「保護について」（223ページ）を参照してください。**

Microsoft Cluster Server上で構成されているCell Managerのアップグレード

Microsoft Cluster Server (MSCS)上のData Protector A.06.00、A.06.10、またはA.06.11 Cell ManagerをData Protector 6.20にアップグレードするには、Windows用インストールDVD-ROMからローカルに実行する必要があります。

注記：

すべてのクラスターノードにMSI 2.0をインストールすることを お勧めします。

前提条件

- アップグレードオプションがサポートされるのは、以前にインストールされたData Protectorソフトウェアがクラスター対応モードでインストールされたCell Managerである場合のみです。クラスター内のシステムにData Protectorソフトウェアがクラスター非対応でインストールされている場合、セットアップを開始する前にこのソフトウェアをアンインストールする必要があります。

アップグレード手順

アップグレードは、以下の手順で行ってください。

1. Windows用インストールDVD-ROMを挿入し、¥Windows_other¥i386¥setup.exeを実行します。現在アクティブ化されている仮想サーバーノードでセットアップを開始することをお勧めします。

   自動的に旧バージョンの製品が検出され、Data Protector 6.20にアップグレードするよう促すメッセージが表示されます。

   [Next]をクリックし、次に進みます。

2. Install済みのコンポーネントがData Protectorによって自動的に選択されます。

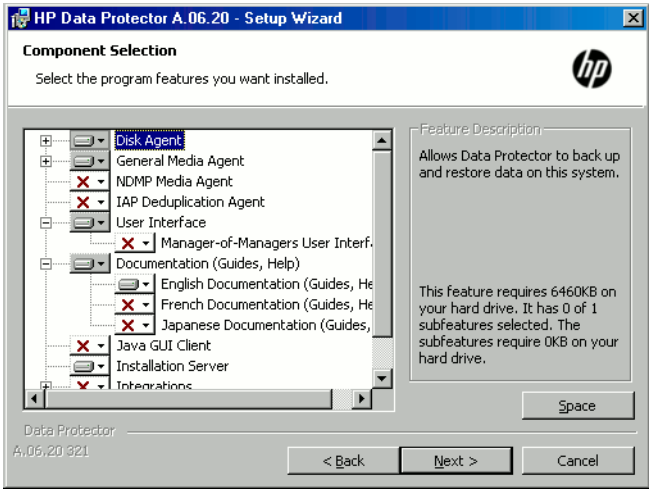


図 45 コンポーネントの選択

3. コンポーネント選択サマリーリストが表示されます。[Install]をクリックして、アップグレードを開始します。

アップグレード後には、すべてのノードに同じコンポーネントセットがインストールされます。

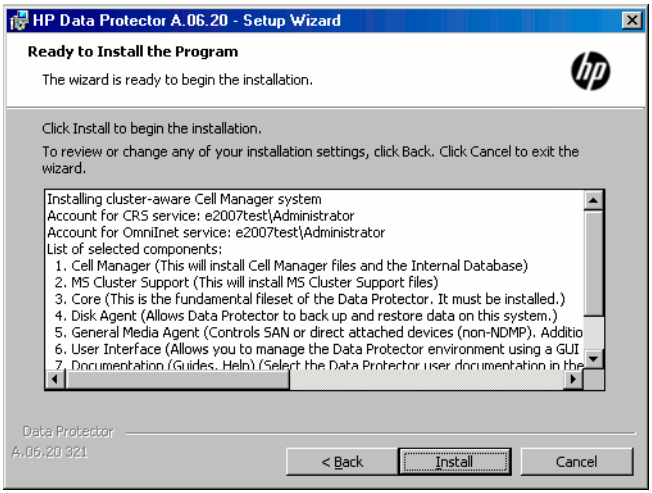


図 46 コンポーネント選択サマリーページ

4. [Installation status]ページが表示されます。[Next]をクリックします。

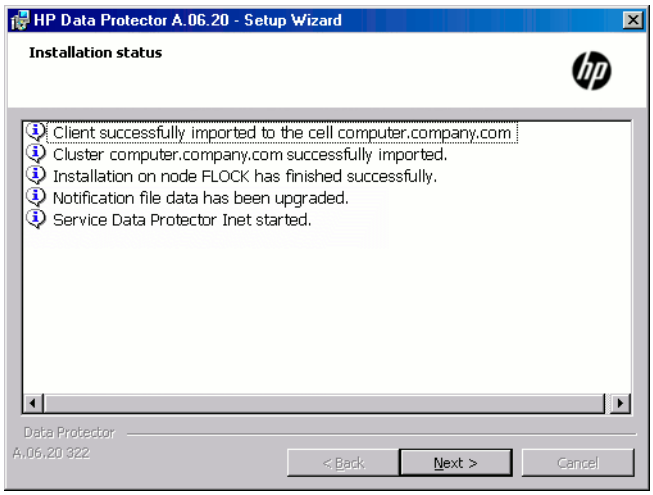


図 47 [Installation status]ページ

5. セットアップ後すぐにData Protectorを起動するには、[Start the Data Protector Manager GUI]を選択します。

   『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を表示するには、[Open the Product Announcements]を選択します。

   HP AutoPassユーティリティは、すべてのノードではなく1つのノードにのみインストールされるため、HP AutoPassユーティリティをMicrosoft Cluster Serverにインストールすることはお勧めしません。ただし、AutoPassをインストールする場合は、Data Protectorをシステムから削除するために、インストールされているノードと同じノードからData Protectorをアンインストールする必要があります。

   [Finish]をクリックします。

注記：

クラスター対応クライアントをアップグレードする場合は、まずすべてのクラスターノードを個別にアップグレードしてから、仮想サーバーを再度インポートします。リモートアップグレードはサポートされていません。

5 Data Protectorライセンス

この章の内容

この章は、次の項目で構成されています。

- Data Protectorライセンスチェック機能とレポート機能
- Data Protectorパスワードの取得とインストール
- Data Protectorの製品構成とライセンス

概要

Data Protector 6.20製品構成およびライセンスには、3つの主なカテゴリがあります。

1. スターターパック
2. ドライブとライブラリの使用権
3. 機能拡張

注記：

UNIX用の製品ライセンスは、どのプラットフォーム上でも使用でき、すべてのプラットフォームでその機能を提供します。一方、Windows用の製品ライセンスは、Windows、Linux、およびNetWareプラットフォーム上でしか使用できません。

パスワードはCell Managerに割り当てられ、Data Protectorセル全体に対して有効です。クライアントでは、ファイルシステムまたはディスクイメージバックアップのライセンスは不要です。

ライセンスチェック機能とレポート機能

Data Protectorライセンスは、さまざまなData Protectorオペレーション中にチェックされ、見つからない場合にはレポートされます。以下に例を示します。

- たとえば、Data Protectorのチェックおよび保守メカニズムの一環としてライセンスがチェックされ、ライセンスが見つからない場合は、Data Protectorイベントログに記録されます。Data Protectorイベントログは、Cell Manager上の Data_Protector_program_data¥log¥server¥Ob2EventLog.txt(Windows Server 2008の場合)、Data_Protector_home¥log¥server¥Ob2EventLog.txt(その他のWindowsシステムの場合)、/var/opt/omni/server/log/Ob2EventLog.txt(UNIXシステムの場合)に置かれています。Data Protectorチェックおよび保守機構の詳細については、オンラインヘルプの索引「イベントログ」を参照してください。
- ライセンスが見つからないというレポートがData Protectorイベントログに記録されている場合、Data Protectorのユーザーインタフェースの起動時に、イベントログの通知が表示されます。Data Protectorイベントログの詳細は、オンラインヘルプの索引「イベントログ」を参照してください。
- Data Protectorセッションの起動時には、ライセンスがチェックされ、もし見つからなかった場合はレポートされます。

Data Protectorライセンス では、以下のような特性がグループ化されます。

- Cell Manager関連ライセンス
- エンティティーベースのライセンス
- 容量ベースのライセンス

Cell Manager関連ライセンス

Data Protector Cell Managerには、以下の関連ライセンスがあります。

- スターターパック
- Manager-of-Managers使用権
- シングルサーバー版

Cell Manager (スターターパックに含まれる)やManager-of-Managers(MoM)などの一部のData Protectorコンポーネントがセル内に存在する場合は、必要とされる基本または特別ライセンスの存在のみがチェックされます。

エンティティーベースのライセンス

Data Protectorのエンティティーベースのライセンスは、以下のとおりです。

- 61-250スロットライブラリ使用権(1台)、および、スロット数無制限ライブラリ使用権(1台)
- SAN、すべてのプラットフォーム用追加ドライブ使用権、およびWindows、NetWare、Linux用追加ドライブ使用権
- UNIX用オンラインバックアップ使用権(システム1台)、およびWindows、Linux用オンラインバックアップ使用権(システム1台)
- Data Protectorクライアントシステム暗号化使用権(1台)
- 1台のデータベースサーバーのGranular Recovery extension

前述のいずれかのエンティティーベース使用権の対象となる製品がセル内で構成されている場合は、必要なエンティティーベース使用権の存在とその数がチェックされます。

Data Protectorでは、構成されているエンティティーベース項目の数とエンティティーベースのライセンスの数を比較します。ライセンスの数が構成されている項目の数より少ない場合は、通知が発生します。

前述の最初の2つのライセンスでは、以下の作業も必要です。

バックアップデバイスがSAN環境内の複数のData Protectorクライアントに対して構成されている場合は、Multipath機能を使って、Data Protectorで1台のバックアップデバイスとして認識されるようにする必要があります。

容量ベースのライセンス

Data Protectorの容量ベースのライセンスは、以下のとおりです。

- UNIXゼロダウンタイムバックアップ使用権(1TB、10TB)
- UNIXインスタントリカバリ使用権(1TB、10TB)
- Linuxゼロダウンタイムバックアップ使用権(1TB、10TB)
- Linuxインスタントリカバリ使用権(1TB、10TB)
- Windowsゼロダウンタイムバックアップ使用権(1TB、10TB)
- Windowsインスタントリカバリ使用権(1TB、10TB)
- NDMPダイレクトバックアップ使用権(1TB、10TB)
- アドバンストバックアップ使用権(1TB、10TB、100TB)

容量ベースのライセンス(アドバンストバックアップ使用権以外)のチェックでは、バックアップされる論理ユニット上の*合計*ディスク容量が、インストールされているライセンス数と比較されます。

ライセンスのチェックは、ライセンスを受けている容量を使い果たした場合でも、インスタントリカバリまたはバックアップの実施の妨げにならないよう行われます。容量がなくなると、バックアップセッション中に、ライセンスを受けた容量を越えたことを示す警告メッセージが表示されます。

使用されたディスクの容量は、各ZDBバックアップセッションから集めた履歴情報を基に計算されます。考慮される期間は24時間です。Data Protectorでは、過去24時間以内に発生したすべてのセッションで使用されたディスクを基に使用ディスク容量が計算され、算出された容量をライセンスを受けた容量と比較します。

ライセンス違反が起こると、バックアップ処理中に警告メッセージが表示されます。さらに、ライセンスレポートツールは毎日実行され、ライセンスを受けた容量を越えるとData Protectorイベントログに通知が書き込まれます。

使用容量の計算

使用される容量の計算では、過去24時間以内に使用されたディスクアレイごとに、ライセンスを受けている容量を算出します。指定した期間内に複数回使用されたディスクは、1回だけカウントされます。ディスクアレイユニットは、各アレイに使用されている識別番号によって識別されます。アレイの識別番号を使用すると、既にカウント済みのアレイの認識が可能です。

インスタントリカバリが含まれたZDBバックアップを実行している場合は、ZDBに使用された各ディスクアレイの容量に加え、インスタントリカバリに使用された各ディスクアレイの容量が、元の単位の総容量の計算対象になります。

たとえば、2台のP6000 EVA ディスクアレイがあるとします。1台のアレイには、データ保護のために使用される200GBの容量のディスク(App.1)が1台あります。インスタントリカバリオプションは、1日に3回起動される各バックアップセッションに含まれています。一度に3つのスナップショットが保存され、インスタントリカバリ用にローテーションされます。もう1台のディスクアレイには、150GBと120GBの容量の2台のディスク(App.2とApp.3)があります。ディスクApp.2では1日に1回バックアップが実行され、データがテープに移動された後、スナップショットは削除されます。App.3では、1日に3回バックアップが実行され、インスタントリカバリ用に5つのスナップショットがローテーションされます。詳細は、図48(313ページ)を参照してください。

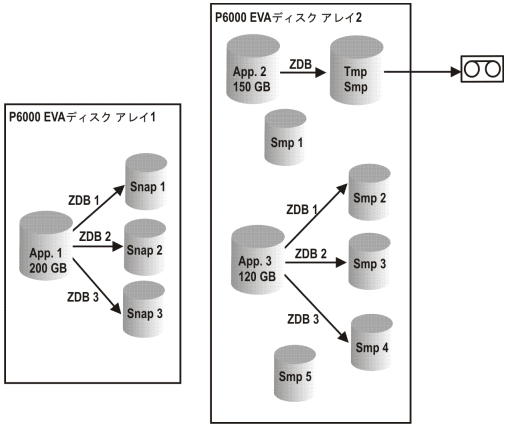


図 48 使用容量の計算シナリオ

過去24時間のバックアップセッションで使用されたすべてのディスクをZDB使用容量として計算すると、200GB (App.1) + 150GB (App.2) + 120GB (App.3) = 470GB。

インスタントリカバリ使用容量の計算では、インスタントリカバリ用にデータを残したZDBセッションのソース容量を計算します。同じディスクは1度しか計算されず、200 GB (App.1)+ 120GB (App.3) = 320GB。

アドバンストバックアップ使用権

Data Protectorファイルライブラリにバックアップするには、アドバンストバックアップ使用権(LTU)が必要です。仮想テープライブラリ(VTL)には、ドライブおよびライブラリライセンスの代わりに、このアドバンストバックアップ使用権を使用できます。このライセンスは、バックアップディスクストレージで利用可能なネイティブ容量(TB)ごとに必要です。

- Data Protectorファイルライブラリの使用可能なネイティブ容量は、そのファイルライブラリで使用されるすべてのファイルのディスクのサイズです。このサイズは、ファイルシステムにより報告されます。
  - 合成フルまたは仮想フルバックアップに統合される仮想フルバックアップおよび増分バックアップは、このライセンスを必要とするData Protectorファイルライブラリに保存する必要があります。
- Data ProtectorでVTLのみを使用している場合は、VTLの物理容量と同量のライセンスが必要です。これは使用可能なネイティブ容量とも呼ばれます。
- 「VTLの使用可能なネイティブ容量は、Data Protector内部データベースに従って保護バックアップや保護バックアップのコピーおよびミラーが格納されるスペースです。
  - VTLごとに、ディスクにバックアップを取るライセンスモデルにするのか、テープドライブにバックアップを取るライセンスモデルにするのかを選択できます。1つのVTLで、この両方の方法を合わせて使用することはできません。

- バックアップデータをディスクキャッシュから別のディスクまたはテープに移行するための組み込み容量がVTLにある場合は、移行されるストレージ容量を完全にライセンスする必要があります。VTLにより排他的に制御されるテープライブラリにはドライブおよびライブラリライセンスは必要ありませんが、***物理テープライブラリのすべてのテープで使用される容量はライセンスする必要があります。***ただし、バックアップデータを別のディスクまたはテープに移行するためにData Protectorのオブジェクトコピー機能が使用されている場合は、この方法は使用できません。
- デフォルトでは、Data Protectorは、VTLデバイスを通常のライブラリ(SCSI IIライブラリなど)として扱います。SCSIライブラリ、外部制御、ADIC/GRAU DASライブラリ、およびStorageTek ACSライブラリには、容量ベースのライセンス(アドバンストバックアップ使用権)を使用できます。アドバンストバックアップ使用権を利用するには、デバイスの構成時にデバイスにVTLのマークを付ける必要があります。VTLをコマンドラインインタフェース(CLI)を使用して構成する方法は、後述の例(314ページ)を参照してください。VTLをグラフィックユーザーインタフェース(GUI)を使用して構成する方法は、オンラインヘルプの索引「仮想テープライブラリ」を参照してください。

- Manager-of-Managers (MoM)でライセンスを集中管理している場合は、ディスクへのアドバンストバックアップ機能を使用して、最低でも1TBを各セルに割り当てる必要があります。

注記:

Data Protectorは、最新の仮想テープライブラリおよび' ファイルライブラリをホストしている一部のファイルサーバーの装備およびインタフェースが欠けているために、必要なライセンスの容量をレポートできません。ライセンス定義と一致するようにライセンスを容量に割り当てるのは、ユーザーの責任です。

例

omniuploadコマンドを使用してコマンドラインインタフェース(CLI)で「VTL_2010」という名前の仮想テープライブラリを構成する場合は、構成ファイルのVTLCAPACITY文字列に対してライブラリ容量の推定消費量を指定する必要があります。この推定値は、結果的にライセンスチェッカーレポートのアドバンストバックアップ使用権に使用される容量に追加されます。

注記:

推定仮想ライブラリ容量消費量の値(VTLCAPACITY)は、「指定したVTL容量は無効です」というエラーメッセージを避けるために、テラバイト(TB)単位で整数で指定する必要があります。

「C:¥Temp」ディレクトリにある「libVTL.txt」という名前の構成ファイル内で、ライブラリ容量の推定消費量として、たとえば11と入力し、次のコマンドを実行します。

omniupload -create_library VTL_2010 -file C:¥Temp¥libVTL.txt

構成を確認するには、次のコマンドを実行します。

omnidownload -library VTL_2010

```
#omnidownload -library VTL_2010 NAME "VTL2010"
DESCRIPTION "" HOST computer.company.com POLICY SCSI-II TYPE DDS LIBVIRTUAL
VTLCAPACITY 11 IOCTLSERIAL "" CONTROL "SCSI address" REPOSITORY "SCSI
repository" MGMTCONSOLEURL ""
```

ライセンス確認では、使用されているライセンス容量がレポートされます。これは、ファイルライブラリ(FL)に使用されているディスク上のスペースで、仮想テープライブラリ上のディスクスペースの推定サイズです。たとえば、バックアップによりFLで2TBのディスクスペースを使用していて、VTL上に10TBのディスク容量を使用しているものとします。使用中の合計容量は12TBです。5TBのライセンス容量しかインストールされていない場合には、アドバンストバックアップ使用権(1TB)がさらに7つ必要であるという通知が表示されます。

```
#omnicc -check_licenses -detail
-----------------------------------------------------------------
ライセンスカテゴリ                    :アドバンストバックアップ使用権(1TB)
インストールされたライセンス容量      :5TB 使用されているライセンス容量
 :12.0TB 必要な追加のライセンス容量:7TB

サマリー -------- 説明                                          必要なライセンス
アドバンストバックアップ使用権(1TB)                                    7
```

容量ベースのライセンスの例

ここでは、容量ベースのライセンスの計算方法の例を示します。

例1

図49およびでは、800GBの論理ユニット1つからのデータが、ディスクへのZDB(ZDB-to-Disk)セッションで1日に3度バックアップされる状況が例として示されています。

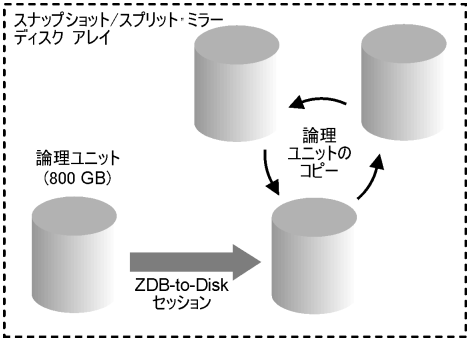


図 49 ディスクへのZDBセッション

インスタントリカバリに備えて、3つのスプリットミラーコピーまたはスナップショットコピー(複製)がローテーションおよび保管されます。この場合、容量ベースのライセンスは、以下のように計算します。

800GBの論理ユニット1つを使用するディスクへのZDB (ZDB-to-Disk)セッション:

1 x 800GB = 0.8TB用として「ゼロダウンタイムバックアップ使用権(1 TB)」ライセンス

インスタントリカバリに備えて、同じ800GBの論理ユニットの3つの複製が保管されます。なお、ライセンスの対象となるのは、複製の容量ではなく、ソースボリュームの容量です。

1 x 800GB = 0.8TB用として「インスタントリカバリ使用権(1TB)」ライセンス

「ゼロダウンタイムバックアップ使用権(1TB)」ライセンスが1つ、および「インスタントリカバリ使用権(1TB)」ライセンスが1つ必要です。

例2

図50 (317ページ)では、800GBの論理ユニット1つからのデータが、テープへのZDB (ZDB-to-Tape)セッションで1日に2度バックアップされる状況が例として示されています。したがって、インスタントリカバリ用のスプリットミラーコピーまたはスナップショットコピー(複製)は保管されません。この場合、容量ベースのライセンスは、以下のように計算します。

800GBの論理ユニット1つを使用するディスクへのZDB (ZDB-to-Disk)セッション:

1 x 800GB = 0.8TB用として「ゼロダウンタイムバックアップ使用権(1TB)」ライセンス

この場合は、「ゼロダウンタイムバックアップ使用権(1TB)」ライセンスが1つ必要です。

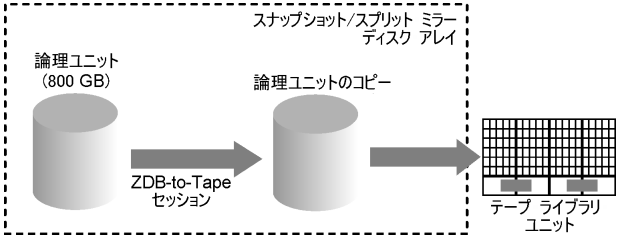


図 50 テープへのZDBセッション

例3

図51 (318ページ) では、800GBの論理ユニット1つからのデータが、ディスク/テープへのZDB (ZDB-to-Disk+Tape)セッションで1日に3度バックアップされる状況が例として示されています。インスタントリカバリに備えて、5つのスプリットミラーコピーまたはスナップショットコピー(複製)がローテーションおよび保管されます。この場合、容量ベースのライセンスは、以下のように計算します。

ディスク/テープへのZDB (ZDB-to-Disk+Tape)セッションに800GBの論理ユニットを1つ使用するため、以下のライセンスが必要です。

1 x 800GB = 0.8TB用として「ゼロダウンタイムバックアップ使用権(1TB)」ライセンス

インスタントリカバリに備えて、同じ800GBの論理ユニットの5つの複製が保管されます。なお、ライセンスの対象となるのは、複製の容量ではなく、ソースボリュームの容量です。

1 x 800GB = 0.8TB用として「インスタントリカバリ使用権(1TB)」ライセンス

この場合は、「ゼロダウンタイムバックアップ使用権(1TB)」ライセンスが1つ、および「インスタントリカバリ使用権(1 TB)」ライセンスが1つ必要です。

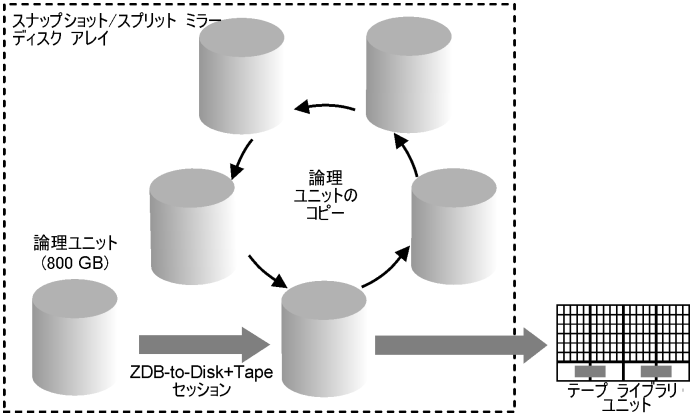


図 51 ディスク+テープへのZDBセッション

例4

ZDBセッションで、200GBの論理ユニットが1つ、500GBの論理ユニットが1つ、120 GBの論理ユニットが1つ、および300GBの論理ユニットが1つ使用されるため、以下のライセンスが必要です。

1 x 200GB + 1 x 500GB + 1 x 120GB + 1 x 300GB = 1.12TB用として「ゼロダウンタイムバックアップ使用権(1TB)」ライセンス

200GBの論理ユニット1つ、120GBの論理ユニット1つ、300GBの論理ユニット1つのスプリットミラーまたはスナップショットコピーが、インスタントリカバリの目的で保存されます。

1 x 200GB+ 1 x120GB + 1 x 300GB = 0.62TB用として「インスタントリカバリ使用権(1 TB)」ライセンス

図49(316ページ)から図51(318ページ)までの3つの例すべてがセル内で構成されている場合は、「ゼロダウンタイムバックアップ使用権(1TB)」ライセンス1つ、およびで十分です。

必要に応じたライセンスレポートの作成

セルからの関連情報のライセンスについてレポートを生成するには、以下を実行します。

```
omnicc -check_licenses [-detail]
```

-detailオプションが指定されなかった場合は、Data Protectorライセンスが存在するかどうかを示す情報が返されます。以下の情報が返されます。レポートが生成された時刻、ライセンスモード、およびライセンスサーバーの情報が返されます。

-detailオプションを指定すると、詳細なレポートが作成されます。ライセンス確認処理から、セルの各ライセンスについて、ライセンス名、インストールされているライセンス、使用されているライセンス、および必要な追加ライセンス(容量)の情報が返されます。

ドライブ使用権LTUの場合、ライセンス確認では構成されたドライブと推奨された追加ライセンスに関する情報が返されます。いずれかの時点で使用するドライブの台数と同じ数のライセンスが必要です。これは、すべてのドライブを同時に使用できるようにするため、通常は構成されたドライブの総数になります。

なお、ライセンスの有効期限は表示されません。環境とインストールされているライセンスによっては、レポートの作成に若干時間がかかることがあります。ライセンスの有効期限に関する情報を取得するには、次のコマンドを実行します。

```
omnicc -password_info
```

重要:

CMMDBが構成されたMoM環境で、ライブラリとドライブのライセンスの対象となる製品のライセンスレポートを作成する場合は、CMMDBがインストールされたCell Managerで、omniccコマンドを実行する必要があります。

詳細は、omniccのマンページまたは『*HP Data Protector Command Line Interface Reference*』を参照してください。

Data Protector 6.20以前のライセンスのチェックとレポート

Data Protector 6.20のライセンス確認では、特定のライセンスが以前のData Protectorリリースから新しいData Protector製品構造にマッピングされ、新しいライセンスとしてレポートされます。ライセンスの適用時に制限事項が発生する場合があります。詳細は、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』の制限事項を参照してください。

この章は、次の項目で構成されています。

- 「マルチドライブサーバー使用権のレポート」(319ページ)
- 「以前のオンラインライセンスのレポート」(322ページ)
- 「NDMPダイレクトバックアップ使用権のレポート」(323ページ)
- 「スロットライブラリ使用権のレポート」(324ページ)
- 「以前のZDBおよびIRのライセンスのレポート」(324ページ)

マルチドライブサーバー使用権のレポート

UNIX用マルチドライブサーバー使用権は、6つのSAN、すべてのプラットフォーム用追加ドライブ使用権としてレポートされます。

マルチドライブ使用権は、GUIでクライアントを選択する際に[**詳細設定**]タブ以下の[**クライアント**]コンテキストで[**クライアントをデバイスサーバーとして設定する**]オプションを設

定した場合に、デバイスサーバーのみで使用されます。このオプションが設定されていない場合は、マルチドライブ使用権はインストールされていても使用されません。

InstallされているSAN、すべてのプラットフォーム用追加ドライブ使用権の数は、6つ単位で増加します。たとえば、UNIX用マルチドライブサーバー使用権1ライセンスとSAN、すべてのプラットフォーム用追加ドライブ使用権1ライセンスがデバイスサーバーにインストールされているとします。ライセンス確認では、SAN、すべてのプラットフォーム用追加ドライブ使用権が7ライセンス(1シングルドライブ、および1マルチドライブから6つ)インストールされていることが示されます。

システム上に10台のドライブが構成されている場合、ライセンス確認では、すべてのドライブを同時に使用するために、SAN、すべてのプラットフォーム用追加ドライブ使用権3ライセンスの追加が推奨されることがレポートされます。

```
#omnicc -check_licenses -detail ライセンスカテゴリ
:インストールされているSAN、すべてのプラットフォーム用追加ドライブ使用権        :7
構成されているドライブ          :10 推奨する追加ライセンス: 3

サマリー 説明                              推奨する追加のドライブライセンス
SAN、すべてのプラットフォーム用追加ドライブ使用権                                3

警告:いかなるときも、操作(フォーマット、バックアップ、復元、メディアとオブジェクトのコピー、メディアとオブジェクトの検証、オブジェクトのミラーリング、スキャン、ディザスタリカバリなど)に使用しているドライブと同数のライセンスが必要になります。すべてのドライブを同時に使用できるようにするには、構成されているドライブと同数のライセンスが必要です。

ライセンスがカバーされています。
```

Windowsシステムのライセンスについても同様です。Windows/NetWare用マルチドライブサーバー使用権もライセンス確認のレポートから削除され、Windows、NetWare、Linux用追加ドライブ使用権4ライセンス分としてレポートされます。Windows、NetWare、Linux用追加ドライブ使用権の数は、4つ単位で増加します。10台のドライブが構成されている環境で、マルチドライブ使用権1ライセンスとシングルドライブ使用権1ライセンスがインストールされている場合、ライセンス確認では、すべてのドライブを同時に使用するために、Windows、NetWare、Linux用追加ドライブ使用権5ライセンス(10必要で、うち5つは1マルチドライブからの4つと1シングルドライブからの1つでカバー済み)の追加が推奨されることがレポートされます。

```
#omnicc -check_licenses -detail
ライセンスカテゴリ          :Windows、NetWare、Linux用追加ドライブ使用権
インストールされたライセンス        :5 構成されているドライブ          :10
推奨する追加ライセンス: 5
```

```
サマリー 説明                                推奨する追加のドライブライセンス
SAN、すべてのプラットフォーム用追加ドライブ使用権                                5

警告:いかなるときも、操作(フォーマット、バックアップ、復元、メディアとオブジェクトの
コピー、メディアとオブジェクトの検証、オブジェクトのミラーリング、スキャン、ディザス
タリカバリなど)に使用しているドライブと同数のライセンスが必要になります。すべてのドラ
イブを同時に使用できるようにするには、構成されているドライブと同数のライセンスが必要
です。

ライセンスがカバーされています。
```

また、以前の組み合わせライセンスとして、UNIX用Cell Managerおよびマルチドライブサーバーと、Windows/NetWare用Cell Managerおよびマルチドライブサーバーがあります。

UNIX用Cell Managerおよびマルチドライブサーバー使用権1ライセンスがインストールされている場合、omniccコマンドでは、すべてのプラットフォーム用Cell Manager使用権1ライセンスと、UNIX用マルチドライブサーバー使用権1ライセンスがインストールされていることがレポートされます。

```
#omnicc ライセンスモード      :ローカルライセンスサーバー      :computer.company.com

カテゴリ                          ライセンスの数 すべてのプラットフォーム用Cell
Manager                                   1 Windows/Linux用Cell
Manager                                 0
SAN、すべてのプラットフォーム用追加ドライブ                          0
Windows、NetWare、Linux用追加ドライブ                    0
UNIX用マルチドライブサーバー                                    1
Windows/NetWare用マルチドライブサーバー                          0
```

この組み合わせの使用権は、UNIX用Cell Managerおよびシングルドライブサーバー1ライセンス、およびSAN、すべてのプラットフォーム用追加ドライブ使用権5ライセンス分としてレポートされます。つまり、ライセンス確認では、すべてのプラットフォーム用Cell Manager使用権1ライセンスと、SAN、すべてのプラットフォーム用追加ドライブ使用権6ライセンスがレポートされます。

システム上に10台のドライブが構成されていて、UNIX用Cell Managerおよびマルチドライブサーバー使用権1ライセンスがインストールされている場合、ライセンス確認では、すべてのドライブを同時に使用するために、SAN、すべてのプラットフォーム用追加ドライブ使用権4ライセンス(10必要で、うち6つはマルチドライブ使用権でカバー済み)の追加が推奨されることがレポートされます。

```
#omnicc -check_licenses -detail
ライセンスカテゴリ          :インストールされているすべてのプラットフォーム用Cell
```

```
Manager使用権              :1 使用されているライセンス                    :1
必要な追加ライセンス                    : 0

ライセンスカテゴリ:インストールされているWindows、NetWare、Linux用追加ドライブ使用権
        :6 構成されているドライブ          :10 推奨する追加のライセンス: 4

サマリー 説明                              推奨する追加のライセンス
SAN、すべてのプラットフォーム用ドライブ使用権                                  4

警告:いかなるときも、操作(フォーマット、バックアップ、復元、メディアとオブジェクトの
コピー、メディアとオブジェクトの検証、オブジェクトのミラーリング、スキャン、ディザス
タリカバリなど)に使用しているドライブと同数のライセンスが必要になります。すべてのドラ
イブを同時に使用できるようにするには、構成されているドライブと同数のライセンスが必要
です。

ライセンスがカバーされています。
```

Windowsシステムの組み合わせライセンスについても同様です。Windows/NetWare用Cell Managerおよびマルチドライブサーバー使用権は、Windows用Cell Manager およびシングルドライブサーバー使用権1ライセンスと、Windows、NetWare、Linux用追加ドライブ使用権4ライセンス分としてレポートされます。ライセンス確認では、Windows/Linux用Cell Manager使用権1ライセンスと、Windows、NetWare、Linux用追加ドライブ使用権5ライセンスがインストールされていることがレポートされます。

ライセンス確認では足りないライセンスの数がレポートされますが、バックアップ中、インストールされているライセンスのチェックは変更されません。ドライブサーバーにインストールされたマルチドライブ使用権では、構成済みドライブの数は無制限に同時に使用することは可能です。しかし、構成済みドライブサーバーがないにも関わらずマルチドライブ使用権がインストールされている場合は、ライセンス確認で十分なシングルドライブ使用権がインストールされているとレポートされていても、バックアップができない場合があります。

以前のオンラインライセンスのレポート

UNIX用オンラインバックアップ使用権およびWindows/Linux用オンラインバックアップ使用権は、セル内のすべてのクライアントに有効です。以前のData Protectorリリースのオンラインバックアップ使用権は、インストールされている現在のライセンスの数が1ずつ増加します。

ライセンス確認では、セル内のシステムが多数ある場合に、追加のオンラインバックアップ使用権が必要であるとレポートされる場合があります。たとえば、セル内にオンラインバックアップを使用する5つのWindowsシステムがあり、Windows用オンラインバックアップ使用権1ライセンスがインストールされているものとします。インストールされているライセンスでは1つのシステムがカバーされるため、他の4つのシステム用に、4ライセンスの追加

が必要となります。ライセンス確認では、Windows/Linux用オンラインバックアップ使用権(システム1台)4ライセンスが必要であることがレポートされます。

```
#omnicc -check_licenses -detail
ライセンスカテゴリ
:インストールされているWindows/Linux用オンラインバックアップ使用権(システム1台)1
使用されているライセンス                    :5 必要な追加ライセンス: 4

サマリー 説明                                          必要なライセンス
Windows/Linux用オンラインバックアップ使用権(システム1台)                    4

ライセンスがカバーされていません。
```

さらに3つのWindows/Linux用オンラインバックアップ使用権(システム1台)がインストールされている場合は、Windows/Linux用オンラインバックアップ使用権(システム1台)がもう1ライセンス(5つ必要で、うち4つは以前のもの1つとシステム1台用3つでカバー済み)必要であるという通知が表示されます。

```
#omnicc -check_licenses -detail
ライセンスカテゴリ
:インストールされているWindows/Linux用オンラインバックアップ使用権(システム1台)4
使用されているライセンス                    :5 必要な追加ライセンス: 1

サマリー 説明                                          必要なライセンス
Windows/Linux用オンラインバックアップ使用権(システム1台)                    1

ライセンスがカバーされていません。
```

NDMPダイレクトバックアップ使用権のレポート

NDMPサーバー使用権(1台)は、NDMPダイレクトバックアップ使用権(1TB)1ライセンス分としてレポートされます。1つ目はエンティティーベースのライセンスで、つまり、1つのNDMPサーバーごとに1つのライセンスが必要になります。一方、NDMPダイレクトバックアップ使用権(1TB)は容量ベースのライセンスで、1つのNDMPサーバーで1 TBのバックアップをするために必要となります。

InstallされているNDMPダイレクトバックアップ使用権(1TB)のライセンス容量は、インストールされているNDMPサーバー使用権(1台)の数ごとに増加します。たとえば、NDMPダイレクトバックアップ使用権(1TB) 1ライセンスと、NDMPダイレクトバックアップ使用権(1TB) 1ライセンスがインストールされている場合は、インストールされているライセンス容量は合計で2 TBとなります。結果として、ライセンス確認で追加のライセンスが必要であるとレポートされる場合があります。たとえば、NDMPを使用して5 TBのバックアップを行う際に、NDMPサーバー使用権(1台) 1ライセンスと1つのNDMPダイレクトバックアップ使用権(1TB) 1ライセンスがインストールされているものとします。ライセンス確認では、NDMPダイレクト

バックアップ使用権(1TB) 3ライセンス(5つ必要、2つは以前の1つと新しいライセンス1つでカバー済み)が必要であるとレポートされます。

```
#omnicc -check_licenses -detail
ライセンスカテゴリ
:インストールされているNDMPダイレクトバックアップ使用権(1TB)ライセンス容量      :2TB
使用されているライセンス容量          :5.0TB 必要な追加のライセンス容量:3TB

サマリー 説明                                          必要なライセンス
NDMPダイレクトバックアップ使用権(1TB)                                  3
```

スロットライブラリ使用権のレポート

プラットフォーム固有のライブラリ使用権(1つはWindowsシステム用、1つはUNIXシステム用)は、プラットフォームに依存しないライセンスとしてレポートされます。

Installされている61-250スロットライブラリ使用権(1台)の数は、インストールされているプラットフォーム固有の61-250スロットライブラリ使用権の数ごとに増加します。また、プラットフォーム固有の無制限ライセンスがインストールされているスロット数無制限ライブラリ使用権(1台)の数に追加されます。

UNIX用スロット数無制限ライブラリ使用権1ライセンスとWindows用スロット数無制限ライブラリ使用権1ライセンスがインストールされている場合、ライセンス確認では、スロット数無制限ライブラリ使用権(1台) 2ライセンス分がインストールされていることがレポートされます。

```
#omnicc -check_licenses -detail
ライセンスカテゴリ
:インストールされている61-250スロットライブラリ使用権(1台)      :2
使用されているライセンス                    :0 必要な追加ライセンス:0
ライセンスカテゴリ
:インストールされているスロット数無制限ライブラリ使用権(1台)      :2
使用されているライセンス                    :0 必要な追加ライセンス: 0
```

プラットフォームに依存しないスロットライブラリ使用権により、ライセンスの履行はライセンスのチェックよりも強力になります。バックアップ中に、Data Protectorは異なるプラットフォームのライセンスをチェックします。ライセンス確認で十分かつ適切なライセンスがシステムにインストールされているとレポートされていても、特定のプラットフォームでライセンスが足りないためにバックアップが実行できない場合があります。

以前のZDBおよびIRのライセンスのレポート

- ゼロダウンタイムバックアップ使用権(1TB)(B7025CA)は、以前のData Protectorリリースのディスクアレイ固有のゼロダウンタイムバックアップ使用権を置き換えます。

- HP StorageWorks Modular SAN Array 1000用ZDB使用権(1TB)(HP StorageWorks Modular SAN Array 1000用ゼロダウンタイムバックアップ使用権(1TB)(B7036AA))
- HP StorageWorks P6000 EVAディスクアレイファミリ用ZDB使用権(1TB)(汎用ゼロダウンタイムバックアップ使用権(1TB) (B7025CA))
- HP StorageWorks P9000 XPディスクアレイファミリ用ZDB使用権(1TB)(HP StorageWorks XP用ゼロダウンタイムバックアップ使用権(1TB)(B7023CA))
- EMC Symmetrix/DMX用ZDB使用権(1TB)(EMC Symmetrix/DMX用ゼロダウンタイムバックアップ使用権(1TB) (B6959CA))

すべてのディスクアレイ固有のライセンスは、ライセンスチェッカーによって、汎用ゼロダウンタイムバックアップ使用権(1TB)(B7025CA) 1ライセンス分としてレポートされます。インストールされている汎用ライセンスの容量は、すべての特定のアレイの種類のライセンスごとに増加します。使用中のライセンス容量は、すべてのアレイ上で使用されているデータの合計です。たとえば、各ディスクアレイに固有のライセンスカテゴリが1つずつ、合計4つのZDBライセンスがインストールされていて、EMC Symmetrixに2TB、P9000 XPアレイに2TB、P6000 EVAアレイに6TBのバックアップを行うものとします。この場合、10ライセンスが必要となりますが、4ライセンスしかないため、ライセンス確認では、ゼロダウンタイムバックアップ使用権(1 TB) 6ライセンス(10必要で、4つインストール済み)の追加が必要であるとレポートされます。

```
#omnicc -check_licenses -detail
------------------------------------------------------------
ライセンスカテゴリ                    :ゼロダウンタイムバックアップ使用権(1TB)
インストールされたライセンス容量      :4TB 使用されているライセンス容量
:10.0TB 必要な追加のライセンス容量:6TB

サマリー ------- 説明
 必要なライセンス ゼロダウンタイムバックアップ使用権(1
TB)                                    6

ライセンスがカバーされていません。
```

以前のEMC SymmetrixおよびP9000 XPアレイ用の無制限ZDBライセンスは、以下のようにレポートされます。

- EMC Split Mirror使用権(B6959AA)は、EMC Symmetrix/DMX用ゼロダウンタイムバックアップ使用権(1TB)(B6959CA) 3ライセンス分としてレポートされます。
- HP XP Split Mirror使用権(B7023AA)は、HP StorageWorks XP用ゼロダウンタイムバックアップ使用権(1TB)(B7023CA) 3ライセンス分としてレポートされます。
- EMC Symmetrix用ゼロダウンタイムバックアップ使用権(1台)(B6959BA)は、EMC Symmetrix/DMX用ゼロダウンタイムバックアップ使用権(1TB)(B6959CA) 3ライセンス分としてレポートされます。

- HP StorageWorks XP用ゼロダウンタイムバックアップ使用権(1台)(B7023BA)は、HP StorageWorks XP用ゼロダウンタイムバックアップ使用権(1TB)(B7023CA) 3ライセンス分としてレポートされます。

これは、以前のEMC SymmetrixおよびP9000 XPアレイ用のライセンスも同様に、ゼロダウンタイムバックアップ使用権(1TB)3ライセンス分としてレポートされることを意味します。

たとえば、システム上に各ライセンスカテゴリから1つのZDBライセンスがインストールされていて、ライセンス確認でゼロダウンタイムバックアップ使用権(1TB)が16(1+1+1+1+3+3+3+3)ライセンス分インストールされているものとします。

- インスタントリカバリ使用権(1TB)(B7028AA)は、以前のData Protectorリリースのディスクアレイ固有のインスタントリカバリ使用権を置き換えます。
  - HP StorageWorks Modular SAN Array 1000用IR使用権(1TB)(HP StorageWorks Modular SAN Array 1000用インスタントリカバリ使用権(1TB)(B7037AA))
  - HP StorageWorks P6000 EVAディスクアレイファミリ用IR使用権(1TB)(汎用インスタントリカバリ使用権(1TB) (B7028AA))
  - HP StorageWorks P9000 XPディスクアレイファミリ用IR使用権(1TB)(HP StorageWorks XP用インスタントリカバリ使用権(1TB)(B7026CA))

  すべてのディスクアレイ固有のライセンスは、ライセンスチェッカーによって、汎用インスタントリカバリ使用権(1TB) 1ライセンス分としてレポートされます。インストールされている汎用ライセンスの容量は、すべてのディスクアレイ固有のライセンスごとに増加します。ライセンス容量は、すべてのアレイ上で使用されているデータの合計です。

```
#omnicc -check_licenses -detail
-------------------------------------------------------
ライセンスカテゴリ
:インストールされているインスタントリカバリ使用権(1TB)      :3TB
使用されているライセンス容量          :5.0TB 必要な追加のライセンス容量:2TB

サマリー ------- 説明
必要なライセンス
インスタントリカバリ使用権(1TB)                                    2

ライセンスがカバーされていません。
```

ライセンスの履行はライセンスのチェックよりも強力になります。ZDBバックアップ中は、ライセンス確認で十分な数のZDBおよびIR使用権がレポートされていても、特定のストレージアレイのライセンスが足りないためにバックアップが実行できない場合があります。

Data Protectorパスワード

Data Protector製品のインストール後は、60日間製品を利用できます。この期間が過ぎると、Cell Managerに恒久パスワードをインストールしてソフトウェアを有効にする必要があります。恒久パスワードがなくてもData Protector Cell Managerでソフトウェアを起動することはできますが、特定のData Protector機能に必要なライセンスにはパスワードが必要なため、構成作業を行うことはできません。

Data Protectorのライセンスには、以下のパスワードのいずれか1つが必要です。

- 一時パスワード

  一時パスワードは、インストール時に製品に組み込まれています。インストール後は、Data Protectorによってサポートされている任意のシステム上で、60日間ソフトウェアを使用できます。この期間内に*HP Password Delivery Center (PDC)*に恒久パスワードを請求し、インストールする必要があります。

- 恒久パスワード

  Data Protector製品は、購入者が恒久パスワードを取得する権利を与える*権利保証書 (Entitlement Certificate)*とともに出荷されます。必要なライセンスをすべて購入した場合、恒久パスワードを使用して、ユーザーのバックアップ方針に合ったData Protectorセルを構成できます。恒久パスワードを請求する前に、Cell Managerシステムを決定し、セル構成条件を理解しておくことが重要です。

- 緊急用パスワード

  緊急事態が発生して、インストールされているパスワードが現行のシステム構成と一致しなくなった場合に、緊急用または予備パスワードを使用することができます。これらのパスワードを使用すると、任意のシステムを120日間操作できます。

  緊急用パスワードは、サポートサービスによって発行されます。緊急用パスワードは、HPサポート担当者によって請求され、HPサポート担当者に対して発行されます。サポートに問い合わせるか、HPのライセンスサイト(http://webware.hp.com)を参照してください。

  緊急用パスワードの目的は、元のシステムを再構成する間、または新しい恒久的なインストール先に移るまでの間、バックアップ操作を可能にすることです。ライセンスを移動する場合は、License Move Formに必要事項を入力し、*HP Password Delivery Center (PDC)*に送るか、パスワードの生成や移動が可能なWebサイト(http://webware.hp.com)を利用します。

パスワードの入手には、HP AutoPassユーティリティを使用することをお勧めします。このユーティリティは、Cell Managerのインストール処理中にインストールできます。Cell Managerのインストール処理中にHP AutoPassユーティリティをインストールし、インストール後にこのユーティリティを使用してパスワードを取得する手順は、「HP AutoPassユーティリティを使用した恒久パスワードの取得とインストール」(328ページ)を参照してください。

HP AutoPassユーティリティ以外の方法でパスワードを取得してインストールする手順は、「恒久パスワードの取得とインストールのためのその他の方法」(330ページ)を参照してください。

HP AutoPassユーティリティを使用した恒久パスワードの取得とインストール

HP AutoPassユーティリティを使用すると、HP製品の購入済みライセンスのパスワードをインターネット経由で直接HPのPassword Delivery Center Webサーバーからインストールできます。HP AutoPassユーティリティの詳細は、HP AutoPassのオンラインヘルプを参照してください。

前提条件

HP AutoPassユーティリティを使用して恒久パスワードの取得とインストールを行うには、以下の条件を満たす必要があります。

- Cell ManagerでHP AutoPassユーティリティをインストールします。Data Protectorをインストールする前にこのユーティリティをシステムにインストールしなかった場合は、omnisetup. shスクリプト(UNIXシステム)を使用するか、Cell Managerのインストール中にインストール(Windowsシステム)することができます。
- Java Runtime Environment (JRE) 1.5.0_06または最新の更新をCell Managerにインストールします。
- MC/ServiceGuardでは、HP AutoPassユーティリティをすべてのノードにインストールする必要があります。
- 恒久ライセンス権利証書が必要です。
- 購入済みライセンスのHP注文番号が必要です。
- Cell ManagerまたはManager-of-ManagersのIPアドレスが必要です。
- AutoPassをHP-UX 11.23 (Itanium)にインストールするには、以下のパッチをインストールしてください。
  - PHSS_36343 1.0 aC++ Runtime (IA:A.06.15, PA:A.0376)
  - PHSS_37039 1.0 Integrity Unwind Library

制限事項

HP AutoPassには、以下の制限事項があります。

- Windows 2003 x64、Windows Vista x64、Windows Server 2008 x64、Linuxの各オペレーティングシステムでは、HP AutoPassユーティリティはインストールされません。

- HP AutoPassは、すべてのノードではなく1つのノードにのみインストールされるため、HP AutoPassユーティリティをMicrosoft Clusterにインストールすることはお勧めしません。
- omniinstlicコマンドは、JRE 1.5.0_06以上がCell Managerにインストールされている場合にのみ動作します。

その他の前提条件および制限事項については、HP AutoPassのオンラインヘルプを参照してください。

パスワードはCell Managerにインストールされ、セル全体に対して有効です。

手順

恒久パスワードを取得し、インストールするには、以下の手順に従ってください。

1. 恒久パスワードを取得するために必要な情報を集めます。必要な情報についてはHP AutoPassのオンラインヘルプを参照してください。
2. *HP AutoPass*ユーティリティを使用してオンラインでパスワードを注文します。*HP AutoPass*ユーティリティを開始するには、以下のコマンドをCell Managerで実行します。

注記:

Manager-of-Managers (MoM)環境では、MoMシステム上(Data Protectorの集中型ライセンスを使用する場合)、またはパスワードが注文されインストールされるCell Manager上(Data Protectorの集中型ライセンスを使用しない場合)で、omniinstlicコマンドを実行する必要があります。

opt/omni/sbin/omniinstlic (UNIX用Cell Managerの場合)、または

Data_Protector_home¥bin¥omniinstlic (Windows用Cell Managerの場合)

詳細は、omniinstlicのマンページまたは『*HP Data Protector Command Line Interface Reference*』を参照してください。

3. *HP AutoPass*ユーティリティウィザードに従い、必要な情報を入力します。

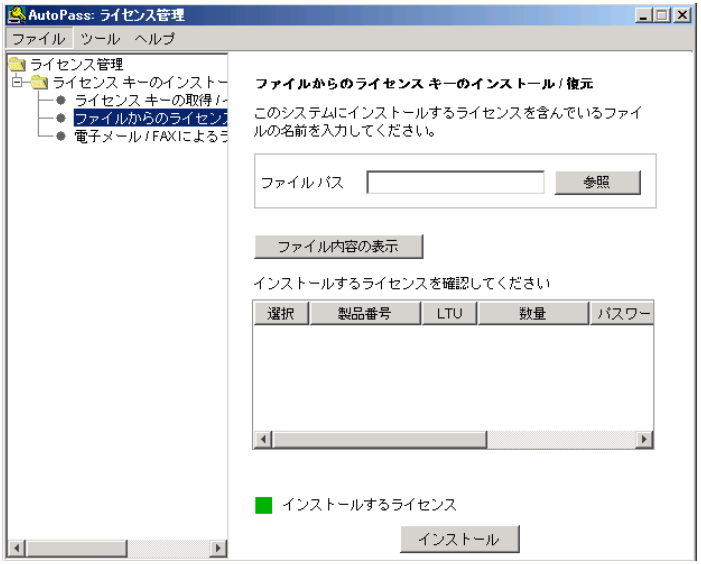


図 52 HP AutoPassウィザード

ウィザードの手順の最後で[Get password]をクリックすると、*HP Password Delivery Center*からCell Managerに、購入したライセンスの恒久パスワードが転送されます。

[Finish]をクリックすると、購入したライセンスの恒久パスワードが、Cell Managerにインストールされます。

4. Installされているパスワードを確認する手順は、「パスワードの検証」(333ページ)を参照してください。

恒久パスワードの取得とインストールのためのその他の方法

取得

恒久パスワードを取得するには、以下の手順に従ってください。

1. Permanent Password *Request Form*に記入する情報を収集します。このフォームの場所とフォームの入力方法は、「Data Protectorライセンスフォーム」(340ページ)を参照してください。
2. 製品構成の詳細は、「Data Protector 6.20の製品構成とライセンス」(336ページ)を参照してください。請求フォームを送るときと同じ方法で、*HP Password Delivery Center*から恒久パスワードが届きます。たとえば、請求フォームを電子メールで送信した場合は、恒久パスワードは電子メールで送信されます。

3. 次のいずれかの作業を行います。
   - オンラインの*HP Password Delivery Center*サイト(http://www.webware.hp.com)にアクセスします。
   - *Permanent Password Request Form*に必要事項を記入して、以下のいずれかの方法で*HP Password Delivery Center*に送信します。デリバリセンターのファックス番号、電話番号、電子メールアドレス、営業時間については、製品に付属する権利保証書(Entitlement Certificate)を参照してください。
     - フォームを*HP Password Delivery Center*にファックスで送付します。
     - *HP Password Delivery Center*に電子メールで送信します。

       以下の名前のファイルにデータとして含まれているライセンスフォームも使用できます。ファイルは、Cell Managerまたは配布メディアに含まれています。
       - Windows Cell Managerの場合: `Data_Protector_home¥Docs¥license_forms.txt`
       - UNIX Cell Managerの場合: `/opt/omni/doc/C/license_forms_UNIX`
       - Windows用のインストールDVD-ROMの場合: `Disk_Label:¥Docs¥license_forms.txt`

       上記のフォームを使用して、*Password Delivery Center (HP PDC)*へのメッセージをコピーして貼り付けることもできます。

       通常は、*Permanent Password Request Form*をお送りいただいてから24時間以内に、恒久パスワードをお届けします。

インストール

この項では、*HP Password Delivery Center (HP PDC)*から通知された恒久パスワードをインストールする手順を説明します。

前提条件

*HP Password Delivery Center*から恒久パスワードが届き、Cell ManagerにData Protectorユーザーインタフェースがインストールされている必要があります。パスワードはCell Managerにインストールされ、セル全体に対して有効です。

GUIを使用する場合

Data Protector GUIを使用して恒久パスワードをインストールするには、以下の手順に従ってください。

1. コンテキストリストで[**クライアント**]をクリックします。
2. Scopingペインで[**Data Protectorセル**]を右クリックし、[**ライセンスの追加**]をクリックします。

3. パスワードは、*パスワード証明書*に記載されているとおりに入力します。

   パスワードは、4文字ごとのグループをスペースで区切った8つのグループと、それに続く文字列で構成されます。パスワードの中に行送り文字や改行文字を含めることはできません。パスワードの例を次に示します。

   2VFF 9WZ2 C34W 43L7 RYY7 HBYZ S9MQ 1LZA JUUQ TA48 EPNB QFRN MR9F 2A2A 7UEG 9QR3 Y3QW LZA9 AZA9 EQ97 "Product; Cell Manager for UNIX"

   パスワードを入力し終えたら、以下のチェックを行ってください。

   - 画面上のパスワードが正しいことを確認します。
   - パスワードの前後にスペースがなく、また余分な文字が含まれていないことを確認します。
   - 数字の“1”と小文字の"l"を混同していないことを確認します。
   - 大文字の"O"と数字の"0"を混同していないことを確認します。
   - 大文字と小文字を正しく入力していることを確認します。パスワードでは、大文字と小文字が区別されます。

   [OK]をクリックします。

Cell Manager上の以下のファイルにパスワードが書き込まれます。

- Windows Server 2008の場合: Data_Protector_program_data¥Config¥server¥Cell¥lic.dat
- その他のWindowsシステムの場合: Data_Protector_home¥Config¥server¥Cell¥lic.dat
- UNIXシステムの場合: /etc/opt/omni/server/cell/lic.dat

CLIを使用する場合

Data Protector CLIを使用して恒久パスワードをインストールするには、以下の手順に従ってください。

1. Cell Managerにログオンします。

2. 以下ののコマンドを実行します。
   - Windowsの場合:

     Data_Protector_home¥bin¥omnicc -install_license password
   - UNIXの場合: /opt/omni/bin/omnicc -install_license password

   passwordには、パスワードを入力します。*Password Certificate*に記載されているとおりに入力する必要があります。パスワードは1行で、組み込み改行が含まれないようにしてください。パスワードは引用符で囲まれている必要があります。パスワードに引用符に囲まれた説明が含まれる場合は、説明を示す引用符の直前にバックスラッシュが必要です。例および詳細は、omniccのマンページまたは『*HP Data Protector Command Line Interface Reference*』を参照してください。

パスワードをCell Manager上の以下のファイルに追加することもできます。

- Windows Server 2008の場合: Data_Protector_program_data¥config¥server¥cell¥lic.dat
- その他のWindowsシステムの場合: Data_Protector_home¥config¥server¥cell¥lic.dat
- UNIXシステムの場合: /etc/opt/omni/server/cell/lic.dat

ファイルが存在しない場合は、viやメモ帳などのエディターを使用して作成します。パスワードの例は、グラフィカルユーザーインタフェース用の手順ステップ 3(332ページ)を参照してください。

パスワードの検証

GUIを使用する場合

Installしたライセンスのパスワードが正しいかどうかを検証するには、Data Protector GUIで以下の手順に従います。

1. [ヘルプ]メニューで**[情報]**をクリックします。
2. **[ライセンス]**タブをクリックします。インストールされているすべてのライセンスが表示されます。入力したパスワードが間違っている場合は、「パスワードをデコードできませんでした。」という注釈が付きます。

CLIを使用する場合

Installしたライセンスのパスワードが正しいかどうかを検証するには、以下の手順に従います。

- Windowsの場合:

  Data_Protector_home¥bin¥omnicc -password_info

- UNIXの場合: /opt/omni/bin/omnicc -password_info

このコマンドを実行すると、インストールされているすべてのライセンスが表示されます。入力したパスワードが間違っている場合は、「パスワードをデコードできませんでした。」という注釈が付きます。

インストール済みライセンスの数を調べる

GUIを使用する場合

恒久パスワードのインストール後、Cell Manager上に現在インストールされているライセンスの数を確認できます。

1. Data Protector Managerを起動します。
2. メニューバーで、[**ヘルプ**]、[**情報...**]の順にクリックします。[Managerについて]ウィンドウが開き、インストールされているライセンスが表示されます。

CLIを使用する場合

コマンドラインを使用する場合は、以下の手順に従ってください。

1. Cell Managerにログオンします。
2. 次のコマンドを実行します。
   - Windowsの場合: Data_Protector_home¥bin¥omnicc -query
   - UNIXの場合: /opt/omni/bin/omnicc -query

現在インストールされているライセンスのリストが表示されます。

他のCell Managerシステムへのライセンスの移動

以下の場合は、*HP Password Delivery Center*にご連絡ください。

- Cell Managerを他のシステムに移動する場合。
- Cell Managerにインストールされているライセンスのうち、セル内で現在使用していないライセンスを他のData Protectorセルに移動する場合。

注記:

UNIXライセンスを別のUNIX用Cell ManagerまたはWindows用Cell Managerに移動することは可能ですが、WindowsライセンスをUNIX用Cell Managerに移動することはできません。

ライセンスをCell Manager間で移動するには、以下の手順に従います。

1. 新しいCell Managerごとに*ライセンス移動フォーム(License Move Form)*を1つ作成し、*HP Password Delivery Center*に送付します。現在は購入できない製品のライセンスを移動する場合は、以前のバージョンに付属している*License Move Forms*を使用してください。「Data Protectorライセンスフォーム」(340ページ)を参照してください。

   フォームでは、既存のCell Managerから移動するライセンスの数を明記する必要があります。

2. 以下のファイルを削除します。
   - Windows Server 2008の場合: `Data_Protector_program_data¥config¥server¥cell¥lic.dat`
   - その他のWindowsシステムの場合: `Data_Protector_home¥config¥server¥cell¥lic.dat`
   - UNIXシステムの場合:`/etc/opt/omni/server/cell/lic.dat`

3. ライセンス移動フォーム(*License Move Form*)に必要事項を記入し、*HP Password Delivery Center (PDC)*に送付した後は、移動元のCell ManagerからData Protectorのパスワードをすべて削除してください。

4. 新しいパスワードをインストールします。パスワードは、新しいCell Managerごとに配布されます。ライセンスが現在のCell Managerに残される場合は、現在のCell Managerにも新しいパスワードが配布されます。現在のCell Managerのパスワードエントリーは、新しいパスワードによって置き換えられます。

集中型ライセンス

Data Protectorでは、マルチセル環境全体を対象とする集中型ライセンスを構成できます。これにより、ライセンスを簡単に管理できるようになります。すべてのライセンスは、Manager-of-Managers (MoM) Managerシステムに保管されます。ライセンスは、MoM Manager上で構成された状態で、特定のセルに割り当てられます。

ライセンスの構成方法の詳細は、Data Protectorオンラインヘルプを参照してください。

注記：

UNIXライセンスを別のUNIX用Cell ManagerまたはWindows用Cell Managerに割り当てることは可能ですが、WindowsライセンスをUNIX用Cell Managerに割り当てることはできません。

MoM機能を使用すると、MoMセル間でライセンスを移動(再割り当て)することができます。詳細は、オンラインヘルプの索引「MoM環境」を参照してください。

新しいData Protectorライセンスをインストールする場合は、ライセンスを請求する前にMoM機能を確認してください。集中型ライセンスを後から適用する場合は、適用時に移動の手順を実行する必要があります。

注記：

MoM機能によって、集中型ライセンスが実現されます。これは、すべてのライセンスをMoM Managerにインストールしてから、MoMセルに属するCell Managerにライセンスを配布できることを意味します。後からMoMセル間でライセンスを移動(再配布)することもできます。詳細は、オンラインヘルプの索引「MoM環境」を参照してください。

Data Protector 6.20の製品構成とライセンス

この項では、Data Protector製品構成の使用方法について説明しており、購入する必要がある製品番号を簡単に特定できます。

製品構成は、図53(337ページ)に示すように、いくつかのセクションに分かれています。Data Protectorソリューションは、これらセクションに沿って、以下の手順でご注文ください。

1. スターターパックを選択します。適切な製品番号は、Cell Managerシステムのオペレーティングシステムによって異なります。
2. 環境内に構成されているドライブの数と、使用するテープライブラリを確定します。
3. 必要となるその他の機能を特定します。推奨される機能は、オンラインバックアップからインスタントリカバリまでさまざまです。

スターターパックライセンスとメディアは最低1つ必要です。

注記：

UNIX製品用に提供されるライセンスは、すべてのオペレーティングシステムに適用できます。

DP6.2 ライセンスガイド用製品構成一覧

	シングルサーバー版	すべてのプラットフォーム	Windows	HP-UX		Solaris
	LTU のみ / スターターパックへの移行 DVD のみ （言語を選択）	言語ごと *	B7030BA/B7031AA	B7020BA/B7021AA		B7020CA/B7021DA
1	スターターパック （必須）	すべてのプラットフォーム	Windows	Linux	HP-UX	Solaris
1	LTU のみ 1×セル DVD のみ （言語を選択）	言語ごと *	B6961BA	B6961CA	B6951BA	B6951CA
1	ドライブとライブラリの使用権	すべてのプラットフォーム	Windows, NetWare, Linux		SAN, UNIX, NAS	
1	ドライブ LTU 1×ドライブ ライブラリ LTU 1×61 ～ 250/スロット数無制限 1×スロット数無制限アップグレード	B6957BA/B6958BA B6958CA	B6963AA		B6953AA	
2	2. Manager of Managers		Windows & Linux		UNIX	
2	Manager-of-Managers LTU 1 × システム		B6966AA		B6956AA	
3	3. ディスクへのバックアップ	すべてのプラットフォーム				
3	ディスクへのアドバンストバックアップ 1LTU×TB/10×TB/100×TB	B7038AA/BA/CA				
4	4. アプリケーション保護	すべてのプラットフォーム	Windows	Linux	UNIX	
4	オンラインバックアップ LTU 1 × システム		B6965BA		B6955BA	
4	ゼロダウンタイムバックアップ LTU 1×TB/10×TB インスタントリカバリ LTU 1×TB/10×TB		QuickSpecs 上の SKU QuickSpecs 上の SKU	B7025CA/B7025DA B7028AA/B7028DA		
4	Granular Recovery 使用権 1 × システム	TB737AA				
4	ノートブック使用権 LTU 1 × 100 / 1000 クライアント	TA032AA/TA033AA			CD only	TA031AA
4	オープンファイルバックアップ LTU 1× Ent. サーバー/5× W/S 1×1サーバー/1×10サーバー	BA155AA/BA154AA BA153AA/BA153BA			CD only	BA152AA
4	暗号化 LTU 1 × 1 サーバー / 1 × 10 サーバー	BB618AA/BB618BA				
4	Media Operation LTU 1 2,000 / 10,000 メディア 1 × 無制限のメディア	B7100AA/B7101AA B7102AA				
4	NDMP LTU 1 × TB / 10 × TB / 100TB	B7022BA/B7022DA/TD186AA				

* HP Web サイトの「QuickSpecs」から確認できる製品番号（SKU） 電子版は、SKU の末尾に「E」を追加してください。

図 53 HP Data Protector製品構成

注記：

*このマニュアルの製品構成は、例示のみを目的として記載されています。*最新の製品構成は、次のWebサイト http://h18006.www1.hp.com/products/quickspecs/Division/Division.html#12647 で入手可能です。

Data Protectorでは、以前のData Protectorバージョンの製品番号が利用されます。そのために、既存のData Protectorライセンスは移行後も有効です。

パスワードについて

以下の項目を参照して、適切な数のパスワードを取得してください。

- 一時パスワードは任意のCell Manager候補で使用できます。ただし、その他のすべてのパスワードには、関連するプラットフォームを指定する必要があります。この場合は、中心的なData Protector管理システムとなるCell Managerも指定する必要があります。恒久パスワードを取得する前に、一時パスワードを使用してセル構成条件を完全に理解しておくことが重要です。
- 恒久パスワードは、別のCell Managerに移動できます。ただし、ライセンス移動フォーム(License Move Form)を*HP Password Delivery Center (PDC)*に送る必要があります。
- パスワードはCell Managerにインストールされ、セル全体に対して有効です。
- Manager-of-Managers (MoM)機能の一部として集中型ライセンスが提供されます。複数のセル用に複数のライセンスを購入した場合は、MoMシステムにすべてのライセンスをインストールしておくことができます。
- 各セルごとに、Cell Managerライセンスが1つ必要です。

注記:

Data Protectorのライセンス(一時ライセンスおよび緊急用パスワードを除く、期間限定または恒久の、IPまたはサブネットにバインドされたIPベースのライセンス)では、Cell ManagerにIPv4アドレスが必要です。IPv6環境で実行する場合は、Cell Managerがデュアルスタックモードで構成され、IPv4とIPv6の両方が有効になっている必要があります。ライセンスの目的には、Cell ManagerのIPv4アドレスが使用されます。

複数のIPアドレスを持つシステム(複数アドレスを持つシステム、RASサーバー、クラスター)にCell Managerがインストールされている場合は、ライセンスをこれらのIPアドレスのいずれにもバインドさせることができます。

- Data Protectorの構成作業やバックアップセッションを開始するたびに、ソフトウェアによってライセンスが定期的にチェックされます。
- 一時パスワードは任意のシステムで使用できますが、評価用パスワードと恒久パスワードは、ライセンス請求時に指定したCell Managerに対してのみ使用できます。

注記：

Cell ManagerのIPアドレスを変更する場合、Cell Managerを別のシステムに移動する場合、セル間でライセンスを移動する場合(MoM機能を使用しない場合)は、*HP Password Delivery Center (PDC)*に連絡し、ライセンスを更新する必要があります。HP Password Delivery Centerへの連絡については、「恒久パスワードの取得とインストールのためのその他の方法」(330ページ)を参照してください。

Data Protector 6.20へのライセンス移行

Data Protector 6.20に直接移行します。Data Protectorの以前のリリースのライセンスは、自動的に移行されます。

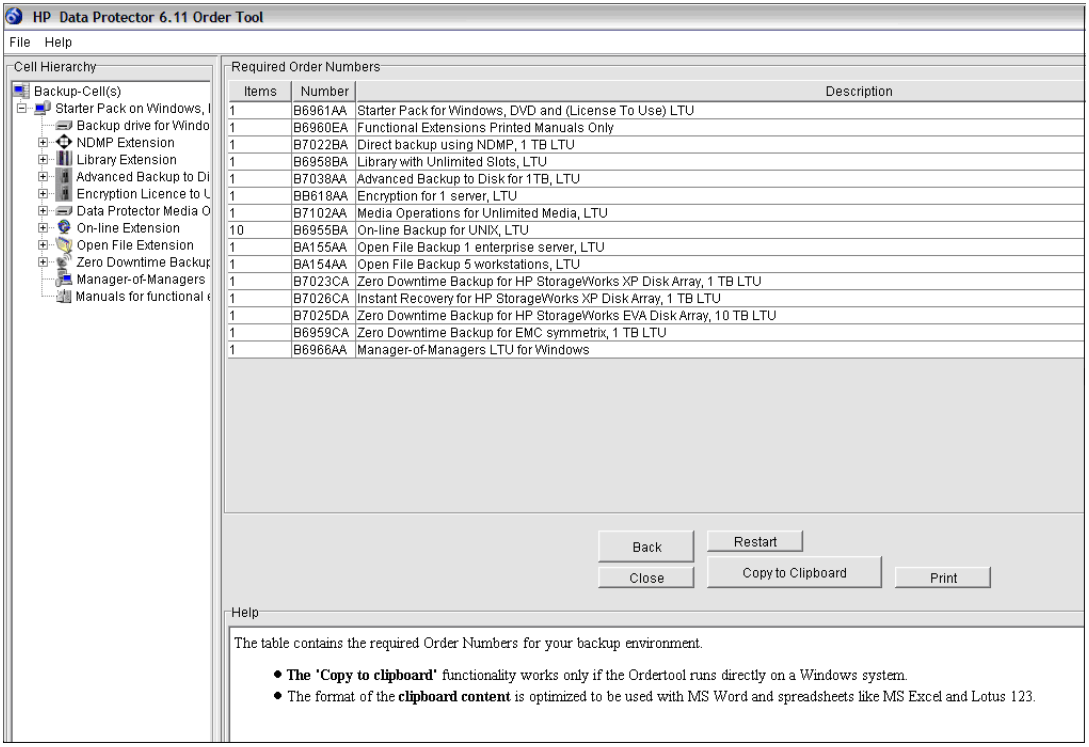
Data Protector A.06.00、A.06.10、またはA.06.11のサポート契約を結んでいるお客様は、Data Protector 6.20を無料で受け取ることができます。環境をData Protector 6.20にアップグレードすると、A.06.00、A.06.10、またはA.06.11で使用していた機能は追加費用なしでData Protector 6.20で使用できるようになります。新しい機能拡張が必要な場合は、新しいライセンスを購入するだけで入手できます。

Data Protector Order Tool

Data Protectorでは、使用環境で必要とされるData Protector製品番号のリストを自動的に生成するシンプルなツールを提供しています。Data Protector Order Toolの手順に従って、システム構成や用途についての簡単な質問に答えると、質問への回答を基にしたセル構成が表示されます。

すべての質問に答えると、お客様の環境に必要な製品番号の一覧がOrder Toolに表示されます。図54(340ページ)に例を示します。

Order ToolはData Protector インストールDVD-ROMに収録されています。



Items	Number	Description
1	B6961AA	Starter Pack for Windows, DVD and (License To Use) LTU
1	B6960EA	Functional Extensions Printed Manuals Only
1	B7022BA	Direct backup using NDMP, 1 TB LTU
1	B6958BA	Library with Unlimited Slots, LTU
1	B7038AA	Advanced Backup to Disk for 1TB, LTU
1	BB618AA	Encryption for 1 server, LTU
1	B7102AA	Media Operations for Unlimited Media, LTU
10	B6955BA	On-line Backup for UNIX, LTU
1	BA155AA	Open File Backup 1 enterprise server, LTU
1	BA154AA	Open File Backup 5 workstations, LTU
1	B7023CA	Zero Downtime Backup for HP StorageWorks XP Disk Array, 1 TB LTU
1	B7026CA	Instant Recovery for HP StorageWorks XP Disk Array, 1 TB LTU
1	B7025DA	Zero Downtime Backup for HP StorageWorks EVA Disk Array, 10 TB LTU
1	B6959CA	Zero Downtime Backup for EMC symmetrix, 1 TB LTU
1	B6966AA	Manager-of-Managers LTU for Windows

図 54 Data Protector Order Toolの例

Data Protectorライセンスフォーム

この章では、Data Protectorライセンスフォームについて説明します。以下のいずれかの方法で恒久パスワードを注文するには、これらのフォームに記入してください。

- 恒久パスワードをインターネット経由で直接HPのPassword Delivery Center Webサーバーからダウンロードしてインストールするには、HP AutoPassユーティリティを使用します。詳細は、「HP AutoPassユーティリティを使用した恒久パスワードの取得とインストール」(328ページ)を参照してください。この方法をお勧めします。
- オンラインの*Password Delivery Center*サイト(http://www.webware.hp.com)から恒久パスワードを注文することも可能です。
- 以下の名前のファイルにデータとして含まれているライセンスフォームを印刷することもできます。このファイルはCell Managerシステムまたは配布メディアに含まれています。
  - HP-UX、Solaris、Linux:/opt/omni/doc/C/license_forms_UNIX
  - Windows DVD-ROM:Disk_Label:Docs¥license_forms.txt

または、電子的なファイルを使用して、メッセージを*Password Delivery Center (PDC)*に「コピー」して「貼り付け」ます。

重要:

情報は正確に記入してください。必要事項に漏れがないように注意してください。

ライセンスフォームで記入が必要な共通のフィールドについて、以下に説明します。

ユーザー情報(Personal Data)	新しいパスワードの送付先となるユーザーに関する情報を記入してください。
ライセンスデータ(Licensing Data)	Data Protectorセルに関するライセンス情報を記入します。
現在の Cell Manager	現在のCell Managerに関して必要な情報を記入します。
新しい Cell Manager	新しいCell Managerに関して必要な情報を記入します。
注文番号(Order Number)	権利保証書(*Entitlement Certificate*)に記載されている*Order Number*を記入します。この*Order Number*は、恒久パスワードを請求する際に必要です。
IPアドレス(IP Address)	このフィールドでは、*Password Delivery Center*がパスワードを生成するシステムのIPアドレスが定義されます。集中型ライセンスを使用する場合(MoM環境のみ)、このシステムはMoM Managerシステムにする必要があります。 Cell Managerに複数のLANカードがある場合、どのIPアドレスでも入力できます。プライマリIPアドレスを入力することをお勧めします。

	MC/ServiceGuard環境または Microsoft Cluster環境内でData Protectorをお使いの場合、仮想サーバーのIPアドレスを入力します。クラスターの詳細については、オンラインヘルプを参照してください。
*Password Delivery Center*ファックス番号	連絡先は、製品に付属する権利保証書(*Entitlement Certificate*)でご確認ください。
製品ライセンスの種類	*Product Numbers*の横のフィールドに、このCell Managerにインストールするライセンスの数量を入力します。この数量は、*Order Number*で購入する全ライセンスでも一部でもかまいません。

6 インストール時のトラブルシューティング

この章の内容

この章では、インストール関連の問題に関する情報を提供します。トラブルシューティング全般については、『*HP Data Protectorトラブルシューティングガイド*』を参照してください。

この章には、以下に関する情報が記載されています。

- 「Windows用Cell Managerインストール時の名前解決に関する問題」(343ページ)
- 「Data Protectorセル内のDNS接続の確認」(344ページ)
- 「インストールのトラブルシューティングとData Protectorのアップグレード」(347ページ)
- 「Solaris上でのData Protector Cell Managerのインストールに関する問題のトラブルシューティング」(349ページ)
- 「UNIXクライアントのインストールに関する問題のトラブルシューティング」(349ページ)
- 「Windows XPクライアントのインストールに関する問題のトラブルシューティング」(351ページ)
- 「Windows VistaおよびWindows Server 2008クライアントのインストールに関する問題のトラブルシューティング」(352ページ)
- 「Data Protectorクライアントのインストール結果の確認 」(352ページ)
- 「アップグレードのトラブルシューティング」(353ページ)
- 「ログファイルの使用」(357ページ)
- 「インストール実行トレースの作成」(359ページ)

Windows用Cell Managerインストール時の名前解決に関する問題

WindowsでのData Protector Cell Managerのインストール時に、必要とされるDNSまたはLMHOSTSファイルがセットアップされていないことが検出され、警告メッセージが表示さ

れます。また、TCP/IPプロトコルがシステムにインストールされていない場合にも通知されます。

問題

DNSまたはLMHOSTSの使用時に名前解決に失敗する

名前の解決に失敗すると、“error expanding hostname”というメッセージが表示され、インストールが中止されます。

- DNSの使用時に名前解決の問題が発生した場合は、現在のDNS構成についての警告メッセージが表示されます。
- LMHOSTSファイルの使用時に名前解決の問題が発生した場合は、LMHOSTSファイルの構成をチェックするように指示する警告メッセージが表示されます。
- DNSとLMHOSTSのどちらも構成していない場合は、DNSまたはLMHOSTSによる名前解決をTCP/IPのプロパティダイアログで有効にするように指示する警告メッセージが表示されます。

操作

DNSまたはLMHOSTSファイルの構成をチェックするか、構成を有効にします。「Data Protectorセル内のDNS接続の確認」(344ページ)を参照してください。

問題

TCP/IPプロトコルがシステム上にインストールおよび構成されていない

Data Protectorでは、TCP/IPプロトコルを使ってネットワーク通信が行われます。したがって、セル内の各クライアントにTCP/IPプロトコルをインストールし、正しく構成しておく必要があります。そうでない場合、インストールは中止されます。

操作

TCP/IPの設定を確認します。詳細は、「Data Protectorのデフォルトのポート番号の変更」(388ページ)を参照してください。

Data Protectorセル内のDNS接続の確認

DNS(ドメインネームシステム)は、TCP/IPホスト用のネームサービスです。DNSは、ホスト名およびIPアドレスのリストで構成されます。これにより、ユーザーは、IPアドレスではなくホスト名でリモートシステムを指定できます。DNSは、Data Protectorセルのメンバー間で適切な通信が行われることを保証します。

DNSが正しく構成されていないと、Data Protectorセル内で名前解決に関する問題が発生し、メンバー相互の通信ができなくなります。

Data Protectorでは、Data Protectorセルのメンバー間のDNS接続を確認するためのomnicheckが提供されています。このコマンドを使用すると、セル内のすべての接続がチェックされますが、Data Protectorセルで最も重要な以下の接続を確認できれば十分です。

- Cell Managerからその他すべてのセルメンバーへの接続、およびその逆。
- Media Agentからその他すべてのセルメンバーへの接続、およびその逆。

omnicheckコマンドの使用

制限事項

- コマンドは、セルのメンバー間の接続のみを検証します。通常、DNSの接続は検証されません。

omnicheckコマンドは、Cell Manager上の以下のディレクトリにあります。

Windowsの場合: Data_Protector_home¥bin

UNIXの場合: /opt/omni/bin

omnicheckコマンドの使用方法は以下のとおりです。

omnicheck -dns [-host *Client* | -full] [-verbose]

さまざまなオプションを使用して、Data Protectorセル内で以下に示すDNS接続を確認できます。

- Cell Managerやセル内の各Media Agentから、セル内の各Data Protectorクライアントへの DNS接続(またはその逆)が正しく名前解決されているかを確認するには、次のコマンドを実行します。

  omnicheck -dns [-verbose]

- 特定のData Protectorクライアントからセル内の各Data Protectorクライアントへの DNS接続(またはその逆)が正しく名前解決されているかを確認するには、次のコマンドを実行します。

  omnicheck -dns -host *client* [-verbose]

  *client*には、確認対象のData Protectorクライアントの名前を指定します。

- セル内のすべてのDNS接続をチェックするには、次のコマンドを実行します。

  omnicheck -dns -full [-verbose]

[-verbose]オプションが指定されると、すべてのメッセージが返されます。このオプションを設定しなければ(デフォルト)、チェック失敗に関するメッセージだけが返されます。

詳細は、omnicheckマンページを参照してください。

omnicheckコマンドの出力メッセージの一覧は、表12(346ページ)を参照してください。出力メッセージでDNSの名前解決の問題が通知された場合は、HP Data Protectorトラブルシューティングガイドの「ネットワークおよび通信のトラブルシューティング」の章を参照してください。

表 12 出力メッセージ

出力メッセージ	意味
client_1がclient_2に接続できません。	*client_2*への接続がタイムアウトしました。
client_1はclient_2に接続していますが接続先のシステムはclient_3として存在しています。	*client_1*の*%SystemRoot%*¥System32¥drivers¥etc¥hosts/etc/hosts (UNIXシステム)ファイルが正しく構成されていないか、*client_2*のホスト名がDNS名に一致しません。
client_1からclient_2に接続できません。	*client_2*がアクセス不能(接続されていないなど)か、*client_1*の*%SystemRoot%*¥System32¥drivers¥etc¥hostsファイル(Windowsシステムの場合)または/etc/hostsファイル(UNIXシステムの場合)が正しく構成されていません。
client_1とclient_2の接続をチェック中	
すべてのチェックが正常に完了しました。	
number_of_failed_checksのチェックが失敗しました。	
clientはこのセルのメンバーではありません。	
clientに接続しましたが、旧バージョンのようです。Hostnameは検証されません。	

インストールのトラブルシューティングとData Protectorのアップグレード

問題

以下のいずれかのエラーメッセージが表示されることがあります。

- Windows Installerサービスにアクセスできませんでした。
- このアプリケーションを実行するには、インストールを行ってください。
- パッチパッケージをオープンできませんでした。
- システムが、指定されたデバイスまたはファイルをオープンできません。

Data Protector 6.20のインストールまたはアップグレード後、Windowsが、一部のアプリケーションについて、インストールされていない、または再インストールが必要だというメッセージを出力することがあります。

原因は、Microsoft Installerのアップグレード手順における エラーです。Microsoft Installerバージョン1.xのデータ情報がData Protectorによってコンピュータにインストールされる Microsoft Installerバージョン2.xに移行されないために発生します。

対処方法

この問題の解決方法については、Microsoft Knowledge BaseのアーティクルQ324906を参照してください。

問題

Cell Manager いずれのWindowsドメインにも所属していないWindowsシステムへのCell Managerのインストールに失敗する

以下のエラーメッセージが表示されます。

Setup is unable to match the password with the given account name. （入力されたアカウント名とパスワードが一致しません。）

対処方法

以下の2通りの対応策があります。

- Cell Managerをインストールしようとしているwindowsシステムをドメインに参加させます。
- CRSサービス用のローカル管理者アカウントを使用します。

問題

以下のエラーメッセージが表示されます。

msvcr90.dll file is not found (msvcr90ファイルが見つかりません)

ネットワーク共有ではmsvcr90.dll (小文字)のみが使用可能になっているため、MSVCR90.dllライブラリ(大文字)が見つかりません。MSVCR90.dllとmsvcr90.dllが同じファイルとして取り扱われていないため、setup.exeが適切なdllを見つけることができません。

対処方法

ファイル名をmsvcr90.dll(小文字)からMSCVCR90.dll(大文字)に変更するか、または、大文字と小文字を区別しないようにネットワーク共有を構成し直します。

問題

インストールをキャンセルしても、すでにインストールされたコンポーネントがアンインストールされない

コンポーネントの一部がすでにインストールされている状態でData Protectorのインストールをキャンセルすると、それらのコンポーネントはアンインストールされません。インストールは終了し、エラーメッセージが表示されます。

対処方法

Installのキャンセル後に、すでにインストールされているコンポーネントを手動でアンインストールします。

Windowsクライアントのリモートインストールに関する問題

問題

セットアッププロセスの起動エラー

Data Protectorのリモートインストール機能でWindowsクライアントをアップグレードしようとしたときに、次のようなエラーが表示されることがあります。

Error starting setup process, err=[1326] Logon failure:unknown user name or bad password.

これは、インストールサーバーコンピュータ上のOmniBack共有へのアクセス権を持たないユーザーアカウントでリモートコンピュータ上のData ProtectorInetサービスが実行されていることを示します。多くの場合は、ローカルユーザーが使用されています。

対処方法

Data Protector Inetサービスのユーザーを Data Protector共有へのアクセス権がある ユーザーに変更します。

Solaris上でのData Protector Cell Managerのインストールに関する問題のトラブルシューティング

問題

一時ディレクトリを作成できない

SolarisシステムへのCell Managerのインストール中に一時ディレクトリが作成できないと、以下のメッセージが出力されてインストールに失敗することがあります。

```
Processing package instance OB2-CORE from /tmp/DP_A0611_SUN8.pkg
```

```
pkgadd:ERROR:unable to make temporary directory //tmp/old//installR.a0j3
```

対処方法

エラーメッセージで示された位置に手作業で一時ディレクトリを作成し、インストール手順を初めからやり直してください。

たとえば、上記のエラーメッセージが表示された場合は、次のディレクトリを作成してください。//tmp/old//installR.a0j3

UNIXクライアントのインストールに関する問題のトラブルシューティング

問題

UNIXクライアントのリモートインストールに失敗する

UNIXクライアントのリモートインストールまたはリモートアップグレードが、以下のエラーメッセージで失敗することがあります。

```
Installation/Upgrade session finished with errors.
```

UNIXクライアントをリモートにインストールまたはアップグレードするときは、インストールするパッケージのうち、最大のパッケージを十分格納できるだけの空き領域がクライアントシステムの/tmpフォルダ内に存在しなければなりません。Solarisクライアントシステムでは、/var/tmpフォルダ内にも同じ量の空き領域が必要です。

対処方法

上記のディレクトリ下に十分なディスクスペースがあるか確認して、インストールまたはアップグレード手順を初めからやり直してください。

ディスクスペース要件は、『*HP Data Protector製品案内、ソフトウェアノート、リファレンス*』を参照してください。

問題

HP-UXクライアントのインストールに関する問題

Data Protectorセルに新しいHP-UXクライアントを追加した場合に、以下のエラーメッセージが表示されることがあります。

```
/tmp/omni_tmp/packet:you do not have the required permissions to perform
this SD function.....
```

```
Access denied to root at to start agent on registered depot /tmp/omni_tmp/
packet.No insert permission on host.
```

対処方法

swagentswagentデーモンインストールのトラブルシューティングswagentデーモンデーモンを一度停止し、再起動します。このためには一度プロセスを終了してから/opt/omni/sbin/swagentdコマンドを実行するか、または/opt/omni/sbin/swagentd -rコマンドを実行します。

hostsファイル(/etc/hosts)にローカルホストとloopbackのエントリがあることを確認してください。

問題

Mac OS Xクライアントのインストールに関する問題

Mac OS XクライアントをData Protectorセルに追加するときに、com.hp.omniプロセスが開始されません。

対処方法

Mac OS Xでは、com.hp.omniプロセスを開始するためにlaunchdが使用されます。

サービスを開始するには、次のディレクトリに移動します。

```
cd /usr/omni/newconfig/System/Library/LaunchDaemons
```

以下のコマンドを実行します。

```
launchctl load com.hp.omni
```

問題

UNIX用のインストール後にInetプロセスを開始できない Cell Manager

Cell Managerの開始時に、以下のエラーメッセージが表示されることがあります。

ERROR: Cannot start "omniinet" service, system error:[1053] Unknown error 1053. ("omniinet"サービスを起動できません。システムエラー: [1053] 不明なエラー 1053。)

対処方法

以下のコマンドにより、inetdまたはxinetdサービスが動作しているかどうかチェックします。

*HP-UXおよびSolaris*の場合: ps -ef | grep inetd

*Linux*の場合: ps -ef | grep xinetd

サービスを開始するには、以下のコマンドを実行します。

*HP-UX*の場合: /usr/sbin/inetd

Solaris:/usr/sbin/inetd -s

*Linux*の場合: rcxinetd start

Windows XPクライアントのインストールに関する問題のトラブルシューティング

問題

Windowsクライアントのリモートインストールに失敗する

Windows XPシステムがワークグループのメンバーで、簡易ファイルの共有セキュリティポリシーが有効になっていると、ネットワーク経由でこのシステムにアクセスするユーザーは、Guestアカウントしか使用できません。リモートインストールには管理者権限が必要なため、Data Protectorは、Data Protectorクライアントのリモートインストール中に有効なユーザー名とパスワードを繰り返し要求します。

対処方法

簡易ファイルの共有を無効にします。Windows XPで[**Windowsエクスプローラ**]または[**マイコンピュータ**]を開き、[**ツール**]メニューをクリックして[**フォルダオプション**]をクリックします。[**表示**]タブを開いて、[**簡易ファイルの共有を使用する(推奨)**]チェックボックスをオフにします。

以下の場合は、簡易ファイルの共有ポリシーは無視されます。

- コンピュータがドメインのメンバーである場合
- ネットワークアクセス: ローカルアカウントの共有とセキュリティモデルのセキュリティポリシー設定がクラシック: ローカルユーザーがローカルユーザーとして認証するに設定されている場合

Windows VistaおよびWindows Server 2008クライアントのインストールに関する問題のトラブルシューティング

問題

Windowsクライアントのリモートインストールに失敗する

Data ProtectorクライアントのWindows VistaまたはWindows Server 2008システムへのリモートインストールに失敗し、以下のエラーメッセージが報告されました。

[正常域]クライアントcomputer.company.comに接続中...

[正常域] 実行されました。

[正常域]クライアントcomputer.company.comにData Protectorブートストラップサービスをインストール中...

[危険域]クライアントcomputer.company.comのSCM (Service Control Manager)に接続できません:[5]アクセスが拒否されました。

対処方法

1. インストールサーバーシステムの場合、次のコマンドを実行して、リモートインストール中にインストールサーバーで使用するローカルオペレーティングシステムの管理者ユーザーグループからユーザーアカウントをマークします。

   omniinetpasswd -inst_srv_user User@Domain

   このユーザーアカウントは、ローカルInet構成にあらかじめ追加されている必要があります。詳細は、*HP Data Protector Command Line Interface Reference*のomniinetpasswdコマンドの説明を参照してください。

2. Data Protectorクライアントのリモートインストールを再度開始します。

Data Protectorクライアントのインストール結果の確認

Data Protectorクライアントのインストール結果の確認では、以下のチェック作業を行います。

- Cell Managerシステムとクライアントシステム上のDNS構成をチェックし、Cell Managerおよびクライアントシステム上で実行したomnicheck -dnsコマンドの出力結果がそれぞれのシステムと一致することを確認します。
- ソフトウェアコンポーネントがクライアントにインストールされているかをチェックします。
- Installするソフトウェアコンポーネントに必要なファイルのリストと、クライアントにインストール済みのファイルとを比較します。
- ソフトウェアコンポーネントに必要なすべての読み取り専用ファイルのチェックサムを確認します。

前提条件

選択したクライアントシステムの種類(UNIXまたはWindows)に合ったインストールサーバーが必要です。

制限事項

この確認手順は、Novell NetWareクライアントには適用できません。

Data Protector GUIを使ってData Protectorのインストール結果を確認する場合は、以下の操作を実行します。

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ペインの[**クライアント**]を展開し、Cell Managerシステムを右クリックします。次に、[**インストールの検証**]をクリックしてウィザードを起動します。
3. ウィザードに従って、セル内のシステムのインストール結果を確認します。[インストールの検証]ウィンドウが開き、インストールの結果が表示されます。

   詳細は、オンラインヘルプを参照してください。

Installが正常に完了しなかった場合は、「ログファイルの使用」(357ページ)を参照してください。

UNIXシステム上のインストール結果をData Protector CLIで確認する方法については、ob2installのマンページを参照してください。

アップグレードのトラブルシューティング

問題

アップグレード後にIDBおよび構成ファイルを使用できない

Cell Managerを以前のリリースバージョンからアップグレードすると、IDBおよびすべての構成ファイルが使用できなくなります。この問題は、アップグレード手順が何らかの理由で中断された場合に発生します。

対処方法

アップグレード前に作成しておいたバックアップからData Protectorを復元し、処理の中断となった原因を解消してから、アップグレードを再開してください。

問題

アップグレード後に古いData Protectorパッチが削除されない

Data Protectorのアップグレード終了後にswlistコマンドを実行すると、古いData Protectorパッチがインストールされたプログラムとともにリストされます。パッチは、アップグレード中にシステムから削除されますが、swデータベースには残ります。

どのData Protectorパッチがインストールされているかを確認する方法は、「どのData Protectorパッチがインストールされているかを確認する」(240ページ)を参照してください。

対処方法

swデータベースから古いパッチを削除するには、次のコマンドを実行します。

```
swmodify -u patch.¥* patch
```

たとえば、“PHSS_30143”パッチをswデータベースから削除するには、以下のコマンドを実行します。

```
swmodify -u PHSS_30143.¥* PHSS_30143
```

問題

データベースファイルの最大サイズが2 GBを超えてしまいます。

HP-UX 11.23および11.31 (Itanium)およびSuSE Linux (x86-64)でデータベースファイル(dirs.dat、fnames.dat、fn?.ext、およびこれらの拡張ファイル)の最大サイズがデフォルトの最大サイズの2 GBを超える場合があります。その結果、Data Protector 6.20へのアップグレード時に、データベースファイルの最大サイズを調整するように勧める警告メッセージが表示されます。

Please run omnidbutil –modifytblspace to adjust maximum size of database files.(データベースファイルの最大サイズに合わせるためにomnidbutil –modifytblspaceを実行してください)

対処方法

データベースファイルの最大サイズの調整手順にはデータベースのサイズによっては時間もかかりスペースも消費されるため、この調整はアップグレードの後に行ってください。Data Protector 6.20では、サイズの調整が行われるまでA.06.00と同様に正しくない表領域サイズを報告します。ただし、バックアップおよび復元を行うことは可能です。

注記:

調整を行う前に、十分なディスクスペースがあることを確認してください。ディスクスペースには、少なくともエクスポートする現在のデータベースのサイズと同じサイズのスペースが必要になります。

すべての操作に十分な時間を確保してください。データベースのエクスポートおよびインポートには、かなりの時間がかかります(データベースの複雑さとサイズによっては、最長7日間)。また、データベースのエクスポートおよびインポート処理中はバックアップや復元を行うことはできません。

以下の手順で問題を解決してください。

1. IDB全体のバックアップを実行します。
2. IDBを既存の一時ディレクトリにエクスポートします。

   omnidbutil -writedb -mmdb *MMDBDirectory* -cdb *CDBDirectory*

   ここで、*CDBDirectory*および*MMDBDirectory*は、CDBおよびMMDBをエクスポートする一時ディレクトリです。
3. IDBを初期化します。

   omnidbinit
4. 表領域ファイルの拡張ファイルを必要に応じて追加します。

   omnidbutil -extendtblspace TablespaceFileName Pathname -maxsize Size_MB

   たとえば、fnames.datのファイルサイズが7 GBであった場合、同じコマンドを3回実行して、最大サイズが2047 MBの拡張ファイルを3つ追加する必要があります。

   omnidbutil -extendtblspace fnames.dat /var/opt/omni/server/db40/datafiles/cdb -maxsize 2047

   omnidbutil -extendtblspace fnames.dat /var/opt/omni/server/db40/datafiles/cdb -maxsize 2047

   omnidbutil -extendtblspace fnames.dat /var/opt/omni/server/db40/datafiles/cdb -maxsize 2047

   これで、fnames.dat1、fnames.dat2、およびfnames.dat3の3つの拡張ファイルが作成されます。
5. 既存のデータベースファイルの最大サイズを調整します。

omnidbutil -modifytblspace

上記の例に従うと、前に7GBに達したfnames.datのサイズが2 GBに制限されます。

6. IDBをインポートします。

   omnidbutil -readdb -mmdb *MMDBDirectory* -cdb *CDBDirectory*

   十分な拡張ファイルを作成していなかった場合、omnidbutilが終了し、以下のメッセージが表示されます。

   表領域TableSpaceNameのディスクスペースがいっぱいになりました。

   必要な拡張ファイルを追加し、インポート操作を再開します。

7. 調整が正常に完了したら、一時ファイルを削除してください。

問題

StorageTekライブラリを使用するMedia Agentクライアントをアップグレードすると、接続に問題が発生する

StorageTekライブラリを使用するシステム上でData Protector Media Agentコンポーネントをアップグレードすると、ライブラリに接続できなくなり、ライブラリを使用するData Protectorセッションの応答停止または異常終了が発生します。

対処方法

StorageTekライブラリをサポートするサービスやデーモンを再起動すると、問題が解消することがあります。

Windowsシステムの場合: [管理ツール]の[サービス]を選択し、LibAttachサービスを再起動します。

HP-UXおよびSolarisシステムの場合: /opt/omni/acs/ssi.sh stopコマンドと/opt/omni/acs/ssi.sh start ACSLS_hostnameコマンドを実行します。*ACSLS_hostname*には、Automated Cartridge Systemライブラリソフトウェアがインストールされているシステムの名前を指定します。

AIXシステムの場合: /usr/omni/acs/ssi.sh stopコマンドと/usr/omni/acs/ssi.sh start ACSLS_hostnameコマンドを実行します。*ACSLS_hostname*には、Automated Cartridge Systemライブラリソフトウェアがインストールされているシステムの名前を指定します。

手動でのアップグレード手順

通常、UNIX インストールサーバーおよびインストールサーバー上のData Protector A.06.00、A.06.10、またはA.06.10は、自動アップグレード手順を実行するomnisetup.shコマンドを実行してアップグレードします。ただし、手動でアップグレードすることもできま

す。詳細は、「ネイティブツールを使用したHP-UX、Solaris、およびLinuxシステムでのアップグレード」(380ページ)を参照してください。

ログファイルの使用

Data Protectorのインストール時に問題が発生した場合は、以下の各ログファイルの内容をチェックして、どのような問題が発生したかを 判断することができます。

- セットアップログファイル(Windows)
- システムログファイル(UNIX)
- Data Protectorログファイル

問題発生時にチェックすべきログファイルは、インストールの種類(ローカルまたはリモート)とオペレーティングシステムによって異なります。

ローカルインストール

ローカルインストールに関する問題が発生した場合は、以下のログファイルをチェックします。

HP-UX Cell Manager:

- /var/adm/sw/swinstall.log
- /var/adm/sw/swagent.log(詳細情報)

Solaris用またはLinux用Cell Managerの場合:

/var/opt/omni/log/debug.log

Windowsクライアントの場合(セットアップが稼動しているシステム):

- Temp¥SetupLog.log
- Temp¥OB2DBG_did__setup_HostName_DebugNo_setup.txt(詳細情報)

  内容は以下のとおりです。

  - did(デバッグID)は、デバッグパラメータを受け付ける最初のプロセスのプロセスIDです。このIDは、デバッグセッションのIDとして使用されます。このIDは、以降のすべてのプロセスで使用されます。
  - *HostName*は、トレースファイルが作成されたシステムの名前です。
  - *DebugNo*は、Data Protectorによって生成された番号です。
- Temp¥CLUS_DBG_DebugNo.TXT(クラスター環境)

Tempディレクトリの場所は、TEMP環境変数で指定されます。この変数の値を確認するには、setコマンドを実行します。

リモートインストール

リモートインストールの実行時に問題が発生した場合は、以下のログファイルをチェックします。

UNIX インストールサーバーの場合:

/var/opt/omni/log/IS_install.log

Windowsクライアント(コンポーネントのインストール先のリモートシステム):

- SystemRoot¥TEMP¥OB2DBG_did_INSTALL_SERVICE_DebugNo_debug.txt
- SystemRoot¥TEMP¥CLUS_DBG_DebugNo.TXT

Tempディレクトリの場所は、TEMP環境変数で指定されます。また、SystemRootは、SystemRoot環境変数で指定されたパスです。

セットアップログファイルが作成されない場合は、debugオプションを指定してリモートインストールを実行してください。詳細は、「インストール実行トレースの作成」(359ページ)を参照してください。

Data Protectorログファイル

下記のData Protectorログファイルは、以下の場所に保存されています。

Windows Vista、Windows Server 2008の場合Data_Protector_program_data¥log

その他のWindowsシステムの場合:Data_Protector_home¥log

HP-UX、Solaris、およびLinuxの場合:/var/opt/omni/log and /var/opt/omni/server/log

その他のUNIXシステムおよびMac OS Xシステムの場合: /usr/omni/log

Novell NetWareの場合: SYS:¥USR¥OMNI¥LOG

Installのトラブルシューティングに役立つログファイルを以下に示します。

debug.log	予期しない状況が記録されます。ユーザーにとって役立つものもありますが、主に当社サポートサービスが使用します。
inet.log	Data Protector inetサービスに対する要求が含まれます。クライアント上でのData Protectorの最近のアクティビティを確認するために役立ちます。

IS_install.log	リモートインスタンスのトレース情報が記録されます。このファイルは、インストールサーバー上に置かれます。
omnisv.log	Data Protectorサービスが開始および停止された日時に関する情報が記録されます。
upgrade.log	このログは、アップグレード処理中に作成されます。UCP(アップグレードコアパート)とUDP(アップグレード詳細パート)のメッセージが記録されます。
OB2_Upgrade.log	このログは、アップグレード処理中に作成されます。アップグレード処理のトレース情報が記録されます。

その他のログファイルについては、『*HP Data Protectorトラブルシューティングガイド*』を参照してください。

インストール実行トレースの作成

HPカスタマサポートサービスに要求された場合は、debugオプションを使用して、インストールを実行します。以下のdebugオプションなどのデバッグの詳細およびHPカスタマサポートサービスに送信するデータの準備に関する詳細は、『*HP Data Protectorトラブルシューティングガイド*』を参照してください。

Windowsの場合:

Windowsシステム上のリモートインストールをデバッグするには、以下に示すように、debugオプション付きでData Protector GUIを実行します。

Manager -debug 1-99 DebugPostfix

セッションを終了または中止した後で、以下のパスからデバッグ出力を収集します。

- インストールサーバーシステムの場合:

  Data_Protector_program_data¥tmp¥OB2DBG_did__BM_ Hostname_DebugNo_DebugPostfix (Windows Server 2008の場合)

  Data_Protector_home¥tmp¥OB2DBG_did__BM_ Hostname_DebugNo_DebugPostfix(その他のWindowsシステムの場合)

- リモートシステムの場合:

  SystemRoot:¥Temp¥ OB2DBG_did__INSTALL_SERVICE_Hostname_DebugNo_DebugPostfix

UNIXの場合:

UNIXシステムでインストールをデバッグする場合は、以下に示すように、debugオプション付きでData Protector GUIを実行します。

```
xomni -debug 1-99 DebugPostfix
```

または

```
xomniadmin -debug 1-99 Debug_postfix
```

セッションを終了または中止した後で、インストールサーバーシステムのtmpディレクトリからデバッグ出力を収集します。

A UNIXネイティブツールを使用したData Protectorのインストールとアップグレード

この付録の内容

この付録では、HP-UXのswinstall、Solarisのpkgadd、Linuxのrpmなど、ネイティブインストールツールを使用してUNIXシステム上でData Protectorをインストールおよびアップグレードする方法について説明します。

注記：

Data Protectorのインストールまたはアップグレードには、omnisetup.shスクリプトを使用することをお勧めします。「UNIX用Cell Managerのインストール」（45ページ）および「UNIX用Cell Managerとインストールサーバーのアップグレード」（266ページ）を参照してください。

ネイティブツールを使用した、HP-UX、Solaris、およびLinuxシステムへのインストール

注記：

パッケージの限定セットを使用してインストールサーバーをインストールする場合、HP-UX、Solaris、およびLinuxへのネイティブインストール手順のみが示されています。Data Protectorは、omnisetup.shを使用してインストールすることをお勧めします。

swinstallを使用したHP-UXシステムへのCell Managerのインストール

UNIX Cell ManagerをHP-UXシステムにインストールするには、以下の操作を行います。

1. HP-UX用インストールDVD-ROMをドライブに挿入してマウントし、/usr/sbin/swinstallユーティリティを実行します。
2. [Specify Source]ウィンドウで**[Network Directory/CDROM]**を選択し、**[Source Depot Path]**にMountpoint/hpux/DP_DEPOTと入力します。**[OK]**をクリックして[SD Install - Software Selection]ウィンドウを開きます。
3. Install可能なソフトウェアパッケージのリスト内で、B6960MAという名前の下にData Protectorが表示されます。

4. [DATA-PROTECTOR]をマウスの右ボタンでクリックし、[Mark for Install]をクリックして、ソフトウェア全体をインストール対象に含めます。

   サブプロダクトごとにインストールするかどうかを指定したい場合には、[DATA-PROTECTOR]をダブルクリックし、各項目をマウスの右ボタンでクリックします。インストールしないパッケージには[Unmark for Install]をクリックし、インストールするパッケージには[Mark for Install]をクリックして選択します。

   以下のサブプロダクトが含まれています。

OB2-CM	Cell Managerソフトウェア
OB2-DOCS	Data Protectorドキュメントサブプロダクト(PDF形式のData Protectorのガイド、およびオンラインヘルプ(WebHelp)を収録)。
OB2-IS	Data Protector インストールサーバーでは、以下の操作を行います。

   UNIX用のCell Managerをシステムにインストールしているときは、[Marked?]ステータスの値(OB2-CMパッケージの横)が[Yes]になっていることを確認してください。詳細は、図55(364ページ) を参照してください。

注記:

32ビットより長いユーザーIDを使用しているときは、Cell Managerのコアソフトウェアコンポーネントをインストールした後で、そのCell Managerにリモートでユーザーインタフェースコンポーネント(OMNI-CS)をインストールする必要があります。

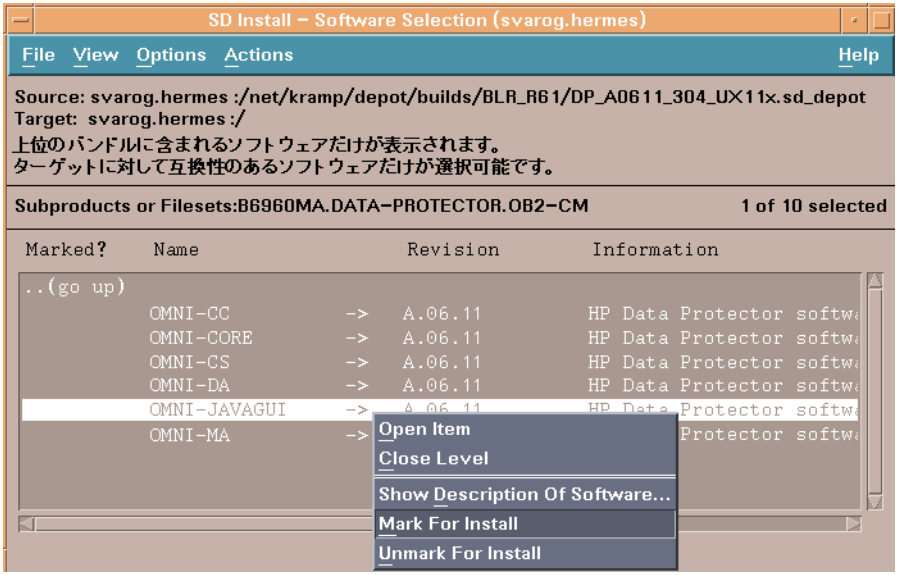


図 55 [SD install - software selection]ウィンドウ

5. [Actions]メニューの[Install (analysis)]をクリックし、[OK]をクリックして次に進みます。[Install (analysis)]で解析が失敗し、エラーメッセージが表示された場合は、[Logfile]をクリックしてログファイルを確認してください。

注記:

テープデバイスからネットワークを介してソフトウェアをインストールする場合は、まず、コンピュータでソースディレクトリをマウントする必要があります。

pkgaddを使用したSolarisシステムへのCell Managerのインストール

Cell ManagerをSolarisシステムにインストールするには、以下の操作を行います。

1. Solaris/Linux用インストールDVD-ROMをドライブに挿入します。
2. メインの*package_source*ディレクトリ、つまりインストールデポファイルが格納されているディレクトリ(この場合はMount_point/solaris/DP_DEPOT)に移動します。

3. Data Protectorのパッケージをインストールするには、pkgaddツールを使用します。

```
pkgadd -d Mount_point/solaris/DP_DEPOT
```

プロダクト内にはCell Managerのインストールに関連する以下のサブプロダクトパッケージが含まれています。

OB2-CORE	Data Protectorのコアソフトウェア。
OB2-CC	Cell Consoleソフトウェア。これには、コマンドラインインタフェースが含まれます。
OB2-CS	Cell Managerソフトウェア
OB2-DA	Disk Agentソフトウェア。このソフトウェアは必須です。このソフトウェアがない場合は、IDBのバックアップを実行できません。
オプションソフトウェア	
OB2-MA	General Media Agentソフトウェア。このコンポーネントは、バックアップデバイスをCell Managerに接続する場合に必要になります。
OB2-DOCS	Data Protectorドキュメントサブプロダクト(PDF形式のData Protectorのガイド、およびオンラインヘルプ(WebHelp)を収録)。
OB2-JAVAGUI	Javaベースのグラフィカルユーザーインタフェース。これには、Cell Managerのグラフィカルユーザーインタフェースおよび Manager-of-Managers(MoM)のグラフィカルユーザーインタフェースが含まれます。Java GUIが存在するクライアントにコマンドラインインタフェースをインストールする場合は、OB2 - CCパッケージをインストールする必要があります。

重要:

Solaris上のサブプロダクトパッケージは、互いに依存しています。これらのパッケージは、上記の順序でインストールしなければなりません。

4. Data Protectorサービスを再起動します。

   /opt/omni/sbin/omnisv stop

   /opt/omni/sbin/omnisv start

注記:

Cell ManagerをSolaris 9またはSolaris 10にインストールした場合、インストールサーバーを使用してCell ManagerにDisk Agentをリモートインストールします。これにより、汎用のSolaris Disk AgentがSolaris 9 Disk AgentまたはSolaris 10 Disk Agentに置き換えられます。Solaris 10では、Cell Manager上でのMedia Agentのリモートインストールも必要です。「Data Protectorクライアントのリモートインストール」(82ページ)を参照するか、またはob2installのマンページを参照してください。

rpmを使用したLinuxシステムへのCell Managerのインストール

Cell ManagerをLinuxシステムにインストールするには、以下の操作を行います。

1. SolarisおよびLinuxインストールDVD-ROMをドライブに挿入してマウントします。
2. linux_x86_64/DP_DEPOTディレクトリへ移動します。

3. 次のコマンドを実行して、パッケージをインストールします。

```
rpm -i package_name-A.06.20-1.x86_64.rpm
```

*package_name*には、サブプロダクトパッケージの名前を指定します。

以下のパッケージは必ずインストールしてください。

OB2-CORE	Data Protectorのコアソフトウェア。
OB2-CC	Cell Consoleソフトウェア。これには、コマンドラインインタフェースが含まれます。
OB2-CS	Cell Managerソフトウェア。
OB2-DA	Disk Agentソフトウェア。このソフトウェアは必須です。このソフトウェアがない場合は、IDBのバックアップを実行できません。
OB2-MA	General Media Agentソフトウェア。このコンポーネントは、バックアップデバイスをCell Managerに接続する場合に必要になります。
OB2-DOCS	Data Protectorドキュメントサブプロダクト(PDF形式のData Protectorのガイド、およびオンラインヘルプ(WebHelp)を収録)。
OB2-JAVAGUI	Javaベースのグラフィカルユーザーインタフェース。これには、Cell Managerのグラフィカルユーザーインタフェースおよび Manager-of-Managers(MoM)のグラフィカルユーザーインタフェースが含まれます。Java GUIが存在するクライアントにコマンドラインインタフェースをインストールする場合は、OB2 - CCパッケージをインストールする必要があります。

重要:

Linuxのサブプロダクトパッケージは互いに依存しています。これらのパッケージは、上記の順序でインストールしなければなりません。

4. Data Protectorサービスを再起動します。

   /opt/omni/sbin/omnisv stop

   /opt/omni/sbin/omnisv start

swinstallを使用したHP-UXシステムへのインストールサーバーのインストール

1. HP-UX用インストールDVD-ROMをドライブに挿入してマウントし、/usr/sbin/swinstallユーティリティを実行します。
2. [Specify Source]ウィンドウで**[Network Directory/CDROM]**を選択し、**[Source Depot Path]**にMountpoint/hpux/DP_DEPOTと入力します。**[OK]**をクリックして[SD Install - Software Selection]ウィンドウを開きます。
3. Install可能なソフトウェアパッケージのリスト内で、B6960MAという名前の下にData Protectorが表示されます。これをダブルクリックすると、UNIX用のDATA-PROTECTOR製品が表示されます。さらにこれをダブルクリックすると、内容が表示されます。

   以下のサブプロダクトが含まれています。

OB2-CM	Cell Managerソフトウェア
OB2-DOCS	Data Protectorドキュメントサブプロダクト(PDF形式のData Protectorのガイド、およびオンラインヘルプ(WebHelp)を収録)。
OB2-IS	Data Protector インストールサーバーでは、以下の操作を行います。

4. [SD Install - Software Selection]ウィンドウで、**[DATA-PROTECTOR]**をダブルクリックすると、インストール可能なソフトウェアが表示されます。**OB2-IS**をマウスの右ボタンでクリックし、**[Mark for Install]**をクリックします。
5. [Actions]メニューの**[Install (analysis)]**をクリックします。**[OK]**をクリックして次に進みます。

Installが終了すると、UNIX用のソフトウェアデポは、/opt/omni/databases/vendorディレクトリに配置されます。

重要:

ネットワーク上にUNIX用のインストールサーバーをインストールしない場合は、HP-UXインストールDVD-ROMを使用して、すべてのUNIXクライアントをローカルにインストールする必要があります。

pkgaddを使用したSolarisシステムへのインストールサーバーのインストール

Solarisへのローカルインストール

UNIX用のインストールサーバーをSolarisシステムにインストールするには、以下の操作を行います。

1. Solaris/Linux用インストールDVD-ROMをドライブに挿入します。

2. メインの*package_source*ディレクトリ、つまりインストールデポファイルが格納されているディレクトリに移動します(この場合はMount_point/solaris/DP_DEPOT)。

   プロダクト内にはインストールサーバーのインストールに関連する以下のサブプロダクトパッケージが含まれています。

OB2-CORE	Data Protectorのコアソフトウェア。インストールサーバーをCell Managerシステムにインストールする場合は、コアソフトウェアはすでにインストールされています。
OB2-C-IS	インストールサーバーのコアソフトウェア
OB2-CFP	すべてのUNIXプラットフォームに共通のインストールサーバーコアインストールパケット
OB2-CCP	すべてのUNIXプラットフォーム用のCell Consoleリモートインストールパケット
OB2-DAP	すべてのUNIXプラットフォーム用のDisk Agentリモートインストールパケット
OB2-MAP	すべてのUNIXプラットフォーム用のMedia Agentリモートインストールパケット

   さらに、(Cell Managerとは別のシステムに)独立した形でインストールサーバーをセットアップし、ユーザーインタフェースを使用したい場合は、次のコンポーネントが必要です。

OB2-CC	Cell Consoleソフトウェア。これには、コマンドラインインタフェースが含まれます。
OB2-JAVAGUI	Java GUIソフトウェア。これには、Cell Managerのグラフィカルユーザーインタフェースおよび Manager-of-Managers(MoM)のグラフィカルユーザーインタフェースが含まれます。

3. 上記のパッケージをインストールするには、pkgadd 機能を使用します。

重要:

Solaris上のサブプロダクトパッケージは、互いに依存しています。これらのパッケージは、上記の順序でインストールしなければなりません。

各パッケージをインストールするには、以下のコマンドを実行します。

```
pkgadd -d package_name
```

注記:

pkgadd **機能はリモートでは使用できず、ローカルな形でのみ実行可能です。**

4. これらのコンポーネントのインストールが終了したら、次にpkgaddコマンドを使用して、リモートインストールする各統合パッケージに必要なリモートインストールパケットをインストールします。以下に例を示します。

OB2-INTGP	Data Protectorの統合コアソフトウェア。このコンポーネントは、統合ソフトウェアをインストールする場合に必要です。
OB2-JGUIP	Java GUIリモートインストールパケットこれには、Cell Managerのグラフィカルユーザーインタフェースおよび Manager-of-Managers(MoM)のグラフィカルユーザーインタフェースが含まれます。Java GUIが存在するクライアントにコマンドラインインタフェースをインストールする場合は、OB2-CCパッケージをインストールする必要があります。
OB2-SAPP	SAP用統合ソフトウェアコンポーネント
OB2-VMWP	VMware用統合ソフトウェアコンポーネント
OB2-SAPDBP	SAP DB用統合ソフトウェアコンポーネント
OB2-INFP	Informix用統合ソフトウェアコンポーネント
OB2-LOTP	Lotus Notes/Domino用統合ソフトウェアコンポーネント
OB2-SYBP	Sybase用統合ソフトウェアコンポーネント
OB2-OR8P	Oracle用統合ソフトウェアコンポーネント
OB2-DB2P	DB2用統合ソフトウェアコンポーネント
OB2-EMCP	EMC Symmetrix用統合ソフトウェアコンポーネント
OB2-SMISP	HP StorageWorks P6000 EVA SMI-S Agentコンポーネント
OB2-SSEAP	HP StorageWorks P9000 XP Agentコンポーネント
OB2-NDMPP	NDMP Media Agentソフトウェア

OB2-OVP	HP NNM用統合ソフトウェアコンポーネント
OB2-FRAP	フランス語版マニュアル(ガイド、ヘルプ)パッケージ
OB2-JPNP	日本語版マニュアル(ガイド、ヘルプ)パッケージ
OB2-CHSP	簡体字中国語版マニュアル(ガイド、ヘルプ)パッケージ
OB2-PEGP	PEGASUSパッケージ
OB2-VLSAMP	VLS-AMパッケージ

全コンポーネントのリストおよびインストールの依存関係については、表9(259ページ)を参照してください。

Installが終了すると、UNIX用のソフトウェアデポは、/opt/omni/databases/vendorディレクトリに配置されます。

重要:

ネットワーク上にUNIX用のインストールサーバーをインストールしない場合は、SolarisおよびLinuxインストールDVD-ROMを使用して、すべてのUNIXクライアントをローカルにインストールする必要があります。

重要:

Data Protectorは、たとえば次のようなリンクディレクトリにインストールすることができます。

/opt/omni/ -> /prefix/opt/omni/

/etc/opt/omni/ -> /prefix/etc/opt/omni/

/var/opt/omni/ -> /prefix/var/opt/omni/

このようにする場合は、インストール前にリンクを作成しておき、インストール先ディレクトリが存在することを確認しておかなければなりません。

注記：

ユーザーインタフェースコンポーネント(グラフィカルユーザーインタフェースまたはコマンドラインインタフェース)をインストールする場合は、使用前に環境変数を更新する必要があります。詳細は、「環境変数の設定」(53ページ)を参照してください。

複数プラットフォームにわたるバックアップや復元をData Protectorユーザーインタフェースを使用して実行するよう計画している場合は、『HP Data Protector製品案内、ソフトウェアノート、リファレンス』を参照して制限事項を確認してください。

この次に行う作業

この時点で、UNIX用のインストールサーバーがネットワーク上にすでにインストールされていなければなりません。準備が整ったら、以下の作業を実施します。

1. 独立した形で(Cell Managerとは別のシステムに)インストールサーバーをセットアップした場合は、このシステムをData Protectorセルに手動で追加(インポート)する必要があります。「セルへのインストールサーバーのインポート」(216ページ)を参照してください。

   注記：

   インストールサーバーをインポートすると、Cell Manager上の`/etc/opt/omni/server/cell/installation_servers`**ファイルが更新されて、リモートインストールパケットがリストに表示されます。CLIからこのファイルを使用して、使用可能なリモートインストールパケットを確認できます。このファイルを最新状態に保つために、リモートインストールパケットをインストールまたは削除したときは、インストールサーバーのエクスポートと再インポートを必ず実行してください。これは、インストールサーバーをCell Managerと同じシステムにインストールしてある場合も同様です。**

2. Data ProtectorセルにWindowsシステムが含まれている場合は、Windows用のインストールサーバーをインストールする必要があります。前提条件(68ページ)を参照してください。
3. ソフトウェアをクライアントに配布します。「Data Protectorクライアントのインストール」(72ページ)を参照してください。

rpmを使用したLinuxシステムへのインストールサーバーのインストール

Linuxへのローカルインストール

UNIX用のインストールサーバーをLinuxシステムにインストールするには、以下の操作を行います。

1. Solaris/Linux用インストールDVD-ROMをドライブに挿入します。
2. Installアーカイブが格納されているディレクトリ(この場合はMount_point/linux_x86_64/DP_DEPOT)に移動します。

3. 個々のパッケージについて、次のコマンドを実行します。

```
rpm -i package_name-A.06.20-1.x86_64.rpm
```

プロダクト内にはインストールサーバーのインストールに関連する以下のサブプロダクトパッケージ(*package_name*)が含まれています。

OB2-CORE	Data Protectorのコアソフトウェア。インストールサーバーをCell Managerシステムにインストールする場合は、コアソフトウェアはすでにインストールされています。
OB2-CORE-IS	インストールサーバーのコアソフトウェア
OB2-CFP	すべてのUNIXプラットフォームに共通のインストールサーバーコアソフトウェア
OB2-CCP	すべてのUNIXプラットフォーム用のCell Consoleリモートインストールパケット
OB2-DAP	すべてのUNIXプラットフォーム用のDisk Agentリモートインストールパケット
OB2-MAP	すべてのUNIXプラットフォーム用のMedia Agentリモートインストールパケット

さらに、(Cell Managerとは別のシステムに)独立した形でインストールサーバーをセットアップし、ユーザーインタフェースを使用したい場合は、次のコンポーネントが必要です。

OB2-CC	Cell Consoleソフトウェア。これには、コマンドラインインタフェースが含まれます。
OB2-JAVAGUI	Java GUIソフトウェア。これには、Cell Managerのグラフィカルユーザーインタフェースおよび Manager-of-Managers(MoM)のグラフィカルユーザーインタフェースが含まれます。

4. これらのコンポーネントのインストールが終了したら、次にrpmコマンドを使用して、リモートインストールする各統合パッケージに必要なリモートインストールパケットをインストールします。以下に例を示します。

OB2-INTGP	Data Protectorの統合コアソフトウェア。このコンポーネントは、統合ソフトウェアをインストールする場合に必要です。
OB2-JGUIP	Java GUIリモートインストールパケットこれには、Cell Managerのグラフィカルユーザーインタフェースおよび Manager-of-Managers(MoM)のグラフィカルユーザーインタフェースが含まれます。Java GUIが存在するクライアントにコマンドラインインタフェースをインストールする場合は、OB2-CCパッケージをインストールする必要があります。
OB2-SAPP	SAP用統合ソフトウェアコンポーネント
OB2-VMWP	VMware用統合ソフトウェアコンポーネント
OB2-SAPDBP	SAP DB用統合ソフトウェアコンポーネント
OB2-INFP	Informix用統合ソフトウェアコンポーネント
OB2-LOTP	Lotus Notes/Domino用統合ソフトウェアコンポーネント
OB2-SYBP	Sybase用統合ソフトウェアコンポーネント
OB2-OR8P	Oracle用統合ソフトウェアコンポーネント
OB2-DB2P	DB2用統合ソフトウェアコンポーネント
OB2-EMCP	EMC Symmetrix用統合ソフトウェアコンポーネント
OB2-SMISAP	HP StorageWorks P6000 EVA SMI-S Agentコンポーネント
OB2-SSEAP	HP StorageWorks P9000 XP Agentコンポーネント
OB2-NDMPP	NDMP Media Agentソフトウェア

OB2-OVP	HP NNM用統合ソフトウェアコンポーネント
OB2-FRAP	フランス語版マニュアル(ガイド、ヘルプ)パッケージ
OB2-JPNP	日本語版マニュアル(ガイド、ヘルプ)パッケージ
OB2-CHSP	簡体字中国語版マニュアル(ガイド、ヘルプ)パッケージ
OB2-DOCSP	英語版マニュアル(ガイド、ヘルプ)パッケージ
OB2-PEGP	PEGASUSパッケージ
OB2-VLSAMP	VLS-AMパッケージ

全インストールパッケージのリストおよび依存関係については、表10(260ページ)を参照してください。

Installが終了すると、UNIX用のソフトウェアデポは、/opt/omni/databases/vendorディレクトリに配置されます。

重要:

ネットワーク上にUNIX用のインストールサーバーをインストールしない場合は、SolarisおよびLinuxインストールDVD-ROMを使用して、すべてのUNIXクライアントをローカルにインストールする必要があります。

重要:

Data Protectorは、たとえば次のようなリンクディレクトリにインストールすることができます。

/opt/omni/ -> /prefix/opt/omni/

/etc/opt/omni/ -> /prefix/etc/opt/omni/

/var/opt/omni/ -> /prefix/var/opt/omni/

このようにする場合は、インストール前にリンクを作成しておき、インストール先ディレクトリが存在することを確認しておかなければなりません。

この次に行う作業

この時点で、UNIX用のインストールサーバーがネットワーク上にすでにインストールされていなければなりません。準備が整ったら、以下の作業を実施します。

1. 独立した形で(Cell Managerとは別のシステムに)インストールサーバーをセットアップした場合は、このシステムをData Protectorセルに手動で追加(インポート)する必要があります。「セルへのインストールサーバーのインポート」(216ページ)を参照してください。

注記:

インストールサーバーをインポートすると、Cell Manager上の`/etc/opt/omni/server/cell/installation_servers`ファイルが更新され、インストールされているリモートインストールパケットがリストに表示されます。CLIからこのファイルを使用して、使用可能なリモートインストールパケットを確認できます。このファイルを最新状態に保つために、リモートインストールパケットをインストールまたは削除したときは、インストールサーバーのエクスポートと再インポートを必ず実行してください。これは、インストールサーバーをCell Managerと同じシステムにインストールしてある場合も同様です。

2. Data ProtectorセルにWindowsシステムが含まれている場合は、Windows用のインストールサーバーをインストールする必要があります。前提条件(68ページ)を参照してください。
3. ソフトウェアをクライアントに配布します。「Data Protectorクライアントのインストール」(72ページ)を参照してください。

クライアントのインストール

Cell Managerやインストールサーバーのインストール中には、クライアントはインストールされません。`omnisetup.sh`を使用するか、Data Protector GUIからコンポーネントをリモートでインストールして、クライアントをインストールする必要があります。クライアントのインストール方法の詳細については、「Data Protectorクライアントのインストール」(72ページ)を参照してください。

ネイティブツールを使用したHP-UX、Solaris、およびLinuxシステムでのアップグレード

swinstallを使用したHP-UXシステムでのData Protectorのアップグレード

Cell Managerのアップグレードは、HP-UXインストールDVD-ROMから実行する必要があります。

インストールサーバーもインストールされているCell Managerをアップグレードする場合には、最初にCell Managerをアップグレードし、次にインストールサーバーをアップグレードする必要があります。

Cell Managerシステムにインストールされているクライアントコンポーネントは、Cell Managerのアップグレード中にはアップグレード*されません*。omnisetup. shを使用するか、インストールサーバーからコンポーネントをリモートでインストールして、アップグレードする必要があります。詳細は、「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)または「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

アップグレード手順

Data Protector A.06.00、A.06.10、またはA.06.11をData Protector 6.20にアップグレードするには、swinstallを使用し、以下の手順に従ってください。

1. rootでログインし、/opt/omni/sbin/omnisv -stopコマンドを実行して、Cell Manager上のData Protectorサービスをシャットダウンします。

   ps -ef | grep omniコマンドを実行して、すべてのサービスがシャットダウンされているかどうかを確認します。ps -ef | grep omniコマンドの出力結果には、Data Protectorサービスは表示されないはずです。

2. Cell Managerやインストールサーバーをアップグレードする場合には、「swinstallを使用したHP-UXシステムへのCell Managerのインストール」(362ページ)や「swinstallを使用したHP-UXシステムへのインストールサーバーのインストール」(368ページ)で説明されている手順に従います。

Install手順では、旧バージョンが自動的に検出され、*選択されたコンポーネントのみが*アップグレードされます。旧バージョンのData Protectorにインストールされていたコンポーネントが選択されなかった場合、そのコンポーネントのアップグレードは実行されません。そのため、アップグレードの必要のあるすべてのコンポーネントを選択しなければなりません。

注記:

同じシステム上でCell Managerとインストールサーバーの両方をアップグレードする場合、[Match what target has]オプションはサポートされません。

pkgaddを使用したSolarisシステムでのData Protectorのアップグレード

Solaris用Cell Managerまたはインストールサーバーをアップグレードする場合は、製品の旧バージョンをアンインストールしてから、新しいバージョンをインストールします。

Cell Managerシステムにインストールされているクライアントコンポーネントは、Cell Managerのアップグレード中にはアップグレードされません。omnisetup.shを使用するか、インストールサーバーからコンポーネントをリモートでインストールして、アップグレードする必要があります。詳細は、「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)または「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

アップグレード手順

Data Protector A.06.00 、A.06.10またはA.06.11をData Protector 6.20にアップグレードするには、pkgaddを使用し、以下の手順に従ってください。

1. rootでログインし、/opt/omni/sbin/omnisv -stopコマンドを実行して、Cell Manager上のData Protectorサービスをシャットダウンします。

   ps -ef | grep omniコマンドを実行して、すべてのサービスがシャットダウンされているかどうかを確認します。ps -ef | grep omniコマンドの出力結果には、Data Protectorサービスは表示されないはずです。

2. pkgrmを使用してData Protectorをアンインストールします。

   このユーティリティでは、構成ファイルおよびデータベースは、現在の状態のまま維持されます。

3. pkginfoコマンドを実行し、旧バージョンのData Protectorのアンインストールが完了していることを確認します。Data Protectorの旧バージョンは表示されないはずです。

   データベースと構成ファイルが存在していることを確認します。以下のディレクトリが存在し、バイナリが含まれているはずです。

   - /opt/omni
   - /var/opt/omni
   - /etc/opt/omni

4. Cell Managerをアップグレードする場合、SolarisおよびLinuxインストールDVD-ROMをドライブに挿入してマウントします。次に、pkgaddを使用して、Cell Managerをインストールします。詳細な手順については、「pkgaddを使用したSolarisシステムへのCell Managerのインストール」(364ページ)を参照してください。

   インストールサーバーをアップグレードする場合、Solaris/Linux用インストールDVD-ROMを挿入してマウントし、インストールサーバーをインストールします。詳細な手順については、「pkgaddを使用したSolarisシステムへのインストールサーバーのインストール」(369ページ)を参照してください。

注記:

Solaris 9またはSolaris 10上でCell Managerをアップグレードした場合は、アップグレード完了後にインストールサーバーを使用してCell Manager上にDisk Agentをリモートインストールします。これにより、汎用のSolaris Disk AgentがSolaris 9 Disk AgentまたはSolaris 10 Disk Agentに置き換えられます。Solaris 10では、Cell Manager上でのMedia Agentのリモートインストールも必要です。「Data Protectorクライアントのリモートインストール」(82ページ)を参照するか、または`ob2install`のマンページを参照してください。

rpmを使用したLinuxシステムでのData Protectorのアップグレード

Linux用Cell Managerまたはインストールサーバーをアップグレードする場合は、製品の旧バージョンをアンインストールしてから、新しいバージョンをインストールします。

Cell Managerシステムにインストールされているクライアントコンポーネントは、Cell Managerのアップグレード中にはアップグレード*されません*。omnisetup.shを使用するか、インストールサーバーからコンポーネントをリモートでインストールして、アップグレードする必要があります。詳細は、「UNIXおよびMac OS Xクライアントのローカルインストール」(146ページ)または「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

アップグレード手順

Data Protector A.06.00、A.06.10、またはA.06.11をData Protector 6.20にアップグレードするには、rpmを使用し、以下の手順に従ってください。

1. rootでログインし、/opt/omni/sbin/omnisv -stopコマンドを実行して、Cell Manager上のData Protectorサービスをシャットダウンします。

   ps -ef | grep omniコマンドを実行して、すべてのサービスがシャットダウンされているかどうかを確認します。ps -ef | grep omniコマンドの出力結果には、Data Protectorサービスは表示されないはずです。

2. rpmを使用してData Protectorをアンインストールします。

   このユーティリティでは、構成ファイルおよびデータベースは、現在の状態のまま維持されます。

3. rpm -qコマンドを実行し、旧バージョンのData Protectorのアンインストールが完了していることを確認します。Data Protectorの旧バージョンは表示されないはずです。

   データベースと構成ファイルが存在していることを確認します。以下のディレクトリが存在し、バイナリが含まれているはずです。

   - /opt/omni
   - /var/opt/omni
   - /etc/opt/omni

4. Cell Managerをアップグレードする場合、SolarisおよびLinuxインストールDVD-ROMをドライブに挿入してマウントします。次に、rpmを使用して、Cell Managerをインストールします。詳細な手順については、rpmを使用したLinuxシステムへのCell Managerのインストールを参照してください。

   インストールサーバーをアップグレードする場合、Solaris/Linux用インストールDVD-ROMを挿入してマウントし、インストールサーバーをインストールします。詳細な手順については、rpmを使用したLinuxシステムへのインストールサーバーのインストールを参照してください。

B システムの準備と保守作業

この付録の内容

この付録では、本来は本書の範囲外ながらも、インストール手順に特に関係のある作業についての情報を説明します。これらの作業には、システムの準備と保守作業が含まれます。

UNIXシステムでのネットワーク構成

UNIXシステムにData Protectorをインストールする際、Data Protector Inetがネットワークサービスとして登録されます。これには通常、次の手順が含まれます。

- Data Protector Inetがリスンするポートを登録するための/etc/servicesファイルの変更。
- システムのinetdデーモンまたはそれに相当するデーモン(xinetd、launchd)のData Protector Inetの登録。

ネットワーク構成を変更すると、初期のData Protector Inet構成が不完全または無効になることがあります。これは、特にインターネットプロトコルバージョン6 (IPv6)ネットワークインタフェースを追加または削除する場合に、IPv6サポートをネットワークサービスに追加するためのシステム固有の設定が原因で発生します。

Data Protector Inet構成を更新するために、dpsvcsetup. shユーティリティが使用できます。このユーティリティは(インストールでも使用され、必要な情報を収集し、それに応じてシステム構成を更新します)、オペレーティングシステムによって、/opt/omni/sbinまたは/usr/omni/binディレクトリにあります。

- Data Protector Inetの構成を更新するには、次のコマンドを実行します。

  dpsvcsetup. sh -update

- Data Protector Inetをネットワークサービスとして登録するには、次のコマンドを実行します。

  dpsvcsetup. sh -install

- Data Protector Inetのネットワークサービスとしての登録を解除するには、次のコマンドを実行します。

```
dpsvcsetup.sh -uninstall
```

TCP/IP設定をチェックする

TCP/IP プロトコルは、ホスト名を正しく解決できるようにセットアップする必要があります。ネットワーク内の各システムは、Cell Managerのアドレス、およびMedia Agentと物理メディアデバイスが接続されたすべてのクライアントのアドレスを解決できなければなりません。Cell Managerは、セル内のすべてのクライアントの名前を解決できる必要があります。

TCP/IPプロトコルのインストール後、pingコマンドおよびipconfig/ifconfigコマンドを使ってTCP/IP構成を確認できます。

一部のシステムでは、pingコマンドはIPv6アドレスに使用できません。その場合は、代わりにping6コマンドを使用します。

1. コマンドラインで、次のコマンドを実行します。

   Windowsシステムの場合:ipconfig /all

   UNIXシステムの場合:ifconfig *interface*、ifconfig -a、nestat -iのいずれか(システムによって異なります)

   TCP/IP構成に関する詳細情報、およびネットワークアダプタに設定されているアドレスが表示されます。IPアドレスとサブネットマスクが正しく設定されていることを確認してください。

2. ping *your_IP_address*と入力して、ソフトウェアのインストールおよび構成を確認します。デフォルトでは、4つのエコーパケットが表示されます。

3. ping *default_gateway*と入力します。

   サブネット上ではゲートウェイが動作している必要があります。ゲートウェイへのpingに失敗した場合は、ゲートウェイのIPアドレスが正しいかどうか、およびゲートウェイが動作しているかどうかを確認してください。

4. 上記の各チェックで問題がなければ、名前の解決メカニズムをテストします。システム名を指定してpingコマンドを実行し、hostsファイルとDNSの一方または両方をテストしてください。マシン名がcomputer、ドメイン名がcompany.comの場合は、次のように入力します。ping computer.company.com.

   このコマンドが動作しない場合は、TCP/IPプロパティのウィンドウでドメイン名が正しいかどうかを確認します。hostsファイルとDNSもチェックする必要があります。Cell Managerとなるシステムおよびクライアントとなるシステムに対して、以下の2つの方法で、名前が正しく解決されることを確認してください。

   - Cell Managerから各クライアントに対して、pingコマンドを実行します。
   - 各クライアントから、Cell Manager と、Media Agentがインストールされている他のクライアントに対して、pingコマンドを実行します。

注記:

名前の解決にhostsファイルを使用する場合、前述のテストでは、名前の解決が正しく動作しているかどうかは保証されません。このような場合は、Data Protectorのインストール後にDNSチェックツールを使用する方法があります。

重要:

前述の方法で名前が解決されなかった場合は、Data Protectorが適切にインストールされていない可能性があります。

また、Windowsのコンピュータ名がホスト名と同じである必要があります。同じ名前でない場合は、Data Protectorをセットアップする際、警告が表示されます。

5. Data Protectorをインストールし、Data Protectorセルを作成した後、DNSチェックツールを使用して、Cell Manager、およびMedia Agentがインストールされている各クライアントから、同じセル内の他のすべてのクライアントへのDNS接続、およびその逆のDNS接続が解決されるかどうかを確認できます。この確認を行うには、Data_Protector_home¥binディレクトリからomnicheck -dnsコマンドを実行します。失敗したチェックとその合計数が表示されます。

   omnicheckコマンドの詳細については、『*HP Data Protector Command Line Interface Reference*』を参照してください。

デフォルトのポート番号の変更

Data Protectorのデフォルトのポート番号の変更

Data Protector Inetサービス(プロセス)は、バックアップと復元に必要な他のプロセスを起動するサービスですが、セル内の各システムで同じポート番号を使用する必要があります。

デフォルトでは、Data Protectorはポート番号5555を使用します。このポート番号が別のプログラムに使用されていないことを確認するには、/etc/servicesを参照してください。 servicesファイルファイルservices ファイルの内容を調べるか(UNIXの場合)、または、netstat -anetstatコマンドコマンドnetstat コマンド(Windowsシステムの場合)を実行する必要があります。ポート番号 5555が他のプログラムに使用されている場合は、他の未使用のポート番号に変更する必要があります。このポート番号がクライアントシステム上でのみ使用不能な場合は、Cell Managerをインストールした後でポート番号を変更できます。Cell Managerのインストール先となるシステムでこのポート番号が使用不能な場合は、インストール前にポート番号を変更する必要があります。

UNIXの場合

UNIXシステムでポート番号を変更するには、以下の手順に従ってください。

- Cell Managerをインストールする前に、以下の手順を実行します。

  必要なポート番号で、/tmp/omni_tmp/socket.datファイルを作成します。

- Cell Managerをインストールした後で、以下の手順を実行します。

  1. /etc/servicesファイルを編集します。このファイルには、デフォルトで次のエントリが含まれています。

     ```
     omni 5555/tcp # DATA-PROTECTOR
     ```

     番号 5555を未使用のポート番号に変更します。

  2. /etc/opt/omni/client/customize/socketファイルと/opt/omni/newconfig/etc/opt/omni/client/customize/socketファイルがシステム上に存在する場合は、その内容を必要なポート番号に更新します。

  3. kill -HUP *inetd_pid*コマンドを使用して関連プロセスを終了することによって、Inetサービスを再起動します。プロセスID(*inetd_pid*)を特定するには、ps -efと入力します。

  4. グローバルオプションファイルで、Port変数に新しい値を設定します。

5. Data Protectorサービスを再起動します。

   /opt/omni/sbin/omnisv stop

   /opt/omni/sbin/omnisv start

Windowsの場合

Windowsシステムでポート番号を変更するには、以下の手順に従ってください。

- Cell Managerをインストールする前に、以下の手順を実行します。
  1. コマンドラインからregeditを実行して、レジストリエディタを開きます。
  2. レジストリエントリInetPortを、HKEY_LOCAL_MACHINE¥SOFTWARE¥Hewlett-Packard¥ OpenView¥OmniBackII¥Commonのキーで作成します。

     レジストリエントリの名前:InetPort

     レジストリエントリの種類:REG_SZ(文字列)

     レジストリエントリの値:*port_number*

- Cell Managerをインストールした後で、以下の手順を実行します。
  1. コマンドラインからregeditを実行して、レジストリエディタを開きます。
  2. [**HKEY_LOCAL_MACHINE**]、[**SOFTWARE**]、[**Hewlett-Packard**]、[**OpenView**]、[**OmniBack**]の順に展開し、[**Common**]を選択します。
  3. [**InetPort**]をダブルクリックして、[文字列の編集]ダイアログボックスを開きます。[値のデータ]テキストボックスに未使用のポート番号を入力します。CommonフォルダのParametersサブフォルダについても同様の手順を繰り返します。
  4. Windows コントロールパネルの[管理ツール] - [サービス]から、[**Data Protector Inet**]サービスを選択し、サービスを再起動します(ツールバーの[**サービスの再起動**]アイコンをクリックします)。

Novell NetWare

Novell NetWareシステムでポート番号を変更するには、以下の手順に従ってください。

1. セル内でData Protectorセッションが実行していないことを確認してください。
2. Novell NetWareコンソールから、コマンドUNLOAD HPINETを実行します。
3. AUTOEXEC.NCFファイルを開き、次の行を探します。

   LOAD HPINET.NLM -PORT 5555

   エントリ5555を未使用のポート番号に変更します。

4. SYS:¥ETC¥SERVICESファイルを開き、次の行を追加します。

   omni PortNumber/tcp

   PortNumberは、手順3で使用したポート番号と同じでなければなりません。

5. Novell NetWareコンソールから、コマンドWS2_32 RELOAD SERVICESを実行し、もう一度ファイルSYS:¥ETC¥SERVICESが読み取られるようにします。

6. コマンドLOAD HPINETを実行してHPINETを再ロードします。

Java GUIのデフォルトのポート番号の変更

Java GUI Serverのポート番号(デフォルトで、5556)を変更するには、以下の手順に従ってください。

1. JGUI_BBC_SERVER_PORT変数をomnircファイルにコピーし、その変数の値を使用されていないポート番号に設定します。

   例:

   JGUI_BBC_SERVER_PORT=5557

2. Data Protectorサービスを再起動します。

   omnisv -stop

   omnisv -start

Java GUI Clientは、UIProxyサービスに接続するため、同じポートを使用する必要があります。

Cell Managerに接続するときは、**[Cell Managerに接続する]**ダイアログボックスに*CellManagerName:PortNumber*を入力し、**[接続]**をクリックします。

例:

mycellmanager:5557

Data ProtectorインストールのためのWindows Server 2008上で実行するMicrosoftサーバークラスターの準備

Windows Server 2008上でMicrosoft Cluster Service (MSCS)が実行されているサーバークラスターに、クラスター対応のData Protector Cell ManagerまたはData Protectorクライアントをインストールできるようにするには、事前にクラスターを準備する必要があります。クラスターの準備をしていない場合、ディザスタリカバリの準備でバックアップが必要な

ローカルのCONFIGURATIONオブジェクトのバックアップセッションに失敗し、データの損失が発生する可能性があります。

前提条件

- ドメインのユーザーアカウントでシステムにログオンしていることを確認します。このドメインユーザーアカウントは、ローカルのAdministratorsグループのメンバーでなければなりません。

準備の手順

Data Protectorインストールのためにクラスターを適切に準備するには、以下の手順を実行します。

1. 両方のクラスターノードで、Windowsファイアウォールを開始し、ファイルとプリンタの共有の例外を有効にします。
2. アクティブなクラスターノード上で、[フェールオーバークラスターの管理]を開始し、クォーラムリソース内の監視ディスクがオンラインになっていることを確認します。リソースがオフラインになっている場合はオンラインにします。

   以下の手順を、アクティブなクラスターノード上のみで実行します。
3. マジョリティノードセット(MNS)が構成されていないクラスターを準備する場合は、Windowsエクスプローラを起動して、WitnessDiskLetter:¥Clusterフォルダの所有者をローカルのAdministratorsグループに変更します。[Clusterのセキュリティの詳細設定]ウィンドウで所有者を変更する際は、必ず**[サブコンテナとオブジェクトの所有者を置き換える]**オプションをオンにしてください。[Windowsセキュリティ]ダイアログボックスで、操作を確認して**[はい]**をクリックし、その後に表示される通知を確認して**[はい]**をクリックします。
4. MNSが構成されていないクラスターを準備する場合は、WindowsエクスプローラでWitnessDiskLetter:¥Clusterフォルダのアクセス許可を変更して、SYSTEMおよびローカルのAdministratorsグループのフルコントロールを許可します。両方のグループのアクセス許可設定が、図56(392ページ)で示す設定と一致することを確認してください。

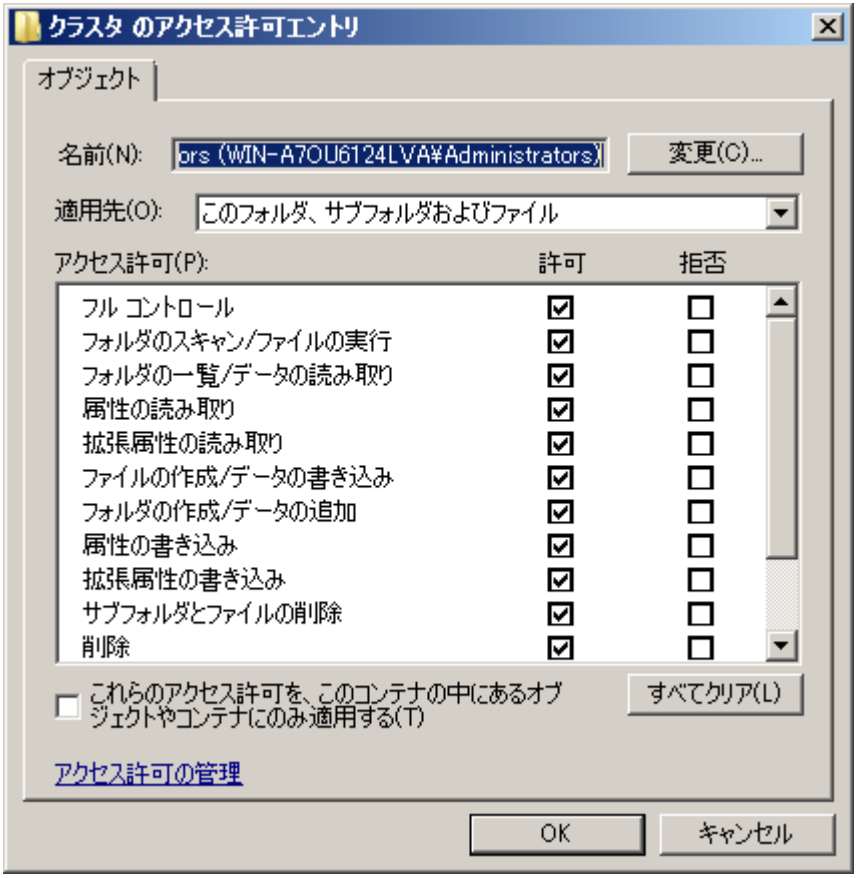


図 56 ClusterフォルダおよびAdministratorsローカルユーザーグループのアクセス許可エントリの修正

5. Data Protector Cell Managerとして使用するクラスターを準備する場合は、[フェールオーバークラスターの管理]で[クラスターアクセスポイント]リソースを追加します。**[リソースの追加]**を選択し、**[1クライアントアクセスポイント]**をクリックして,新しいリソースウィザードを開始します。
   a. [クライアントアクセスポイント]ペインで、[名前]テキストボックスに仮想サーバーのネットワーク名を入力します。
   b. [アドレス]テキストボックスに仮想サーバーのIPアドレスを入力します。
6. Data Protector Cell Managerとして使用するクラスターを準備する場合は、[フェールオーバークラスターの管理]でクラスターに共有フォルダを追加します。**[共有フォルダの追加]**をクリックして共有フォルダの準備ウィザードを開始します。

a. [共有フォルダの場所]ペインで、[場所]テキストボックスにディレクトリパスを入力します。選択したディレクトリに、Data Protectorインストールで作成されるデータを保存するための十分な空き領域があることを確認してください。**[次へ]**をクリックします。

b. [NTFSアクセス許可]、[共有プロトコル]、[SMB設定]の各ペインで、オプションの値をデフォルトのまま変更しないでおきます。**[次へ]**をクリックして次のペインに進みます。

c. [SMBアクセス許可]ペインで、**[Administratorsがフルコントロールを持ち、他のすべてのユーザーとグループは読み取りと書き込みのみのアクセス権を持つ]**オプションを選択します。**[次へ]**をクリックします。

d. [DFS名前空間への発行]で、オプションの値をデフォルトのままにします。**[次へ]**をクリックします。

e. [設定の確認と共有の作成]ペインで、**[作成]**をクリックします。

Veritas Volume ManagerがインストールされたMicrosoft Cluster ServerへのData Protectorのインストール

Veritas Volume ManagerがインストールされたMicrosoft Cluster Server (MSCS)にData Protectorをインストールするには、まずMSCSにData Protectorをインストールする一般的手順を実行します。「Microsoft Cluster ServerへのData Protectorのインストール」(195ページ)を参照してください。

Installが完了したら、Data Protector Inetサービスを有効にして、Microsoftのリソースドライバではなく専用のリソースドライバを使用しているローカルおよびクラスターディスクリソースと、そうではないディスクリソースを区別するために、追加作業がいくつか必要となります。

1. Cell Manager上で、omnisv -stopコマンドを実行して、Data Protectorサービスおよびプロセスを停止します。

   ```
   Data_Protector_home¥bin¥omnisv -stop
   ```

2. 新しいシステム環境変数OB2CLUSTERDISKTYPESの値をVolume Manager Disk Groupとして定義するか、両方のクラスターノード上でomnirc変数を以下のように設定します。

   OB2CLUSTERDISKTYPES=Volume Manager Disk Group

   NetRAID4ディスクなど、独自のディスクリソースを追加指定する場合は、単純に、リソースの種類の名前をOB2CLUSTERDISKTYPES環境変数の値に追加します。

   OB2CLUSTERDISKTYPES=Volume Manager Disk Group;NETRaid4M Diskset

   omnircファイル変数の使用に関する詳細は、『*HP Data Protectorトラブルシューティングガイドトラブルシューティングガイド*』を参照してください。

3. omnisv -startコマンドを実行して、サービス/プロセスを起動します。

   Data_Protector_home¥bin¥omnisv -start

NISサーバーの準備

ここでは、NISサーバーにData Protector Cell Managerを認識させるための手順を説明します。

NISサーバーにData Protectorの情報を追加するには、以下の手順に従ってください。

1. NISサーバーにrootとしてログインします。

2. /etc/servicesファイルをNIS経由で管理する場合は、/etc/servicesファイルに次の行を追加します。

   omni 5555/tcp # Data Protector for Data Protector inet server

   ポート5555を使用できない場合は、5555を別の値に置き換えてください。「Data Protectorのデフォルトのポート番号の変更」(388ページ)を参照してください。

   /etc/inetd.confファイルをNIS経由で管理する場合は、/etc/inetd.confファイルに次の行を追加します。

   #Data Protector

   omni stream tcp nowait root /opt/omni/lbin/inet -log /var/opt/omni/log/inet.log

3. 以下のコマンドを実行します。これによりNISサーバーがファイルを読み込み、構成を更新します。

   cd /var/yp; make

注記:

NIS環境では、複数の異なる構成ファイルを使用する順序を、nsswitch.conf ファイルで定義します。たとえば、/etc/inetd.conf構成ファイルinet.confinet.conf ファイル ファイルをローカルマシン上で使用するか、それともNISサーバーから使用するかを定義できます。また、名前の保持場所をnsswitch.confで制御するように指定するステートメントをファイルに挿入することもできます。詳細は、マンページを参照してください。

Data Protectorをすでにインストールしている場合は、まずNISサーバーを準備し、次にData Protectorクライアントでもあるすべての NISクライアント上でkill -HUP pid コマンドを実行して関連プロセスを停止することにより、inetサービスを再起動します。

トラブルシューティング

- NIS環境にData Protectorをインストールしても Data Protector Inetサービスを開始できない場合は、/etc/nsswitch.confファイルをチェックします。

  次の行が含まれていないか確認してください。

  services:nis [NOTFOUND=RETURN] files

  この行が含まれている場合は、以下のように変更します。

  services:nis [NOTFOUND=CONTINUE] files

Cell Manager名の変更

Data Protectorのインストール時には、Cell Manager名として現在のホスト名が使用されます。Cell Managerのホスト名を変更する場合は、Data Protectorファイルを手作業で更新する必要があります。

重要:

Cell Manager名に関するクライアント情報を更新する必要があります。Cell Managerのホスト名を変更する前に、クライアントをセルからエクスポートしてください。作業手順は、「セルからのクライアントのエクスポート」(220ページ)を参照してください。ホスト名を変更したら、クライアントを再びセルにインポートします。手順の詳細は、「セルへのクライアントのインポート 」(213ページ)を参照してください。

注記：

元のCell Manager名を使用して構成されたデバイスやバックアップ仕様には、現在の名前を反映させる必要があります。

UNIXの場合

UNIX用Cell Managerでは、以下の操作を行ってください。

1. 以下のファイルにあるCell Managerのホスト名のエントリを変更します。

   /etc/opt/omni/client/cell_server

   /etc/opt/omni/server/cell/cell_info

   /etc/opt/omni/server/users/UserList

2. Data Protectorセルのメンバー間で、名前の解決が適切に行われるかどうかを確認します。

3. 以下のコマンドを実行してIDBのCell Manager名を変更します。

   /opt/omni/sbin/omnidbutil -change_cell_name [old_host]

Windowsの場合

Windows用Cell Managerで、以下の操作を行ってください。

1. 以下のファイルにあるCell Managerのホスト名のエントリを変更します。

   Data_Protector_home¥config¥server¥cell¥cell_info Data_Protector_home¥config¥server¥users¥userlist

2. 次のレジストリキーでCell Manager名を変更します。HKEY_LOCAL_MACHINE¥SOFTWARE¥Hewlett-Packard¥ OpenView¥OmniBack¥Site¥CellServer

C デバイスとメディア関連タスク

この付録の内容

この付録では、本来は本書の範囲外となる作業についてのData Protector固有の情報を説明します。これらの作業には、デバイスドライバ構成、SCSIロボティクスの管理、SCSI環境類の保持が含まれます。

Windowsでのテープドライバおよびロボティクスドライバの使用

Data Protectorでは、Windowsシステムに接続された有効なテープドライブ用として、デフォルトでロードされるネイティブテープドライバをサポートしています。ただし、(ロボティクス)デバイス用としてロードされるWindowsのネイティブドライバは、Data Protectorではサポートされていません。

以下の例では、WindowsシステムにHP 4mm DDSテープデバイスが接続されている場合を想定しています。HP 4mm DDSテープデバイスをWindowsシステムに接続してData Protectorで使用できるように構成する場合は、デバイス用にロードされるネイティブドライバを無効化する必要があります。ここでは、関連する手順について説明します。

テープドライバ

Windowsには、ハードウェア互換性リスト(HCL)に記載されているデバイスが、ドライバとして含まれています。HCLとはWindowsでサポートされるデバイスのリストです。詳細は以下のサイトを参照してください。

http://www.microsoft.com/whdc/hcl/default.mspx

コンピュータが起動すると、デバイスドライバは使用可能なデバイスすべてに自動的にロードされます。更新はこれで完了です。ネイティブテープドライバを個別にロードする必要はありません。Windowsシステム上でネイティブテープドライバを更新するか置き換える場合は、以下の手順に従ってください。

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[**コンピュータの管理**]をダブルクリックします。[**デバイスマネージャ**]をクリックします。
3. [テープドライブ]を展開します。現在デバイスに接続されているドライバを確認するには、テープドライブ名をマウスの右ボタンでクリックし、[**プロパティ**]をクリックします。
4. [**ドライバ**] タブを選択し、[**ドライバの更新**]をクリックします。現在インストールされているネイティブテープドライバを更新するか、別のドライバに置き換えるかを、ウィザードで指定できます。
5. システムを再起動して変更を適用します。

重要:

ドライバがネイティブテープドライバを使用しないでData Protector用として構成されている場合は、そのテープドライブを参照しているすべての構成済みData Protectorバックアップデバイス名を変更する必要があります。たとえば、`scsi1:0:4:0`**から**`tape3:0:4:0`**のような変更が必要になります。**

詳細は、「Windows上でのデバイスファイル(SCSIアドレス)の作成」(400ページ)を参照してください。

ロボティクスドライバ

Windowsでは、使用可能なテープライブラリに対するロボディクスドライバが 自動的にロードされます。Data Protectorでライブラリロボティクスを使用するには、対応するドライバを無効化する必要があります。

ここでは、4mm DDSテープを使用するHP 1557Aテープライブラリを例に取り上げます。Windowsシステムで自動的にロードされるロボティクスドライバ(ddsmc.sys)を無効にするには、以下の手順に従ってください。

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[**コンピュータの管理**]をダブルクリックします。[**デバイスマネージャ**]をクリックします。
3. [デバイスマネージャ]ウィンドウの結果エリアで、[メディアチェンジャ]を展開します。

4. 現在ロードされているドライバを確認するには、[**4mm DDSメディアチェンジャ**] マウスの右ボタンでクリックし、[**プロパティ**]をクリックします。

[**ドライバ**] タブを選択し、[**ドライバの詳細**]をクリックします。以下のウィンドウが表示されます。

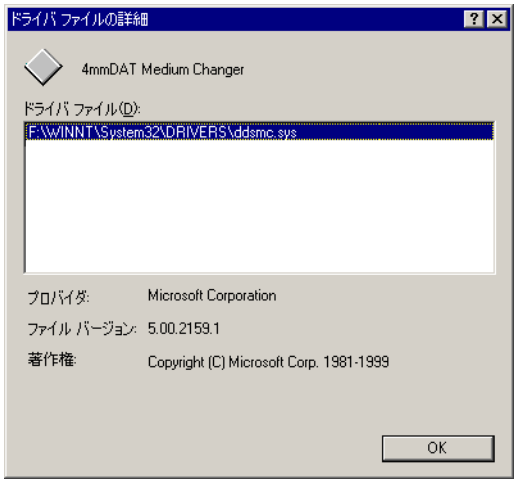


図 57 メディアチェンジャのプロパティ

ネイティブロボティクスドライバを無効にするには、[**4mm DDSメディアチェンジャ**]をマウスの右ボタンでクリックし、[**無効**]を選択してください。

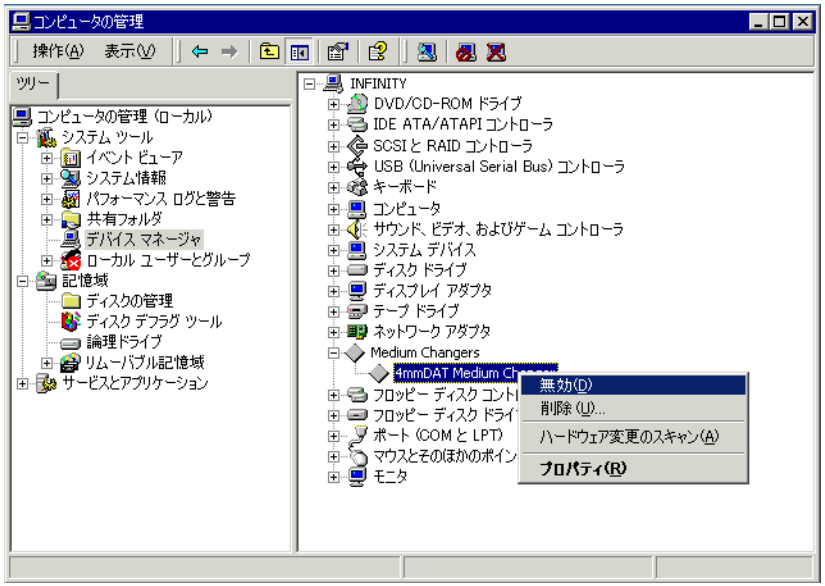


図 58 ロボティクスドライバの無効化

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用に構成できるようになります。

Windows上でのデバイスファイル(SCSIアドレス)の作成

テープデバイスファイル名の構文は、ネイティブテープドライバをテープドライブに対してロード(tapeN:B:T:L)またはアンロード (scsiP:B:T:L) するかによって異なります。

ネイティブテープドライバを使用するWindows

Windowsシステムに接続され、ネイティブテープドライバを使用するテープドライブに対してデバイスファイルを作成するには、以下の手順に従ってください。

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。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。
3. ネイティブテープドライバ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。または、プロパティページの[デバイス情報]で関連する情報を確認することができます。図59(401ページ)を参照してください。

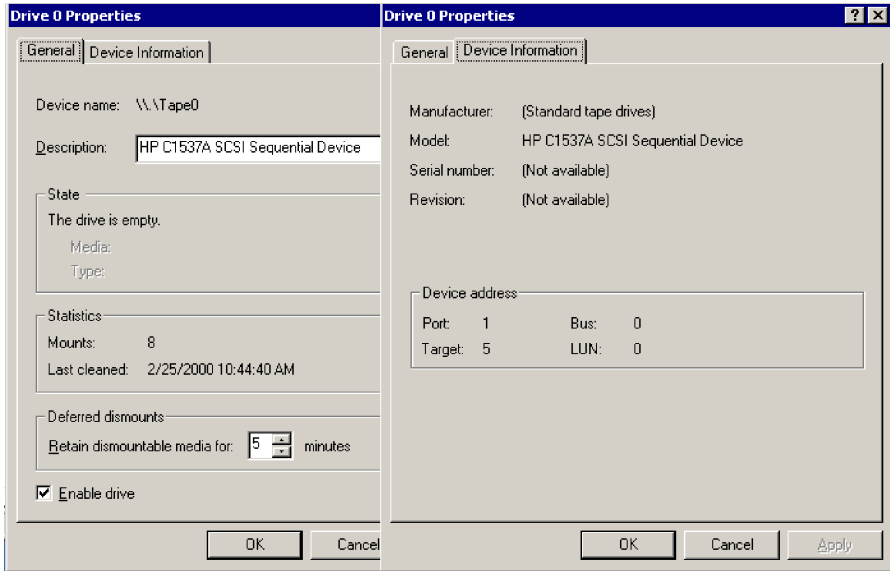


図 59 テープドライブプロパティ

図59(401ページ)のテープドライブのファイル名は、以下のように作成されます。

ネイティブテープドライバを使用している場合	Tape0または Tape0:0:5:0
ネイティブテープドライバを使用していない場合	scsii1:0:5:0

光磁気デバイス

Windowsシステムに光磁気デバイスを接続する場合、ドライブ名は、システムを再起動した後でデバイスに割り当てられます。デバイスファイルを作成した際は、このドライブ名が使用されます。たとえば、E:は、ドライブ文字Eに割り当てられている磁気光デバイス用に作成されたデバイスファイルです。

HP-UX上のSCSIロボティクス構成

HP-UXシステムでは、SCSIパススルードライバを使ってテープライブラリデバイス(HP StorageWorks 12000e など)のSCSIコントローラと制御デバイスの両方を管理します(なお制御デバイスは「ロボティクス」または「ピッカー」とも呼ばれます)。ライブラリの制御デバイスは、ライブラリ内の個々のドライブに対するメディアのロードとアンロード、および、ライブラリデバイスに対するメディアのインポートとエクスポートを制御します。

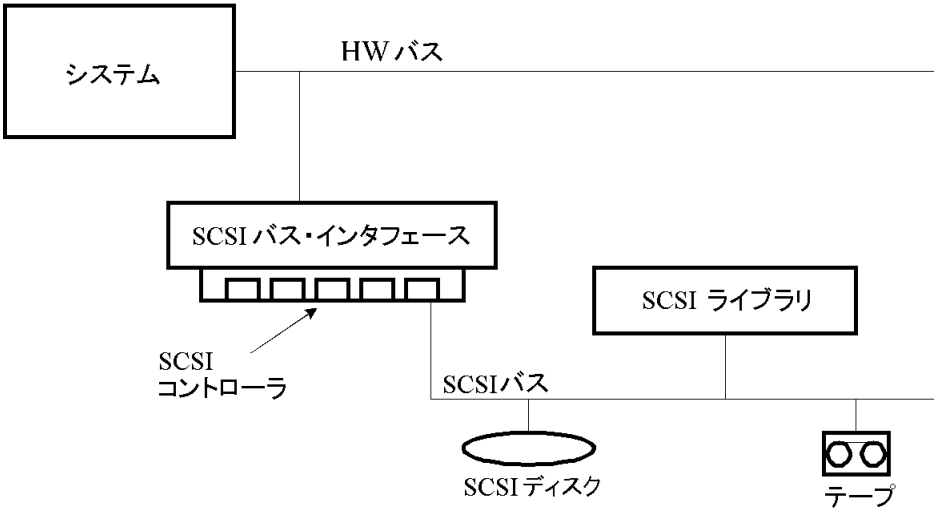


図 60 SCSI 制御デバイス

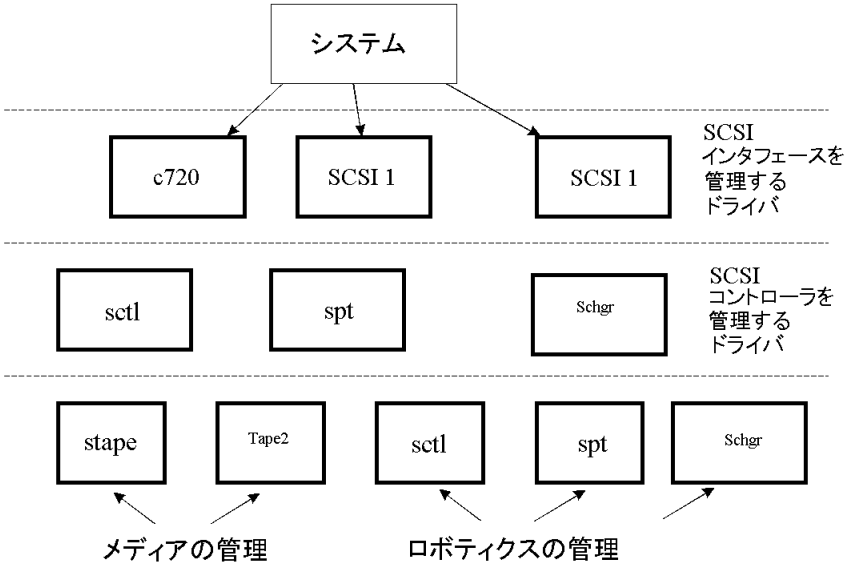


図 61 デバイスの管理

使用されるSCSIロボティクスドライバの種類は、ハードウェアに応じて使い分けます。GSC/HSCまたはPCI バスを搭載しているシステムの場合は、SCSIオートチェンジャドライバschgrが、EISAを搭載しているシステムの場合はSCSIパススルードライバsctlが、それぞれ事

前にカーネルに組み込まれています。ただし、NIOバスを搭載したHPサーバーの場合は、sptという名前のSCSIパススルードライバを使用します。このドライバは、デフォルトでシステムにインストールされていますが、カーネルには組み込まれていません。

SCSIロボティクスドライバがカレントカーネルにまだリンクされていない場合は、手作業で追加して、接続されているテープライブラリのロボティクスに割り当てる必要があります。

SCSIロボティクスドライバを手作業でカーネルに追加して再ビルドするには、以下の手順に従ってください。

ヒント：

HP-UXプラットフォームでは、*HP System Administration Manager (SAM)*ユーティリティを使用してカーネルをビルドすることもできます。第2章の「HP-UXクライアントのインストール」(99ページ)を参照してください。

目的のライブラリにSCSIロボティクスドライバがすでに割り当てられているかどうかをチェックするには、/opt/omni/sbin/ioscan -fコマンドを 使います。

```
root@superhik$ ioscan -f
Class        I  H/W Path     Driver       S/W State H/W Type  Description
==========================================================================
bc           0               root         CLAIMED   BUS_NEXUS
bc           1  8            ccio         CLAIMED   BUS_NEXUS I/O Adapter
unknown     -1  8/0                       CLAIMED   DEVICE    GSC-to-PCI Bus Bridge
ext_bus      0  8/12         c720         CLAIMED   INTERFACE GSC Fast/Wide SCSI Interfac
e
target       0  8/12.0       tgt          CLAIMED   DEVICE
disk         0  8/12.0.0     sdisk        CLAIMED   DEVICE    SEAGATE ST19171W
target       1  8/12.1       tgt          CLAIMED   DEVICE
tape         5  8/12.1.0     stape        CLAIMED   DEVICE    QUANTUM DLT7000
target       2  8/12.2       tgt          CLAIMED   DEVICE
ctl          0  8/12.2.0     sctl         CLAIMED   DEVICE    EXABYTE EXB-210
target       3  8/12.7       tgt          CLAIMED   DEVICE
ctl          0  8/12.7.0     sctl         CLAIMED   DEVICE    Initiator
ba           0  8/16         bus_adapter  CLAIMED   BUS_NEXUS Core I/O Adapter
ext_bus      2  8/16/0       CentIf       CLAIMED   INTERFACE Built-in Parallel Interface
audio        0  8/16/1       audio        CLAIMED   INTERFACE Built-in Audio
tty          0  8/16/4       asio0        CLAIMED   INTERFACE Built-in RS-232C
ext_bus      1  8/16/5       c720         CLAIMED   INTERFACE Built-in SCSI
target       4  8/16/5.2     tgt          CLAIMED   DEVICE
disk         2  8/16/5.2.0   sdisk        CLAIMED   DEVICE    TOSHIBA CD-ROM XM-5401TA
target       7  8/16/5.3     tgt          NO_HW     DEVICE
tape         3  8/16/5.3.0   stape        NO_HW     DEVICE    SONY     SDX-300C
target       6  8/16/5.5     tgt          NO_HW     DEVICE
tape         0  8/16/5.5.0   stape        NO_HW     DEVICE    SONY     SDX-300C
target       5  8/16/5.7     tgt          CLAIMED   DEVICE
```

図 62 SCSIパススルードライバ(sctl)のステータス

図62(403ページ)では、SCSIパススルードライバsctlがExabyteテープデバイスの制御デバイスに割り当てられています。対応するハードウェアパス(H/W Path)は8/12. 2. 0です。(SCSI=2, LUN=0)

同じSCSIバスに接続されているテープドライブがありますが、このテープドライブを制御しているドライバはstapeです。対応するハードウェアパス(H/W Path)は8/12. 1. 0です。(SCSI=0, LUN=0)

重要:

SCSIアドレス7はSCSIコントローラが常時使用しています。ただし、ioscan -fコマンドによる出力には、それを示す行は表示されません。上記の例では、SCSIコントローラはsctlによって管理されています。

```
# ioscan -f
Class       I  H/W Path  Driver    S/W State H/W Type  Description
===================================================================
bc          0            root      CLAIMED   BUS_NEXUS
ext_bus     0  52        scsi1     CLAIMED   INTERFACE HP 28655A - SCSI Interface
target      4  52.1      target    CLAIMED   DEVICE
disk        4  52.1.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      1  52.2      target    CLAIMED   DEVICE
disk        0  52.2.0    disc3     CLAIMED   DEVICE    TOSHIBA CD-ROM XM-4101TA
target      3  52.4      target    CLAIMED   DEVICE
tape        0  52.4.0    tape2     CLAIMED   DEVICE    HP       C1533A
spt         1  52.4.1    spt       CLAIMED   DEVICE    HP       C1553A
target      6  52.5      target    CLAIMED   DEVICE
disk        5  52.5.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      2  52.6      target    CLAIMED   DEVICE
disk        1  52.6.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
lanmux      0  56        lanmux0   CLAIMED   INTERFACE LAN/Console
tty         0  56.0      mux4      CLAIMED   INTERFACE
lan         0  56.1      lan3      CLAIMED   INTERFACE
lantty      0  56.2      lantty0   CLAIMED   INTERFACE
processor   0  62        processor CLAIMED   PROCESSOR Processor
memory      0  63        memory    CLAIMED   MEMORY    Memory
# 
```

図 63 SCSIパススルードライバsptのステータス

図63(404ページ)に示す例では、ロボティクス付きのテープデバイスが接続されており、SCSIパススルードライバsptによって制御されています。このデバイスは、HP StorageWorks 12000eテープライブラリで、SCSIアドレス4を割り当てられており、ハードウェアパス52でSCSIバスに接続されています。対応するハードウェアパスは52.4.1です。ロボティクスには、SCSIパススルードライバsptが正しく割り当てられています。

sctl、spt、またはschgrのドライバがロボティクスに割り当てられていない場合は、ロボティクスのH/W Pathをsystemファイルのドライバステートメントに追加し、カーネルを再ビルドする必要があります。以下の手順に従ってください。

以下は、SCSIロボティクスドライバを*手作業*でカーネルに追加してロボティクスに割り当て、カーネルを手作業で再ビルドする手順を説明したものです。

1. *root*ユーザーとしてログインし、以下のディレクトリに移動します。

   cd /stand/build

2. 次のコマンドを実行して、既存のカーネルから新しいシステムファイルを作成します。

   /usr/lbin/sysadm/system_prep -s system

3. どのSCSIロボティクスドライバが、カレントカーネルに組み込まれているかをチェックします。/standディレクトリから、以下のコマンドを入力してください。

   grep *SCSI Robotic Driver*system

   ここで、SCSI Robotic Driverにはspt、sctl、またはschgrを指定します。ドライバがカレントカーネルにすでに組み込まれている場合は、対応する行が表示されます。

4. エディタを使って、/stand/build/systemファイルに以下のドライバステートメントを追加します。

   driver H/W Path spt

   /stand/build/systemファイルに追加するステートメントのH/W Pathには、デバイスの完全なハードウェアパスを指定します。

   HP StorageWorks 12000eテープライブラリの場合には、以下のように入力します。

   driver 52.4.1 spt

   同じシステムに複数のライブラリが接続されている場合は、それぞれのライブラリロボティクスについて、適切なハードウェアパスを指定するドライバ行を追加する必要があります。

   schgrドライバを構成する場合は、ドライバステートメントに次の行を追加します。

   schgr

5. mk_kernel -s./systemコマンドを入力して、新しいカーネルをビルドします。

6. 元のシステムファイルを別の名前で保存し、新しいシステムファイルを元のシステムファイルにコピーして上書きします。これにより、新しいシステムファイルの内容が適用されます。

   mv /stand/system /stand/system.prev

   mv /stand/build/system /stand/system

7. 元のカーネルを別の名前で保存し、新しいカーネルを元のカーネルにコピーして上書きします。これにより、新しいカーネルの内容が適用されます。

   mv /stand/vmunix /stand/vmunix.prev

   mv /stand/vmunix_test /stand/vmunix

8. 新しいカーネルから以下のコマンドを入力して、システムを再起動します。

   shutdown -r 0

9. システムを再起動したら、もう一度/usr/sbin/ioscan -fコマンドを実行して、変更内容が適用されていることを確認します。

HP-UX上のデバイスファイルの作成

前提条件

デバイスファイルを作成する前に、バックアップデバイスをシステムに接続しておく必要があります。デバイスが正しく接続されているかどうかをチェックするには、/usr/sbin/ioscan -fコマンドを 使用します。バックアップデバイスに対するデバイスファイルを自動的に作成するには、/usr/sbin/infs -eコマンドを 使用します。

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、システムの初期化処理(ブート処理)中またはinfs -eコマンドの実行後に作成されていない場合は、そのデバイスファイルを手作業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。

ここでは、HP-UXシステムに接続されたHP StorageWorks 12000eライブラリデバイス(ライブラリロボティクス)のデバイスファイルを作成する例を示します。このテープドライブのデバイスファイルは、システムの再ブート後に自動作成されますが、制御デバイスのデバイスファイルは手作業で作成する必要があります。

図63(404ページ)は、HP-UXシステム上でioscan -fコマンドを実行したときに表示されるリストの例を示したものです。

```
# ioscan -f
Class        I  H/W Path  Driver    S/W State H/W Type  Description
=================================================================
bc           0            root      CLAIMED   BUS_NEXUS
ext_bus      0  52        scsi1     CLAIMED   INTERFACE HP 28655A - SCSI Interface
target       4  52.1      target    CLAIMED   DEVICE
disk         4  52.1.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target       1  52.2      target    CLAIMED   DEVICE
disk         0  52.2.0    disc3     CLAIMED   DEVICE    TOSHIBA CD-ROM XM-4101TA
target       3  52.4      target    CLAIMED   DEVICE
tape         0  52.4.0    tape2     CLAIMED   DEVICE    HP       C1533A
spt          1  52.4.1    spt       CLAIMED   DEVICE    HP       C1553A
target       6  52.5      target    CLAIMED   DEVICE
disk         5  52.5.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target       2  52.6      target    CLAIMED   DEVICE
disk         1  52.6.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
lanmux       0  56        lanmux0   CLAIMED   INTERFACE LAN/Console
tty          0  56.0      mux4      CLAIMED   INTERFACE
lan          0  56.1      lan3      CLAIMED   INTERFACE
lantty       0  56.2      lantty0   CLAIMED   INTERFACE
processor    0  62        processor CLAIMED   PROCESSOR Processor
memory       0  63        memory    CLAIMED   MEMORY    Memory
# 
```

図 64 接続済みデバイスのリスト

この例のSCSIバスインタフェースは、scsi1システムドライバによって制御されています。これは、SCSI NIOインタフェースです。SCSI NIOバス上のライブラリロボティクスにアクセスするには、SCSIパススルードライバsptを使用する必要があります。このドライバはすでにインストールされており、HP StorageWorks 12000eテープデバイスのロボティクスに割り当てられています。ハードウェアパスは52.4.1です。

注記:

SCSI NIOベースのバスインタフェースを使用しない場合は、sptドライバではなく、sctlドライバが必要になります。

デバイスファイルを作成するには、SCSIパススルードライバのメジャー番号とマイナー番号を取得しておく必要があります(なお、マイナー番号は、どちらのドライバの場合も共通です)。

sptのメジャー番号を取得するには、以下のシステムコマンドを実行します。

```
lsdev -d spt
```

図64(406ページ)の例の場合、このコマンドを実行すると、メジャー番号75が返されます。

sctlのメジャー番号を取得するには、以下のシステムコマンドを実行します。

```
lsdev -d sctl
```

この場合は、コマンドを実行すると、メジャー番号 203が返されます。

どちらのSCSIパススルードライバの場合も、共通のマイナー番号は以下の形式をとります。

0xIITL00

II -> ioscan -fの出力に示されるSCSIバスインタフェースのインスタンス番号(デバイスそのものの番号ではない)は、リストの二番目の列(Iの列)に表示されます。この例では、インスタンス番号は0なので、2桁の16進数00を入力する必要があります。

T ->ライブラリロボティクスのSCSIアドレス。この例では、SCSIアドレスは4 なので、4を入力します。

L ->ライブラリロボティクスのLUN 番号。この例では、LUN番号は1 なので、 1と入力します。

00 -> 2桁の16進値ゼロ。

デバイスファイルの作成

デバイスファイルは、以下のコマンドで作成します。

```
mknod /dev/spt/devfile_name c Major # Minor #
```

通常、sptのデバイスファイルは/dev/sptまたは/dev/scsiディレクトリに保存します。この例の場合、制御デバイスファイルを/dev/spt/SS12000eという名前で保存します。

/dev/sptディレクトリにSS12000eという名前のデバイスファイルを作成するには、以下のように入力します。

```
mknod /dev/spt/SS12000e c 75 0x004100
```

sct1のデバイスファイルを作成してSS12000eという名前で/dev/scsiディレクトリに保存するには、以下のように入力します。

```
mknod /dev/scsi/SS12000e c 203 0x004100
```

SCSIコントローラのパラメータの設定

Data Protectorでは、デバイスのブロックサイズを変更できますが、一部のSCSIコントローラで64KBを超えるブロックサイズの書き込みを可能にするには、パラメータ設定の変更が必要になる場合があります。

WindowsシステムでAdaptec SCSIコントローラやAdaptecチップセット搭載のSCSIコントローラのパラメータを設定するには、そのコントローラのレジストリ値を編集します。

1. 次のレジストリ値を設定します。HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥ aic78xx¥Parameters¥Device0¥MaximumSGList
2. 4KBサイズのブロックの数に1を加えたDWORD値を入力します。

   MaximumSGList = (OBBlockSize in kB / 4) + 1

   たとえば、260KBまでのブロックサイズを有効にするには、MaximumSGListの値を少なくとも(260 / 4) + 1 = 66に設定します。
3. システムを再起動します。

注記:

このレジストリ値では、ブロックサイズの上限を設定します。デバイスで実際に使用するブロックサイズは、デバイス構成用のData Protector GUIを使って設定する必要があります。

HP-UX上の未使用のSCSIアドレスの取得

HP-UXシステムに接続したバックアップデバイスのアクセスと制御は、デバイスファイルを通じて行い、各物理デバイスに対応するデバイスファイルが必要です。デバイスファイルを作成する前に、新しいデバイスに割り当てることのできる未使用のSCSIアドレス(ポート)を見つける必要があります。

HP-UXでは、/usr/sbin/ioscan -fシステムコマンドを実行して、すでに使用されているSCSIアドレスのリストを表示することができます。/usr/sbin/ioscan -fコマンドの出力リストに含まれていないアドレスは、未使用のアドレスとみなすことができます。

図65(409ページ)は、HP-UX 11.xシステム上で/usr/sbin/ioscan -fコマンドを実行したときに表示されるリストの例を示しています。

```
# ioscan -f
Class        I  H/W Path  Driver    S/W State H/W Type  Description
===================================================================
bc           0            root      CLAIMED   BUS_NEXUS
ext_bus      0  52        scsi1     CLAIMED   INTERFACE HP 28655A - SCSI Interface
target       4  52.1      target    CLAIMED   DEVICE
disk         4  52.1.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target       1  52.2      target    CLAIMED   DEVICE
disk         0  52.2.0    disc3     CLAIMED   DEVICE    TOSHIBA CD-ROM XM-4101TA
target       3  52.4      target    CLAIMED   DEVICE
tape         0  52.4.0    tape2     CLAIMED   DEVICE    HP       C1533A
spt          1  52.4.1    spt       CLAIMED   DEVICE    HP       C1553A
target       6  52.5      target    CLAIMED   DEVICE
disk         5  52.5.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target       2  52.6      target    CLAIMED   DEVICE
disk         1  52.6.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
lanmux       0  56        lanmux0   CLAIMED   INTERFACE LAN/Console
tty          0  56.0      mux4      CLAIMED   INTERFACE
lan          0  56.1      lan3      CLAIMED   INTERFACE
lantty       0  56.2      lantty0   CLAIMED   INTERFACE
processor    0  62        processor CLAIMED   PROCESSOR Processor
memory       0  63        memory    CLAIMED   MEMORY    Memory
#
```

図 65 HP-UXシステム上で実行したioscan -fコマンドの出力

利用可能なSCSIアドレスは、このリストの3番目の列(H/W Path)と5番目の列(S/W State)の値に基づいて調べることができます。3番目の列(H/W Path)の値は、以下の形式で示されます。

SCSI_bus_H/W_Path.SCSI_address.LUN_number

この例の場合、ハードウェアパス52を使用するSCSIバスが1つだけ存在します。このバス上のアドレスのうち、リストに表示されていない0および3が、利用可能なアドレスとなります。

図65(409ページ)に示す例では、SCSIバス上のSCSIアドレスのうち、以下のアドレスがすでに使用されています。

- SCSIアドレス1は、SCSIディスクに使用されています。
- SCSIアドレス2は、CD-ROMに使用されています。
- SCSIアドレス4、LUN 0は、テープドライブに使用されています。
- SCSIアドレス4、LUN 1は、テープライブラリロボティクスに使用されています。
- SCSIアドレス5は、SCSIディスクに使用されています。
- SCSIアドレス6は、SCSIディスクに使用されています。
- SCSIアドレス7は、SCSIコントローラに使用されています。

注記:

リストには、SCSIアドレス7は示されていませんが、これはSCSIコントローラにデフォルトで割り当てられるアドレスです。

どのデバイスについても、S/W State 列にはCLAIMEDと示されており、またH/W Type列にはH/W DEVICEと示されていますが、これはデバイスが現在接続されていることを意味しています。システムからアクセスできないデバイスがある場合は、そのデバイスのS/W State列の値がUNCLAIMEDになり、H/W Type列の値がNO-HWになります。

SCSIアドレス4は、テープライブラリに使用されています。このアドレスのLUN 0はテープドライブに、LUN 1はロボティクスに、それぞれ割り当てられています。このドライブはtape2ドライバによって制御されており、ロボティクスはSCSIパススルードライバsptによって制御されています。説明を見ると、デバイスがHP StorageWorks 12000eライブラリであることが確認できます。このライブラリはテープドライブとロボティックスと同じSCSIアドレスを使用しますが、異なるLUNを使用するため、SCSIライブラリから簡単に見つけることができます。

SCSIバス全体は、scsi1インタフェースモジュールによって制御されています。

Solarisシステム上の未使用のSCSIターゲットIDの取得

Solarisシステムに接続されたバックアップデバイスのアクセスおよび制御は、デバイスファイルを通じて行われます。このデバイスファイルは、バックアップデバイスを接続してクライアントシステムとバックアップデバイスの電源を投入した時点で、Solaris オペレーティングシステムにより/dev/rmtディレクトリに自動的に作成されます。

ただしバックアップデバイスを接続する前に、使用可能なSCSIアドレスを確認し、未割り当てのアドレスをバックアップデバイスに設定するよう注意してください。

Solarisシステム上で使用可能なSCSIアドレスを調べるには、以下の操作を行います。

1. **Stop + A**を押して、システムを停止します。
2. okプロンプトから**probe-scsi-all**コマンドを実行します。

   probe-scsi-all

   ここで、probe-scsi-allコマンドを実行する前に、reset-allコマンドを実行するよう、システムから求められる場合があります。
3. 通常操作に戻るには、ok プロンプトに**go**と入力します。

   go

使用可能なアドレスを調べてバックアップデバイス用のアドレスを選択したら、デバイスを接続して起動する前に、関連する構成ファイルを更新しなければなりません。構成ファイルの更新方法は、次の項を参照してください。

Solarisシステム上でのデバイスおよびドライバ構成の更新

構成ファイルの更新

デバイスおよびドライバの構成には、次の構成ファイルが使用されます。接続されたデバイスを使用する前に、これらのファイルを確認し、必要に応じて編集してください。

- st.conf
- sst.conf

st.conf:すべてのデバイス

このファイル は、テープデバイスが接続された各Data Protector Solarisクライアント上に必要です。ファイル内には、そのクライアントに接続されているすべてのバックアップデバイスに関するデバイス情報とSCSIアドレスが記述されていなければなりません。シングルドライブデバイスについては単一のSCSIエントリが必要で、マルチドライブライブラリデバイスについては複数のSCSIエントリが必要です。

1. 前の項の説明に従ってクライアント上で使われていないSCSIアドレスを調べ、接続するデバイス用のアドレスを選択してください。
2. 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。
3. クライアントシステムの電源を切ります。
4. バックアップデバイスを接続します。
5. 最初にデバイスの電源を投入し、次にクライアントシステムの電源を投入します。
6. Stop + Aを押して、システムを停止します。
7. ok プロンプトから**probe-scsi-all**コマンドを実行します。

   probe-scsi-all

   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。
8. 通常操作に戻るには、次のように入力します。

   go

9. /kernel/drv/st.confファイルを編集します。このファイルはSolaris st (SCSIテープ)ドライバで使用されます。ファイル内には、Solarisが正式にサポートするデバイスの一覧と、サードパーティデバイス用の構成エントリが記述されています。サポート対象のデバイスを使用する場合は、デバイスを接続するだけで、追加の構成作業を行わなくても使用できるはずです。サポート対象外のデバイスについては、次の種類のエントリをst.confファイルに追加しなければなりません。

- テープ構成リストエントリ(およびテープデータの変数定義)。ファイル内には、コメントアウトされた形でエントリ例が記述されています。いずれかのエントリをそのまま使用するか(該当する場合)、必要に応じて変更してください。

  このエントリは、ファイル内の最初のname=エントリよりも前に、次の形式で記述しなければなりません。

  tape-config-list= "Tape unit", "Tape reference name", "Tape data";

  各部分の説明:

Tape unit	テープデバイスのベンダーおよび製品IDを指定します。この文字列は、デバイス製造元のドキュメントに記載されているとおりに正確に指定しなければなりません。
Tape reference name	各自が選択した名前を指定します。システムはこの名前でテープデバイスを識別します。指定した名前によりテープ製品IDが変更されることはありませんが、システムのブート時には、システムにより認識された周辺デバイスの一覧に、この参照名(reference name)が示されます。
Tape data	追加されるテープデバイスの一連の構成項目を参照する変数です。変数定義も、デバイス製造元のドキュメントに記載されているとおりに正確に指定しなければなりません。

  例:

  tape-config-list= “Quantum DLT4000”, “Quantum DLT4000”, “DLT-data”;

  DLT-data = 1,0x38,0,0xD639,4,0x80,0x81,0x82,0x83,2;

2番目のパラメータである0x38は、テープタイプDLTtapeを「その他SCSIドライブ」として指定しています。ここに指定する値は/usr/include/sys/mtio.h内に定義されていなければなりません。

注記:

テープ構成リスト内の最後のエントリの後ろには、必ずセミコロン (;)を付けてください。

- マルチドライブデバイスの場合は、ターゲットエントリは次のようになります。

  name="st" class="scsi"

  target=X lun=Y;

  各部分の説明:

  X データドライブ(またはロボティクス機構)に割り当てるSCSIポートです。

  Y 論理ユニット番号です。

  例:

  name="st" class="scsi"

  target=1 lun=0;

  name="st" class="scsi"

  target=2 lun=0

  通常 st.confファイルには、ドライブ用のターゲットエントリのみを指定する必要があり、別のターゲット上にあるロボティクス機構用のエントリは必要ありません。ロボティクス機構用のエントリは、通常sst.confファイルに指定します(詳細は以下を参照)。ただしHP StorageWorks 24x6などの一部のデバイスでは、ロボティクス機構が他のドライブと同様に取り扱われます。この場合は、同一のターゲットと異なるLUNを指定した2つのエントリ(ドライブ用とロボティクス用に1つずつ)が必要です。

  例:

  name="st" class="scsi"

  target=1 lun=0;

  name="st" class="scsi"

  target=1 lun=1

sst.conf:ライブラリデバイス

このファイル は、マルチドライブライブラリデバイスが接続された各Data Protector Solaris クライアント上に必要です。通常このファイルには、クライアントに接続された各ライブラリデバイスのロボティクス機構のSCSIアドレス用エントリを指定する必要があります。ただし、前の項で説明したように、HP StorageWorks 24x6などの一部の例外もあります。

1. sstドライバ(モジュール)と構成ファイルsst.confを、次のディレクトリにコピーします。
   - 32ビットオペレーティングシステムの場合

     ```
     $cp /opt/omni/spt/sst /usr/kernel/drv/sst
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```

   - 64ビットオペレーティングシステムの場合

     ```
     $cp /opt/omni/spt/sst.64bit /usr/kernel/drv/sparcv9/sst
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```

2. sst.confファイルを開いて、次のエントリを追加します。

   name="sst" class="scsi" target=*X* lun=*Y*;

   各部分の説明:

   X ロボティクス機構のSCSIアドレスを指定します。

   Y 論理ユニットを指定します。

   例:

   ```
   name="sst" class="scsi" target=6 lun=0;
   ```

3. ドライバをSolarisカーネルに追加します。

   ```
   add_drv sst
   ```

デバイスファイルの作成とチェック

構成ファイルの設定とドライバのインストールが終了したら、次の手順に従って新しいデバイスファイルを作成してください。

1. /dev/rmt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。次のコマンドを入力してください。

   ```
   cd /dev/rmt rm *
   ```

2. 次のコマンドを入力してシステムをシャットダウンします。

   ```
   shutdown -i0 -g0
   ```

3. 次のコマンドを入力してシステムを再起動します。

   boot -rv

   bootコマンドにrスイッチを指定すると、カーネルのコンパイルが実行され、テープデバイスとの通信に使われる専用のデバイスファイルが作成されます。またvスイッチを指定することで、システム起動の詳細モード表示が有効化されます。詳細モードを指定した場合は、起動処理の/devicesディレクトリ構成段階で、デバイスが接続されたことを示すために、ユーザーが選択した*Tape reference name*(テープ参照名)文字列が表示されます。

4. 次のコマンドを入力してインストール結果を確認します。

   mt -t /dev/rmt/0 status

   このコマンドの出力は、構成されたドライブにより異なります。およそ以下のようになります。

   Quantum DLT7000 tape drive:sense key(0x6)= Unit Attention residual= 0 retries= 0 file no= 0 block no= 0

5. 再起動が完了したら、コマンドls -allを使用して、作成されたデバイスファイルを確認できます。ライブラリデバイスの場合、このコマンドの出力は次のようになります。

/dev/rmt/0hb	1番目のテープドライブ用
/dev/rmt/1hb	2番目のテープドライブ用
/dev/rsst6	ロボティクスドライブ用

Windowsシステム上の未使用のSCSIターゲットIDの取得

Windowsシステム上で未使用のSCSIターゲットID(アドレス)を調べるには、以下の手順に従ってください。

1. Windowsの[コントロールパネル]で、**[SCSIアダプタ]**をクリックします。
2. SCSIアダプタに接続されているデバイスのリストで、各デバイスのプロパティをチェックします。デバイスの名前をダブルクリックし、**[設定]**をクリックして、プロパティページを開きます。図66(416ページ)を参照してください。

   このページに示されるSCSIターゲットIDとLUN (論理ユニット番号)を確認してください。この方法で、どのSCSIターゲットIDとLUNがすでに使用されているかを調べることができます。

図 66 デバイスの設定

HP StorageWorks 330fxライブラリ上のSCSI IDの設定

ロボティクスおよびドライブに割り当てることのできる未使用のSCSI IDを選択し、ライブラリデバイスのコントロールパネルを使って、ロボティクスとドライブをチェックおよび構成することができます。

例:HP StorageWorks 330fxライブラリを使用する場合は、SCSI IDの構成を以下の手順でチェックできます。

1. READY 状態から[NEXT]を押します。ADMIN*が表示されます。
2. [ENTER]を押し、パスワードプロンプトに対してパスワードを入力します。
3. TEST*が表示されたら、SCSI ID*が表示されるまで[NEXT]を押します。
4. [ENTER]を押します。VIEW IDs*が表示されます。
5. [ENTER]を押します。JKBX ID 6 LUN 0が表示されます。
6. [NEXT]を押します。DRV 1 ID 5 LUN 0が表示されます。
7. [NEXT]を押します。DRV 2 ID 4 LUN 0が表示されます。以下同様に続きます。

READY 状態に戻るには、[CANCEL]を数回押してください。

バックアップデバイスの接続

ここでは、HP-UXシステム、Solarisシステム、Linuxシステム、またはWindowsシステムにバックアップデバイスを接続する際の一般的な手順を示します。

1. バックアップデバイスを接続するクライアントを選択します。
2. 選択したシステムにMedia Agentをインストールします。「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。
3. デバイスに割り当て可能な未使用のSCSIアドレスを調べます。HP-UXシステムについては、「HP-UX上の未使用のSCSIアドレスの取得」(408ページ)を参照してください。Solarisシステムについては、「Solarisシステム上の未使用のSCSIターゲットIDの取得」(410ページ)を参照してください。Windowsシステムについては、「Windowsシステム上の未使用のSCSIターゲットIDの取得」(415ページ)を参照してください。
   - HP-UXシステムにデバイスを接続する場合は、必要なドライバがすでにインストールされており、現在のカーネルに組み込まれていることをチェックします。「HP-UXのカーネル構成のチェック」(100ページ)を参照してください。

     SCSIパススルードライバを構成する必要がある場合は、「HP-UX上のSCSIロボティクス構成」(401ページ)を参照してください。
   - Solarisシステムに接続する場合は、必要なドライバがインストールされており、インストールするデバイスにあわせて構成ファイルが更新されていることを確認してください。「Solarisシステム上でのデバイスおよびドライバ構成の更新」(411ページ)を参照してください。ここでは、sst.confファイルの更新方法についても説明しています。SCSIパススルードライバを構成する場合は、このファイルを更新する必要があります。
   - Windowsクライアントに接続する場合は、Windowsシステムのバージョンにより、ネイティブテープドライバをロードまたは無効化します。「Windowsでのテープドライバおよびロボティクスドライバの使用」(397ページ)を参照してください。

     Data Protector用としてすでに構成されており、ネイティブテープドライバを使用していないデバイスについて、そのデバイスのネイティブテープドライバをロードする場合は、そのデバイスを参照しているすべての構成済み Data Protector 論理デバイスのデバイスファイル名を変更する必要があります。たとえば、scsi1:0:4:0からtape3:0:4:0のような変更が必要です。

     適切なデバイスファイル名の詳細は、「Windows上でのデバイスファイル(SCSIアドレス)の作成」(400ページ)を参照してください。

4. デバイスのSCSIアドレス(ID)を設定します。デバイスの種類にもよりますが、通常はSCSIアドレスをデバイス上のスイッチを使用して設定できます。詳細は、使用するデバイスのマニュアルを参照してください。

   設定例は、「HP StorageWorks 330fxライブラリ上のSCSI IDの設定」(416ページ)を参照してください。

   サポート対象デバイスの詳細は、http://www.hp.com/support/manualsを参照してください。

注記:

AdaptecSCSIアダプタがインストールされており、SCSIデバイスが接続されているWindowsシステムの場合は、システムが正常にSCSIコマンドを実行できるようにHost Adapter BIOSオプションを設定する必要があります。

Host Adapter BIOSオプションを設定するには、システムのブート中にCtrl+Aを押してSCSIアダプタメニューを表示
し、[Configure/View Host Adapter Settings]、[Advanced Configuration Options]を選択して、[Host Adapter BIOS]オプションを有効にします。

5. デバイス、コンピュータの順に電源を投入します。ブート処理が完了するまで待ちます。新しいバックアップデバイスがシステムによって正しく認識されていることを確認します。

- HP-UXシステムの場合は、ioscanユーティリティを以下のコマンドで実行してください。

  /usr/sbin/ioscan -fn

  このコマンドを実行すると、接続済みのデバイスをハードウェアパスおよびデバイスファイルとともに示すリストが出力されます。このリストを調べて、新しいデバイスに正しいSCSIアドレスが割り当てられていることを確認してください。

  デバイスファイルがブート処理中に自動生成されない場合は、手作業で作成する必要があります。「HP-UX上のデバイスファイルの作成」(406ページ)を参照してください。

- Solarisシステム上の/dev/rmtディレクトリで、ls -allコマンドを実行すると、接続済みのデバイスをハードウェアパスおよびデバイスファイルとともに示すリストが出力されます。このリストを調べて、新しいデバイスに正しいSCSIアドレスが割り当てられていることを確認してください。
- Linuxシステム上の/dev/rmtディレクトリで、ls -allコマンドを実行すると、接続済みのデバイスをハードウェアパスおよびデバイスファイルとともに示すリストが出力されます。このリストを調べて、新しいデバイスに正しいSCSIアドレスが割り当てられていることを確認してください。
- Windowsシステムの場合、devbraユーティリティを使用すると、新しいバックアップデバイスが正しく認識されたかどうかを確認できます。Data_Protector_home¥binディレクトリに移動して、次のコマンドを実行します。

  devbra -dev

  devbraコマンドの出力リストでは、接続済みで正しく構成されている各デバイスについて、以下の行が表示されます。

  backup device specification

  hardware_path

  media_type

  .....

  たとえば、以下のようなリストが出力されます。

  HP:C1533A

  tape3:0:4:0

  DDS

  ...

  ...

この例の場合、ドライブインスタンス番号3のHP DDSテープデバイス(ネイティブテープドライバがロードされている状態)がSCSIバス0に接続されており、SCSIターゲットID 4およびLUN番号0が割り当てられています。

以下のようなリストが出力される場合もあります。

```
HP:C1533A
scsi1:0:4:0
DDS
...
...
```

この例の場合、HP DDSテープドライブ(ネイティブテープドライバがアンロードされた状態)がSCSIバス0上のSCSIポート1に接続されており、テープドライブにSCSIターゲットID 4およびLUN 番号 0が割り当てられています。

- AIXシステムの場合は、lsdevユーティリティを以下のコマンドで実行してください。

  ```
  lsdev -C
  ```

  接続されているデバイスと、対応するデバイスファイルについて、リストが表示されます。

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。詳細な手順については、オンラインヘルプを参照してください。

ハードウェア圧縮は、Media Agentクライアントから元のデータを受信したデバイスによって行われ、デバイスは圧縮モードでデータをテープに書き込みます。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るため、テープドライブがデータを受信する速度が向上します。

ソフトウェア圧縮が使用されハードウェア圧縮が無効になっている場合、データはDisk Agentにより圧縮され、圧縮された形でMedia Agentに送信されます。ソフトウェア圧縮を使用した場合は、圧縮アルゴリズムによりDisk Agentシステムのリソースが大量に消費されますが、ネットワークの負荷は軽減されます。

ハードウェア圧縮をWindows上で有効化するには、デバイスやドライブのSCSIアドレスの最後に“C”を追加してください。(例:scsi:0:3:0C [テープドライバ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る場合は、ハードウェア圧縮が使用されます。サポートしていない場合、Cオプションは無視されます。

ハードウェア圧縮をWindows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:0:3:0:N)。

ハードウェア圧縮をUNIX上で有効化/無効化するには、適切なデバイスファイルを選択してください。詳細は、デバイスやオペレーティングシステムのマニュアルを参照してください。

この次に行う作業

ここまでの段階で、バックアップデバイスを正しく接続できたら、次にバックアップデバイスおよびメディアプールを構成します。その他の構成タスクの詳細は、オンラインヘルプの索引「構成、バックアップデバイス」を参照してください。

システム上には、Media Agentをインストールしておく必要があります。手順の詳細は、「Data Protectorクライアントのリモートインストール」(82ページ)を参照してください。

この後の項では、HP StorageWorks Standalone 24テープデバイス、HP StorageWorks 12000eライブラリ、およびHP StorageWorks DLTライブラリ28/48スロットを、それぞれHP-UXシステムまたはWindowsシステムに接続する場合の手順を説明します。

StorageWorks 24スタンドアロンデバイスの接続

StorageWorks 24 DDSバックアップデバイスは、DDS3テクノロジーに基づくスタンドアロンテープドライブです。

HP-UXシステムに接続する場合

HP StorageWorks 24スタンドアロンデバイスをHP-UXシステムに接続するには、以下の手順に従ってください。

1. 必要なドライバ(stapeまたはtape2)がすでに*インストールされており*、カレントカーネルに*組み込まれている*ことをチェックします。「HP-UXのカーネル構成のチェック」(100ページ)を参照してください。
2. テープドライブに割り当て可能な未使用のSCSIアドレスを探します。「HP-UX上の未使用のSCSIアドレスの取得」(408ページ)を参照してください。
3. デバイスのSCSIアドレス(ID)を設定します。デバイス背面のスイッチを使用してください。

   詳細は、使用するデバイスのマニュアルを参照してください。
4. デバイス、コンピュータの順に電源を投入し、ブート処理が完了するまで待ちます。

5. 新しいテープドライブがシステムによって正しく認識されていることを確認します。ioscanユーティリティを以下のコマンドで実行してください。

   /usr/sbin/ioscan -fn

   このコマンドを実行すると、接続済みのデバイスをハードウェアパスおよびデバイスファイルとともに示すリストが出力されます。このリストを調べて、新たに接続したテープドライブに正しいSCSIアドレスが割り当てられていることを確認してください。なお、このドライブのデバイスファイルは、ブート処理中に自動生成されます。

この次に行う作業

デバイスを正しく接続したら、オンラインヘルプの索引「構成、バックアップデバイス」を参照して、新しく接続したデバイスのData Protectorバックアップデバイスを構成する手順を確認してください。

Windowsシステムに接続する場合

HP StorageWorks 24スタンドアロンデバイスをWindowsシステムに接続するには、以下の手順に従ってください。

1. テープドライブに割り当て可能な未使用のSCSIアドレス(ターゲットID)を探します。「Windowsシステム上の未使用のSCSIターゲットIDの取得」(415ページ)を参照してください。
2. デバイスのSCSIアドレス(ID)を設定します。デバイス背面のスイッチを使用してください。詳細は、使用するデバイスのマニュアルを参照してください。
3. デバイス、コンピュータの順に電源を投入します。ブート処理が完了するまで待ちます。
4. 新しいテープドライブがシステムによって正しく認識されていることを確認します。devbraコマンドを Data_Protector_home¥binディレクトリから実行します。以下のように入力してください。

   devbra -dev

   devbraコマンドの出力リストに、HP StorageWorks 24スタンドアロンデバイスのテープドライブが含まれていることを確認してください。

この次に行う作業

デバイスを正しく接続したら、オンラインヘルプの索引「構成、バックアップデバイス」を参照して、新しく接続したデバイスのData Protectorバックアップデバイスを構成する手順を確認してください。

HP StorageWorks DATオートローダーの接続

HP StorageWorks 12000eとStorageWorks DAT24x6の各ライブラリは、6つのカートリッジを格納できるライブラリです。ドライブとロボティクスアームを1つずつ備えています。アームによって、ドライブ上のカートリッジが交換されます。また、ダーティテープ検出機能も組み込まれています。

HP-UXシステムに接続する場合

HP StorageWorks 12000eライブラリデバイスをHP-UXシステムに接続するには、以下の手順に従ってください。

1. オートローダーの裏側のモードスイッチを6に設定してください。
2. 必要なドライバ(stapeまたはtape2)がすでに*インストールされており*、カレントカーネルに*組み込まれていることをチェックします*。「HP-UXのカーネル構成のチェック」(100ページ)を参照してください。
3. 必要なSCSIパススルードライバ(sctlまたはspt)が*インストールされており*、カレントカーネルに*組み込まれていることを確認します*。「HP-UX上のSCSIロボティクス構成」(401ページ)を参照してください。
4. テープドライブとロボティクスに割り当て可能な未使用のSCSIアドレスを探します。「HP-UX上の未使用のSCSIアドレスの取得」(408ページ)を参照してください。

注記:

HP StorageWorks 12000eライブラリは、テープドライブとロボティクスに同じSCSIアドレス上の異なるLUNを割り当てるように設計されています。

5. デバイスのSCSIアドレス(ID)を設定します。詳細は、使用するデバイスのマニュアルを参照してください。
6. デバイス、コンピュータの順に電源を投入します。ブート処理が完了するまで待ちます。
7. 新しいテープドライブがシステムによって正しく認識されていることを確認します。以下のコマンドでioscanユーティリティを実行してください。

   ```
   /usr/sbin/ioscan -fn
   ```

   このコマンドを実行すると、接続済みのデバイスをハードウェアパスおよびデバイスファイルとともに示すリストが出力されます。このリストを調べて、新たに接続したテープドライブに正しいSCSIアドレスが割り当てられていることを確認してください。

8. ドライブのデバイスファイルはブート処理中に自動生成されますが、ロボティクスのデバイスファイルは手作業で作成する必要があります。「HP-UX上のデバイスファイルの作成」(406ページ)を参照してください。

9. 新たに作成したライブラリロボティクスのデバイスファイルが、システムによって正しく認識されていることを確認します。以下のコマンドでioscanユーティリティをもう一度実行してください。

   ```
   /usr/sbin/ioscan -fn
   ```

   コマンドの出力リストに新しいデバイスファイルが含まれていることを確認します。

この次に行う作業

ライブラリデバイスを正しく接続したら、オンラインヘルプの索引「構成、バックアップデバイス」を参照して、新しく接続したデバイスのData Protectorバックアップデバイスを構成する手順を確認してください。

Windowsシステムに接続する場合

HP StorageWorks 12000eライブラリデバイスをWindowsシステムに接続するには、以下の手順に従ってください。

1. オートローダーの裏側のモードスイッチを6に設定してください。

2. テープドライブとロボティクスに割り当て可能な未使用のSCSIアドレスを探します。「Windowsシステム上の未使用のSCSIターゲットIDの取得」(415ページ)を参照してください。

3. デバイスのSCSIアドレス(ID)を設定します。詳細は、使用するデバイスのマニュアルを参照してください。

注記:

HP StorageWorks 12000eライブラリは、テープドライブとロボティクスに同じSCSIアドレス上の異なるLUNを割り当てるように設計されています。

4. デバイス、コンピュータの順に電源を投入し、ブート処理が完了するまで待ちます。

5. 新たに接続したテープドライブとロボティクスが、システムによって正しく認識されていることを確認します。Data_Protector_home¥binディレクトリに移動して、次のコマンドを実行します。

   ```
   devbra -dev
   ```

   devbraコマンドの出力リストに、HP StorageWorks 12000eライブラリデバイスのテープドライブとロボティクスが含まれていることを確認してください。

この次に行う作業

ライブラリデバイスを正しく接続したら、オンラインヘルプの索引「構成、バックアップデバイス」を参照して、新しく接続したデバイスのData Protectorバックアップデバイスを構成する手順を確認してください。

HP StorageWorks DLTライブラリ28/48 スロットの接続

HP StorageWorks DLTライブラリ28/48 スロットは、エンタープライズ環境用のマルチドライブライブラリです。80～600 GBのバックアップ容量を提供します。複数のデータチャネル、1つのメールスロット、1つのバーコードリーダーを備えたDLT 4000またはDLT 7000のドライブが4つあります。

HP-UXシステムに接続する場合

HP-UXシステムにHP StorageWorks DLTライブラリ28/48スロットを接続するには、以下の手順に従ってください。

1. 必要なドライバ（stapeまたはtape2）がすでにインストールされており、カレントカーネルに組み込まれていることをチェックします。「HP-UXのカーネル構成のチェック」（100ページ）を参照してください。
2. 必要なSCSIパススルードライバ（sctlまたはspt）がインストールされており、カレントカーネルに組み込まれていることを確認します。「HP-UX上のSCSIロボティクス構成」（401ページ）を参照してください。
3. テープドライブとロボティクスに割り当て可能な未使用のSCSIアドレスを探します。「HP-UX上の未使用のSCSIアドレスの取得」（408ページ）を参照してください。

注記：

HP StorageWorks DLTライブラリ28/48スロットには、4つのテープドライブとロボティクスを搭載しているため、すべてのテープドライブを使用するには合計5つの未使用のSCSIアドレスが必要です。テープドライブとロボティクスごとに異なるSCSIアドレスを割り当てる必要があります。

4. デバイスのSCSIアドレス(ID)を設定します。詳細は、使用するデバイスのマニュアルを参照してください。
5. デバイス、コンピュータの順に電源を投入し、ブート処理が完了するまで待ちます。

6. 新しいテープドライブがシステムによって正しく認識されていることを確認します。以下のコマンドでioscanユーティリティを実行してください。

   /usr/sbin/ioscan -fn

   このコマンドを実行すると、接続済みのデバイスをハードウェアパスおよびデバイスファイルとともに示すリストが出力されます。このリストを調べて、新たに接続したテープドライブに正しいSCSIアドレスが割り当てられていることを確認してください。

7. ドライブのデバイスファイルはブート処理中に自動生成されますが、ロボティクスのデバイスファイルは手作業で作成する必要があります。「HP-UX上のデバイスファイルの作成」(406ページ)を参照してください。

8. 新たに作成したライブラリロボティクスのデバイスファイルが、システムによって正しく認識されていることを確認します。ioscanユーティリティを以下のコマンドで実行してください。

   /usr/sbin/ioscan -fn

   コマンドの出力リストに新しいデバイスファイルが含まれていることを確認します。

この次に行う作業

HP StorageWorks DLTライブラリ28/48スロットライブラリデバイスを正しく接続したら、オンラインヘルプの索引「構成、バックアップデバイス」を参照して、新しく接続したデバイスのData Protectorバックアップデバイスを構成する手順を確認してください。

Solarisシステムに接続する場合

Solarisシステム上でHP C5173-7000ライブラリデバイスを構成するには、以下の手順に従ってください。この例では、2つのドライブをData Protectorに接続するものと想定します。

1. sstドライバ(モジュール)と構成ファイルsst.confを、次のディレクトリにコピーします。

   - 32ビットオペレーティングシステムの場合

     $cp /opt/omni/spt/sst /usr/kernel/drv/sst

     $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf

   - 64ビットオペレーティングシステムの場合

     $cp /opt/omni/spt/sst.64 /usr/kernel/drv/sparcv9/sst

     $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sparcv9/sst.conf

2. ドライバをSolarisカーネルに追加します。

   add_drv sst

3. /dev/rmt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。次のコマンドを入力してください。

   cd /dev/rmt rm *

4. Stop + Aを押して、システムを停止します。

5. okプロンプトからprobe-scsi-allコマンドを実行して、使用可能なSCSIアドレスを調べます。

   ok probe-scsi-all

   ここで、probe-scsi-allコマンドを実行する前に、reset-allコマンドを実行するよう、システムから求められる場合があります。

   ここでは、SCSIコントロールデバイスにポート6、最初のドライブにポート2、2番目のドライブにポート1を使用します。LUNは0です。

6. 通常操作に戻るには、次のように入力します。

   ok go

7. 構成ファイルst.confを次のディレクトリにコピーします。

   $cp /opt/omni/spt/st.conf /kernel/drv/st.conf

   st.confファイルは各Solaris Data Protectorクライアント上に存在し、そのクライアントに接続されているすべてのバックアップデバイスのSCSIアドレスが記述されています。

8. /kernel/drv/st.confファイルを開いて、以下の行を追加します。

   tape-config-list="QUANTUM DLT7000", "Digital DLT7000", "DLT-data3";

   DLT-data3 = 1,0x77,0,0x8639,4,0x82,0x83,0x84,0x85,3;

   name="st" class="scsi"

   target=1 lun=0;

   name="st" class="scsi"

   target=2 lun=0;

   name="st" class="scsi"

   target=6 lun=0;

   これらのエントリにより、ドライブ1、ドライブ2、およびロボティクスドライブのSCSIアドレスが、それぞれ定義されます。

9. 手順ステップ 1(426ページ)でコピーしたsst.confファイルを開いて、次の行を追加します。

   name="sst" class="scsi" target=6 lun=0;

注記:

このエントリは、st.confファイル内のロボティクスドライブ用のエントリと一致していなければなりません。上の手順ステップ 8(427ページ)を参照してください。

---

10. クライアントシステムの電源を切ってから、ライブラリデバイスを接続します。
11. 最初にライブラリデバイスの電源を投入し、次にクライアントシステムの電源を投入します。

    システムがブートし、ロボティクスドライブとテープドライブ用のデバイスファイルが自動的に作成されます。これらのファイルは、ls -allコマンドを使用して一覧表示できます。ここでは、以下のようになります。

/dev/rmt/0hb	1番目のテープドライブ用
/dev/rmt/1hb	2番目のテープドライブ用
/dev/rsst6	ロボティクスドライブ用

この次に行う作業

HP StorageWorks DLTライブラリ28/48スロットライブラリデバイスを正しく接続したら、オンラインヘルプの索引「構成、バックアップデバイス」を参照して、新しく接続したデバイスのData Protectorバックアップデバイスを構成する手順を確認してください。

Windowsシステムに接続する場合

WindowsシステムにHP StorageWorks DLTライブラリ28/48スロットを接続するには、以下の手順に従ってください。

1. テープドライブとロボティクスに割り当て可能な未使用のSCSIアドレス(ターゲットID)を探します。「Windowsシステム上の未使用のSCSIターゲットIDの取得」(415ページ)を参照してください。

2. デバイスのSCSIアドレス(ターゲットID)を設定します。詳細は、使用するデバイスのマニュアルを参照してください。

注記:

HP StorageWorks DLTライブラリ28/48スロットには、4つのテープドライブとロボティクスを搭載しているため、すべてのテープドライブを使用するには合計5つの未使用のSCSIアドレスが必要です。テープドライブとロボティクスごとに、異なるSCSIターゲットIDを割り当てる必要があります。

3. デバイス、コンピュータの順に電源を投入し、ブート処理が完了するまで待ちます。
4. 新たに接続したテープドライブとロボティクスが、システムによって正しく認識されていることを確認します。Data_Protector_home¥binディレクトリに移動して、次のコマンドを実行します。

   ```
   devbra -dev
   ```

   devbraコマンドの出力リストに、HP StorageWorks DLTライブラリ28/48スロットのテープドライブとロボティクスが含まれていることを確認してください。

この次に行う作業

HP StorageWorks DLTライブラリ28/48スロットライブラリデバイスを正しく接続したら、オンラインヘルプの索引「構成、バックアップデバイス」を参照して、新しく接続したライブラリデバイスのData Protectorバックアップデバイスを構成する手順を確認してください。

Seagate Viper 200 LTO Ultriumテープドライブの接続

Seagate Viper 200 LTO Ultriumテープドライブは、エンタープライズ環境用のスタンドアロンデバイスです。100～200 GBのバックアップ容量を提供します。

Solarisシステムに接続する場合

Solarisシステム上でSeagate Viper 200 LTO Ultriumテープドライブを構成するには、以下の手順に従ってください。

1. このテープドライブに割り当て可能な未使用のSCSIアドレスを探します。modinfoコマンドまたはdmesgコマンドを使用すると、使用されているSCSIコントローラとインストールされているSCSIターゲットデバイスを確認できます。

   ```
   dmesg | egrep "target" | sort | uniq
   ```

   次のような内容が出力されます。

   ```
   sd32 at ithps0:target 2 lun 0
   sd34 at ithps0:target 4 lun 0
   st21 at ithps1:target 0 lun 0
   st22 at ithps1:target 1 lun 0
   ```

注記:

Viper 200 LTOデバイスをSolarisシステムに接続する場合は、glmまたはisp SCSIコントローラを使用することをお勧めします。また、Ultra2 SCSIコントローラまたはUltra3 SCSIコントローラの使用もお勧めします。

2. /kernel/drv/st.confファイルを開いて、以下の行を追加します。

   ```
   tape-config-list =
   "SEAGATE ULTRIUM06242-XXX" , "SEAGATE LTO" , ¥
   "SEAGATE_LTO" ;
   SEAGATE_LTO = 1, 0x7a, 0, 0x1d679, 4, 0x00, 0x00, 0x00, ¥
   0x00, 1;
   ```

3. クライアントシステムの電源を切ってから、デバイスを接続します。
4. 最初にデバイスの電源を投入し、次にクライアントシステムの電源を投入します。

   システムがブートし、テープドライブ用のデバイスファイルが自動的に作成されます。これらのファイル一覧を出力するには、ls -allコマンドを使用します。

この次に行う作業

Seagate Viper 200 LTO Ultriumテープドライブを正しく接続したら、オンラインヘルプの索引「構成、バックアップデバイス」を参照して、新しく接続したデバイスのData Protectorバックアップデバイスを構成する手順を確認してください。

Windowsシステムに接続する場合

WindowsシステムにSeagate Viper 200 LTO Ultriumテープドライブを接続するには、以下の手順に従ってください。

1. テープドライブに割り当て可能な未使用のSCSIアドレス(ターゲットID)を探します。「Windowsシステム上の未使用のSCSIターゲットIDの取得」(415ページ)を参照してください。
2. デバイスのSCSIアドレス(ターゲットID)を設定します。詳細は、使用するデバイスのマニュアルを参照してください。

1. デバイス、コンピュータの順に電源を投入し、ブート処理が完了するまで待ちます。
2. 新たに接続したテープドライブとロボティクスが、システムによって正しく認識されていることを確認します。Data_Protector_home¥binディレクトリに移動して、次のコマンドを実行します。

   ```
   devbra -dev
   ```

   devbraコマンドの出力リストに、新しく接続したSeagate Viper 200 LTO Ultriumテープドライブが含まれていることを確認してください。

この次に行う作業

Seagate Viper 200 LTO Ultriumテープドライブを正しく接続したら、オンラインヘルプの索引「構成、バックアップデバイス」を参照して、新しく接続したデバイスのData Protectorバックアップデバイスを構成する手順を確認してください。

注記:

Seagate Viper 200 LTO UltriumテープドライブをData Protector 向けに構成する場合は、圧縮モードが設定されていることを確認してください。このためには、次に示すように、ドライブのSCSIアドレスの後にCパラメータを指定します。

```
scsi2:0:0:0C
```

Novell NetWare上にインストールしたGeneral Media Agentのチェック

Novell NetWareプラットフォームにインストールしたGeneral Media Agentを確認するには、以下の作業を行います。

- 記憶デバイスを識別します。

- Novell NetWareサーバーのコンソールで、General Media Agentの起動をテストします。
- Novell NetWareサーバーのコンソールで、HPUMA.NLMおよびHPDEVBRA.NLMの起動をテストします。

記憶デバイスの識別

Novell NetWare環境では、以下の形式で記憶デバイスを識別します。

adapter identification number:*target identification number* :*logical unit numbercompression*

たとえば、“0:2:0N”という文字列は、アダプタID 0、ターゲットID 2、論理ユニット番号(LUN)0、および圧縮なしの記憶デバイスを示します。

また、“1:1:0C”という文字列は、アダプタID 1、ターゲットID 1、論理ユニット番号(LUN)0、および圧縮ありの記憶デバイスを示します。

General Media Agentの起動テスト

Novell NetWareシステムにGeneral Media Agentをインストールしたら、Novell NetWareサーバーのコンソールからBackup Media Agent (HPBMA.NLM)の起動をテストできます。

ここでは、AdaptecホストバスアダプタAHA-2940を経由して、エクスチェンジャテープデバイスHP StorageWorks Tape 12000eにアクセスする場合の例を示します。

Data Protector *.NLMコンポーネントを起動する前に、以下の条件が満たされていることを確認してください。

- HPINETが実行されていること。
- Adaptec SCSIホストアダプタが実行されていること。
- General Media Agentソフトウェアが、SYS:USR¥OMNI¥BINディレクトリにインストールされていること。
- 記憶デバイスが正しく接続されていること。
- AdaptecホストバスアダプタおよびTCP/IP通信プロトコルが正しくインストールされており、実行中であること。

上記の条件が満たされていれば、以下の手順に従ってください。

1. 以下のコマンドを入力して、HPBMA.NLMをロードします。

   LOAD HPBMA -name testbma -type *type_number* -policy *policy_number* -ioctl control_device -dev data_device -tty *tty_number*

   type *type_number*オプションでは、Data Protectorのデバイスの種類を指定します。*type_number*に指定可能な値は、以下に示すとおりです。

   - 1=DAT/DDS
   - 2 = 1/4インチカートリッジ(QIC)
   - 3 = 8mm - Exabyte
   - 9 = 汎用磁気テープドライブ
   - 10 =デジタルリニアテープ(DLT)

   policy *policy_number*オプションでは、Data Protectorでデバイスをどのように扱うかを指定します。指定可能な値は、以下に示すとおりです。

   - 1=スタンドアロンデバイス
   - 10= SCSI - IIライブラリ

   ioctl *control_device*オプションでは、ロボティクスのSCSIアドレスを定義します。以下の形式で指定する必要があります。

   adapter_identification_number:*target_identification_number*:

   logical_unit_number

   例:

   - 0:1:1 =>制御デバイス(ロボティクス)がSCSIアダプタ0を使用し、SCSIアドレス1、LUN 1が割り当てられていることを意味します。

   dev *data_device*オプションでは、ロボティクスのSCSIアドレスを定義します。以下の形式で指定する必要があります。

   adapter_identification_number:*target_identification_number*:*logical_unit_number*

   圧縮

   例:

   - 0:1:1C =>制御デバイス(ロボティクス)がSCSIアダプタ0を使用し、SCSIアドレス1、LUN 1が割り当てられていることを意味します。さらに、データ圧縮が有効に設定されていることを示します。

   -tty *tty_number*オプションでは、TCP/IP通信プロトコルのポート番号を定義します。

   Console Media Agent HPCONMA.NLMが起動し、以下のようなプロンプト画面が表示されます。

*** MA listening on port:number

SLOT:[Load(2), Peek(2), Stop(0), Abort(0)]

SLOT: _

現在のリリースでは、以下に示すコマンドを使用できます。

Load(2) - テープをドライブにロードするコマンド。引数を2つ指定する必要があります。

Load *Slot numberflipping flag*

flipping flagは0または1に設定できます。0の場合はメディアのフリップが行われず、1の場合はフリップが行われます。

Stop(0) - 現在のセッションを正常に終了します。

Abort(0) - 現在のセッションを中止します。

この例では、メディアのフリップなしで、SLOT 3からテープをロードします。

2. メディアのフリップなしで、SLOT 3からテープをロードするには、以下のコマンドを入力します。

   SLOT:LOAD 3 0

   ドライブにテープがロードされると、以下のメッセージが表示されます。

   CHECK:[Deny(0), Init(1), Seek(2), Abort(0)]

   CHECK: _

   以下に示すコマンドを使用できます。

   Deny(0)-現在のアクションを拒否します。

   Init(1)- ロードしたテープを初期化します。以下のようにメディアIDを指定する必要があります。

   Init(1) *medium_id*

   Seek(2)-指定した位置まで移動します。以下のように引数を指定します。

   Seek *segment_numberblock number*

   Abort(0) - 現在のセッションを中止します。

3. テープを初期化するには、以下のコマンドを入力します。

   CHECK:Init test

4. Backup Media Agentの画面をNovell Netwareコンソールに切り替えた後、General Media Agentのアクションコマンドや要求コマンドを実行して、バックアップセッションを開始します。

注記:

Data Protector Disk Agentは、load -ma *ホスト ポート*を使用して、選択されたホストで開始する必要があります。これは、HPCONMA.NLMが開始されたら、適切なGeneral Media AgentおよびDisk Agentの通信を有効にして、正しいバックアップセッション操作のポート番号を表示するためです。バックアップセッションが正常に終了すると、メッセージが表示されます。

5. Backup Media Agentを正常に終了するには、Backup Media Agent画面で**CTRL-C**キーを押します。しばらくすると、Console Attention Requestプロンプトが表示されます。

   ATT: [Stop(0), Abort(0), Disconnect(1)] ここでStopコマンドを実行して、セッションを終了します。

HPUMA.NLMおよびHPDEVBRA.NLMの起動テスト

HPUMA.NLMをサーバーのコンソールからロードすると、SCSIコマンドを手作業でテストできます。

HPUMA.NLMをロードするには、以下のコマンドを入力します。

LOAD HPUMA.NLM -ioctl control_device -dev data_device

-tty

ioctl *control_device*オプションでは、ロボティクスのSCSIアドレスを定義します。以下の形式で指定する必要があります。

adapter_identification_number:*target_identification_number*:

logical_unit_number

例:

- 0:1:1 =>制御デバイス(ロボティクス)がSCSIアダプタ0を使用し、SCSIアドレス1、LUN 1が割り当てられていることを意味します。

dev *data_device*オプションでは、ロボティクスのSCSIアドレスを定義します。以下の形式で指定する必要があります。

adapter_identification_number:*target_identification_number*:*logical_unit_number*:

圧縮

例:

- 0:1:1C =>制御デバイス(ロボティクス)がSCSIアダプタ0を使用し、SCSIアドレス1、LUN 1が割り当てられていることを意味します。さらに、データ圧縮が有効に設定されていることを示します。

Novell NetWareサーバーコンソールからDEVBRA.NLMを操作するには、-ttyオプションを指定する必要があります。

HPUMAが起動し、以下のプロンプト画面が表示されます。

prompt

プロンプトは以下の形式で表示されます。
adapter_identification_number:target_identification_number:logical_unit_number 以下に例を示します。

0:2:1

使用可能なコマンドを調べるには、HPUMA画面でHELPコマンドを入力します。たとえば、未使用のスロットとドライブがあるかどうかを確認するには、プロンプトでSTATと入力します。

確認が完了したら、BYE と入力して、HPUMA画面を閉じます。

HPDEVBRA.NLMをローカルにロードすると、Novell NetWareサーバー上にインストールされているデバイスのうち、Novell NetWareサーバーによって検出されたデバイスに関する情報を取得できるようになります。

HPDEVBRA.NLMをロードするには、サーバーコンソールで以下のコマンドを入力します。

LOAD HPDEVBRA.NLM -dev

上記で、-devオプションは、Novell NetWareサーバーに接続されているすべてのデバイスを表示するのに必要です。

現在使用可能なコマンドを調べるには、以下に示すとおり、HELPオプション付きでHPDEVBRA.NLMをロードしてください。

LOAD HPDEVBRA -HELP

D Data Protector 6.20へのアップグレード後のコマンドラインの変更

ここでは、Data Protector 6.20の新しいオプションに関連して変更または機能拡張されたコマンドを紹介します。スクリプトに古いコマンドが使用されていないかどうかチェックの上、必要に応じて修正してください。使用法については、*HP Data Protector Command Line Interface Reference*または該当するマンページを参照してください。

アップグレード前のCell Managerのバージョンに応じて、対応する表を参照してください。

- Data Protector A.06.00からアップグレードした場合は、表13（437ページ）を参照してください。
- Data Protector A.06.10からアップグレードした場合は、表14（448ページ）を参照してください。
- Data Protector A.06.11からアップグレードした場合は、表15（455ページ）を参照してください。
- Application Recovery Manager A.06.00からアップグレードした場合は、表16（458ページ）を参照してください。

表 13 Data Protector A.06.00からのアップグレード

コマンド	影響を受けるオプションまたは引数、注意事項	状態
cjutil	Data Protector Disk Agentコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
ob2install	chs_ls	新しいソフトウェアコンポーネント
	veagent	
	vmware	
	vls_am	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	momgui	削除されるソフトウェアコンポーネント
	snapa	
omnib	-mssps_list	新しい統合ソフトウェア
	-vmware_list	
	-veagent_list	
	-mssharepoint_list	
	-e2010_list	
	-async	新しいオプション
	-encode aes256	
	-clp	
	-resume	
	-ndmp_bkptype	
	-[no_]vss	新しいオプション/変更されるオプション
omnicc	-encryption	新しいオプション
	-enable	
	-cert	
	-key	
	-trust	
	-all	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-add_exception	
	-remove_exception	
	-list_exceptions	
	-status	
	-add_certificate	
	-get_certificate	
	-list_certificates	
	-import_vls	
	-impersonation	
	-create_userrestrictions_tmpl	
	-port	変更されるオプション
	-user	
	-passwd	
omnicjutil	Data Protector Cell Manager上で使用可能です。	新しいコマンド
omnicreatedl	-va	削除されるオプション
	-lun_security	
omnidb	-mssps	新しい統合ソフトウェア
	-vmware	
	-veagent	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-e2010	
	-mssharepoint	
	-auditing	新しいオプション
	-timeframe	
	-type verification	
	-encryptioninfo	
	-detail	変更されるオプション
omnidbcheck	-keystore	新しいオプション
	-summary	
omnidbp4000	このコマンドは、Data Protectorのユーザーインタフェースコンポーネントがインストールされたwindowsシステムで使用できます。	新しいコマンド
omnidbrestore	-keyfile	新しいオプション
omnidbsmis	-ompasswd -delete	新しいオプションの組み合わせ
	-reference	新しいオプション
	-sync_check	
	-exclude	
	-include	
	-namespace	削除されるオプション
	-sync	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
omnidbutil	-free_cell_resources	新しいオプション
	-list_large_directories	
	-list_large_mpos	
	-list_mpos_without_overs	
omnidbva		削除されるコマンド
omnidbvss		再設計されたコマンド
omnidlc	-add_info	新しいオプション
	-pack	
	-no_config	
	-any	
	-del_tracelog	
omnihealthcheck	Windowsプラットフォームの場合、コマンドはUser Interfaceコンポーネントから Cell Managerインストールパッケージに移動されました。	移動されたコマンド
omniinetpasswd	Data Protectorコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omniintconfig.pl	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omniiso	-autoinject	新しいオプション
	-waik	
	-inject_drivers	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
omnikeymigrate	Data Protector Cell Manager上で使用可能です。	新しいコマンド
omnikeytool	Data Protector Cell Manager上で使用可能です。	新しいコマンド
omnimcopy	-encrypt	新しいオプション
	-ams	
	-copy	変更されるオプション
	-from	
	-pool	
omniminit	-ams	新しいオプション
	-init	変更されるオプション
	-pool	
	-slot	
omnimm	-copy_to_mcf	新しいオプション
	-import_from_mcf	
	-output_directory	
	-pool_prefix	
	-no_pool_prefix	
	-orig_pool	
	-no_orig_pool	
	-encryptioninfo	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-ams	
omniobjconsolidate	-encrypt	新しいオプション
omniobjcopy	-mssps	新しい統合ソフトウェア
	-vmware	
	-veagent	
	-e2010	
	-mssharepoint	
	-encrypt	新しいオプション
	-restart	
	-sourceprotect	
	-targetprotect	
	-no_auto_device _selection	
	-protect	削除されるオプション
	-recycle	
	-no_recycle	
omniobjverify	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omnir	-mssps	新しい統合ソフトウェア
	-vmware	
	-veagent	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-e2010	
	-mssharepoint	
	-no_auto_device _selection	新しいオプション
	-omit_unrequired_object_versions	
	-resume	
	-[no_]resumable	
	-omit_unrequired_incrementals	削除されるオプション 次に置き換え -omit_unrequired_object_versions
	-appname	新しいオプション Lotus Notes/Domino Server復元の新しいオプション。
	-instant_restore	新しいオプション VSS復元の新しいオプション。
	-conf_check	
	-no_recovery	
	-use_vds	
	-no_copy_back	
	-copy_back	
	-diskarray_wait	
	-delete_replica	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-no_diskarray_wait	
	-no_retain_source	
	-exch_check	
	-exch_throttle	
	-appsrv	
	-target_tree	
	-exch_RSG	
	-target_dir	
	-delete_current	削除されるオプション
	-stopat	新しいオプション Microsoft SQL Server復元の新しいオプション。
	-target Client	変更されるオプション NDMP Server復元の変更されるオプション。
	-copyback	新しいオプション HP StorageWorks P6000 EVAディスクアレイファミリの新しいオプション
	-switch	
	-leave_source	
	-no_leave_source	
	-no_check_config	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
omnirpt	-copylist_sch	新しいオプション
	-copylist_post	
	-conslist_sch	
	-conslist_post	
	-num_copies	
	-verificationlist_sch	
	-verificationlist_post	
	-no_verificationlist	
	-copylist	削除されるオプション
	-conslist	
	obj_copies	新しいレポート
	session_objcopies	
	session_errors	
	session_statistics	
	backup_errors	削除されるレポート
	backup_statistics	
omnisetup.sh	veagent	新しいソフトウェアコンポーネント
	chs_ls	
	docs	
	javagui	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	vls_am	
	vmware	
	momgui	削除されるソフトウェアコンポーネント
	snapa	
	-IS1	削除されるオプション
	-IS2	
omnistoreapputil	Data Protector Cell Manager上で使用可能です。	新しいコマンド
omniusb	Data Protector Automatic Disaster Recoveryコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
sanconf	-mom	新しいオプション
uma	-vls_address	新しいオプション
	-vls_port	
	-vls_username	
	-vls_password	
util_cmd	veagent	新しい統合ソフトウェア
	vmware	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-encode	新しいオプション

表 14 Data Protector A.06.10からのアップグレード

コマンド	影響を受けるオプションまたは引数、注意事項	状態
ob2install	veagent	新しいソフトウェアコンポーネント
	vmware	
	chs_ls	
	snapa	削除されるソフトウェアコンポーネント
omnib	-resume	新しいオプション
	-ndmp_bkptype	
	-[no_]vss	新しいオプション/変更されるオプション
	-veagent_list	新しい統合ソフトウェア
	-e2010_list	
	-mssharepoint_list	
	-clp	新しいオプションの組み合わせ
omnicc	-encryption	新しいオプション
	-enable	
	-cert	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-key	
	-trust	
	-all	
	-add_exception	
	-remove_exception	
	-list_exceptions	
	-status	
	-add_certificate	
	-get_certificate	
	-list_certificates	
	-impersonation	
	-create_userrestrictions_tmpl	
omnicreatedl	-va	削除されるオプション
	-lun_security	
omnidb	-veagent	新しい統合ソフトウェア
	-e2010	
	-mssharepoint	
	-detail	変更されるオプション
	-encryptioninfo	新しいオプション

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-type verification	
omnidbp4000	このコマンドは、Data ProtectorのユーザーインタフェースコンポーネントがインストールされたWindowsシステムで使用できます。	新しいコマンド
omnidbsmis	-ompasswd -delete	新しいオプションの組み合わせ
	-reference	新しいオプション
	-sync_check	
	-exclude	
	-include	
	-namespace	削除されるオプション
	-sync	
omnidbva		削除されるコマンド
omnidbvss	-get session_persistent	新しいオプション
	-all	
	-details	
	-save_metadata	
	-disable session	
	-enable session	
	-mnttarget	
	-readwrite	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-no_session_id	
	-backhost	
	-resolve	
	-get disk	削除されるオプション
	-list disk	
	-purge	
	-export_metadata	
omnihealthcheck	Windowsプラットフォームの場合、コマンドはUser Interfaceコンポーネントから Cell Managerインストールパッケージに移動されました。	移動されたコマンド
omniintconfig.pl	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omniminit	-ams	新しいオプション
	-init	変更されるオプション
	-pool	
	-slot	
omnimm	-copy_to_mcf	新しいオプション
	-import_from_mcf	
	-output_directory	
	-pool_prefix	
	-no_pool_prefix	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-orig_pool	
	-no_orig_pool	
	-encryptioninfo	
	-ams	
	-show_locked_devs	
omniobjcopy	-veagent	新しい統合ソフトウェア
	-e2010	
	-mssharepoint	
	-restart	新しいオプション
	-sourceprotect	
	-targetprotect	
	-no_auto_device _selection	
	-protect	廃止予定のオプション
	-recycle	
	-no_recycle	
omniobjverify	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omnir	-veagent	新しい統合ソフトウェア
	-e2010	
	-mssharepoint	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-appname	新しいオプション Lotus Notes/Domino Server復元の新しいオプション。
	-resume	新しいオプション
	-no_auto_device _selection	
	-newinstance "None"	新しいオプションの値 Data Protector VMware(レガシー)用統合ソフトウェアの新しいオプション値。
	-no_auto_dev	削除されるオプション 次に置き換え -no_auto_device _selection
	-stopat	新しいオプション Microsoft SQL Server復元の新しいオプション。
	-copyback	新しいオプション HP StorageWorks P6000 EVAディスクアレイファミリの新しいオプション
	-switch	
	-leave_source	
	-no_leave_source	
	-no_check_config	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-target Client	変更されるオプション NDMP Server復元の変更されるオプション。
omnirpt	-verificationlist_sch	新しいオプション
	-verificationlist_post	
	-no_verificationlist	
omnisetup.sh	veagent	新しいソフトウェアコンポーネント
	vmware	
	chs_ls	
	snapa	削除されるソフトウェアコンポーネント
omniusb	Data Protector Automatic Disaster Recoveryコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
sanconf	-mom	新しいオプション
util_cmd	veagent	新しい統合ソフトウェア
	vmware	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-encode	新しいオプション

表 15 Data Protector A.06.11からのアップグレード

コマンド	影響を受けるオプションまたは引数、注意事項	状態
ob2install	veagent	新しいソフトウェアコンポーネント
	chs_ls	
	snapa	削除されるソフトウェアコンポーネント
omnib	-clp	新しいオプションの組み合わせ
	-veagent_list	新しい統合ソフトウェア
	-e2010_list	
	-mssharepoint_list	
omnicc	-encryption	新しいオプション
	-enable	
	-cert	
	-key	
	-trust	
	-all	
	-add_exception	
	-remove_exception	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-list_exceptions	
	-status	
	-add_certificate	
	-get_certificate	
	-list_certificates	
	-impersonation	
	-create_userrestrictions_tmpl	
omnicreatedl	-va	削除されるオプション
	-lun_security	
omnidb	-veagent	新しい統合ソフトウェア
	-e2010	
	-mssharepoint	
omnidbp4000	このコマンドは、Data ProtectorのユーザーインタフェースコンポーネントがインストールされたWindowsシステムで使用できます。	新しいコマンド
omnidbsmis	-ompasswd -delete	新しいオプションの組み合わせ
	-reference	新しいオプション
	-sync_check	
	-exclude	
	-include	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-namespace	削除されるオプション
	-sync	
omnidbva		削除されるコマンド
omnimm	-show_locked_devs	新しいオプション
	-all	
omniobjcopy	-veagent	新しい統合ソフトウェア
	-e2010	
	-mssharepoint	
omniobjverify	-veagent	新しい統合ソフトウェア
	-e2010	
	-mssharepoint	
omnir	-veagent	新しい統合ソフトウェア
	-e2010	
	-mssharepoint	
	-copyback	新しいオプション HP StorageWorks P6000 EVAディスクアレイファミリの新しいオプション
	-switch	
	-leave_source	
	-no_leave_source	
	-no_check_config	
omnirsh	-add	新しいコマンド

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-modify	
omnisetup.sh	veagent	新しいソフトウェアコンポーネント
	chs_ls	
	snapa	削除されるソフトウェアコンポーネント
omniusb	Data Protector Automatic Disaster Recoveryコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
util_cmd	veagent	新しい統合ソフトウェア

表 16 Application Recovery Manager A.06.00からのアップグレード

コマンド	影響を受けるオプションまたは引数、注意事項	状態
omnib	-disk_only	新しいオプション ディスクへのZDBの新しいオプション。
	統合およびファイルシステム用の新しいオプション。	新しいオプション
omnidb	メディアの管理およびその他の新しいData Protectorの機能に関連する新しいオプション。	新しいオプション
omnidbp4000	このコマンドは、Data Protectorのユーザーインタフェースコンポーネントがインストールされたwindowsシステムで使用できます。	新しいコマンド
omnidbsmis	-host	新しいオプション
	-dgrules	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-init	
	-put	
	-get	
	-caconf	
	-session	
	-ir	
	-excluded	
	-original	
	-datalist	
	-show	
	-purge	
	-force	
	-delete	
	-preview	
	-sync	
	-reference	
	-sync_check	
	-exclude	
	-include	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-ompasswd -delete	新しいオプションの組み合わせ
	-namespace	削除されるオプション
	-sync	
omnidbutil	メディアの管理およびその他の新しいData Protectorの機能に関連する新しいオプション。	新しいオプション
omnidbvss	-get session_persistent	新しいオプション
	-list session_persistent	
	-remove session_persistent	
	-all	
	-details	
	-save_metadata	
	-disable session	
	-enable session	
	-mnttarget	
	-readwrite	
	-no_session_id	
	-backhost	
	-resolve	
	-get disk	削除されるオプション
	-list disk	

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-remove disk	
	-purge	
	-export_metadata	
omnihealthcheck	コマンドはUser InterfaceコンポーネントからCell Managerインストールパッケージに移動されました。	移動されたコマンド
omnir	統合およびファイルシステム用の新しいオプション。Application Recovery Manager A.06.00のオプションを使用できます。 詳細は、『*HP Data Protector Command Line Interface Reference*』を参照してください。	再設計されたコマンドの使用法
dbtool.pl	コマンドの機能が内部データベースバックアップに置き換えられました。	削除されるコマンド
注記: **表の最初の部分には、Application Recovery Manager A.06.00ですでに使用可能になっていて、スクリプトに影響する可能性のあるコマンドの変更のみが挙げられています。*Data Protector*に導入されたすべてのコマンドは、新しいコマンドとして以下に挙げられています。**		
cjutil	Data Protector Disk Agentコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
NNMpost.ovpl	Data Protector HP Network Node Manager Integrationコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
NNMpre.ovpl	Data Protector HP Network Node Manager Integrationコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
NNMScript.exe	Data Protector HP Network Node Manager Integrationコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド

コマンド	影響を受けるオプションまたは引数、注意事項	状態
ob2install	Data Protector インストールサーバー上で使用可能です。	新しいコマンド
omniamo	Data Protector Cell Manager上で使用可能です。	新しいコマンド
omnicjutil	Data Protector Cell Manager上で使用可能です。	新しいコマンド
omnicreatedl	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omnidbrestore	Data Protector Cell Manager上で使用可能です。	新しいコマンド
omnidbupgrade	Data Protector Cell Manager上で使用可能です。	新しいコマンド
omnidbxp	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omnidownload	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omnidr	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omniinetpasswd	Data Protectorコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omniintconfig.pl	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omniiso	Data Protector Automatic Disaster Recoveryコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド

コマンド	影響を受けるオプションまたは引数、注意事項	状態
omnikeymigrate	Data Protector Cell Manager上で使用可能です。	新しいコマンド
omnikeytool	Data Protector Cell Manager上で使用可能です。	新しいコマンド
omnimcopy	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omnimigrate.pl	Data Protector Cell Manager上で使用可能です。	新しいコマンド
omniminit	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omnimlist	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omnimm	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omnimnt	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omnimver	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omniobjconsolidate	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omniobjcopy	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド

コマンド	影響を受けるオプションまたは引数、注意事項	状態
omniobjverify	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omniofflr	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omniresolve	Data Protector統合コンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omnirpt	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omnirsh	Data Protector Cell Manager上で使用可能です。	新しいコマンド
omnisetup.sh	UNIXシステム用のData Protectorインストール DVD-ROMに収録されています。	新しいコマンド
omnisrdupdate	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omniupload	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omniusb	Data Protector Automatic Disaster Recoveryコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omniusers	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
sanconf	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド

コマンド	影響を受けるオプションまたは引数、注意事項	状態
syb_tool	Data Protector User Interfaceコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
uma	Data Protector General Media Agentコンポーネントまたは NDMP Media Agentコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
upgrade_cm_from_evaa	Data Protector Cell Manager上で使用可能です。	新しいコマンド
util_cmd	Data Protectorコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
util_oracle8.pl	Data Protector Oracle Integrationコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
util_vmware.exe	Data Protector VMware Integrationコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド

用語集

ACSLS

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

Active Directory

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

AES 256ビット暗号化

256ビット長のランダムキーを使用するAES-CTR(Advanced Encryption Standard in Counter Mode)暗号化アルゴリズムを基にしたData Protectorソフトウェア暗号化。暗号化と復号化の両方で同じキーが使用されます。データはネットワークを介して転送される前およびメディアに書き込まれる前に、AES256ビット暗号化機能によって暗号化されます。

AML

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

AMU

*(ADIC/GRAU固有の用語)*Archive Management Unit(アーカイブ管理単位)の略。

ASRセット

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

されます。これらのフロッピーディスクは、ASRの実行時に必要となります。

BACKINT

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

BC

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

BC Process

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

BCV

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

BRARCHIVE

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

BRBACKUP

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

BRRESTORE

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

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

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

BSM

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

CAP

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

CDB

Catalog Database(カタログデータベース)の略。CDBはIDBの一部で、バックアップ、復元、オブジェクトコピー、オブジェクト統合、オブジェクト検証、メディア管理の各セッションに関する情報が格納されます。選択したロギングレベルによっては、ファイル名とファイルバージョンも格納されます。CDBは、常にセルに対してローカルとなります。
「MMDB」を参照。

CDFファイル

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

Cell Manager

セル内のメインシステム。Data Protectorの運用に不可欠なソフトウェアがインストールされ、すべてのバックアップおよび復元作業がここから管理されます。管理タスク用のGUIは、異なるシステムにインストールできます。各セルにはCell Managerシステムが1つあります。

Change Journal

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

Change Log Provider

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

CMMDB

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

COM+クラス登録データベース

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

Command View VLS

*(VLS固有の用語)*LAN経由でVLSを構成、管理、モニターするのに使用するWebブラウザベースのGUI。
「仮想ライブラリシステム(VLS)」を参照。

CRS

Data Protector Cell Manager上で実行され、バックアップと復元セッションを開始、制御する、Cell Request Serverのプロセス(サービス)。このサービスは、Data ProtectorがCell Manager上にインストールされるとすぐに開始されます。Windowsシステムでは、CRSはインストール時に使用したユーザーアカウントで実行されます。UNIXシステムでは、CRSはアカウントルートで実行されます。

CSM

Data Protectorコピーおよび集約セッションマネージャ(Copy and Consolidation Session Manager)の略。このプロセスは、オブジェクトコピーセッションとオブジェクト集約セッションを制御し、Cell Managerシステム上で動作します。

Data_Protector_home

Windows Vista、Windows 7、およびWindows Server 2008では、Data Protectorのプログラムファイルを含むディレクトリ。その他のWindowsオペレーティングシステムでは、Data Protectorのプログラムファイルとデータファイルを含むディレクトリ。デフォルトのパスは、%ProgramFiles%¥OmniBackですが、パスはインストール時にData Protectorセットアップウィザードで変更できます。
「Data_Protector_program_data」を参照。

Data_Protector_program_data

Windows Vista、Windows 7、およびWindows Server 2008では、Data Protectorのデータファイルを含むディレクトリ。デフォルトのパスは、%ProgramData%¥OmniBackですが、パスはインストール時にData Protectorセットアップウィザードで変更できます。「Data_Protector_home」を参照。

Dbobject

*(Informix Server固有の用語)*Informix Server物理データベースオブジェクト。blobspace、dbspace、または論理ログファイルなどがそれにあたります。

DCBF

DCBF(Detail Catalog Binary Files: 詳細カタログバイナリファイル)ディレクトリは、IDBの一部です。IDBの約80%を占めるファイルバージョンと属性に関する情報を格納します。バックアップに使用されるData Protectorメディアごとに1つのDCバイナリファイルが作成されます。サイズの最大値は、ファイルシステムの設定による制限を受けます。

DCディレクトリ

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

DHCPサーバー

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

Disk Agent

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

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

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

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

DR OS
ディザスタリカバリを実行するオペレーティングシステム環境。Data Protectorに対して基本的な実行時環境(ディスク、ネットワーク、テープ、およびファイルシステムへのアクセス)を提供します。Data Protectorディザスタリカバリを実行する前に、DR OSをディスクにインストールするかメモリーにロードして、構成しておく必要があります。DR OSには、一時DR OSとアクティブDR OSがあります。一時DR OSは、他のオペレーティングシステムの復元用ホスト環境として排他的に使用されます。このホスト環境には、ターゲットとなるオペレーティングシステムの構成データも置かれます。ターゲットシステムを元のシステム構成に復元し終えた後、一時DR OSは削除されます。アクティブDR OSは、Data Protectorディザスタリカバリプロセスのホストとして機能するだけでなく、復元後のシステムの一部にもなります。その場合、DR OSの構成データは元の構成データに置き換わります。

DRイメージ
一時ディザスタリカバリオペレーティングシステム(DR OS)のインストールおよび構成に必要なデータ。

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

Event Log(Data Protector: イベントログ)
イベントログには、Data Protector関連のすべての通知が書き込まれます。デフォルトの送信方法では、すべての通知がイベントログに送信されます。イベントはCell Managerで記録され、Data_Protector_program_data¥log¥server¥Ob2EventLog.txt (Windows Server 2008の場合)、Data_Protector_home¥log¥server¥Ob2EventLog.txt (その他のWindowsシステムの場合)、/var/opt/omni/server/log/Ob2EventLog.txt (UNIXシステムの場合)に書き込まれます。このイベントログにアクセスできるのは、

Data ProtectorのAdminユーザーグループに所属しているユーザーか、Data Protectorの「レポートと通知」ユーザー権限が付与されているユーザーのみです。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。

Exchange Replication Service

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

FCブリッジ

「Fibre Channelブリッジ」を参照。

Fibre Channelブリッジ

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

fnames.dat

IDBのfnames. datファイルには、バックアップしたファイルの名前に関する情報が格納されます。一般に、ファイル名が保存されている場合、それらのファイルはIDBの20%を占めます。

GUI

Data Protectorには、構成、管理、および操作に関するあらゆるタスクに簡単にアクセスできる、グラフィカルユーザーインタフェースが用意されています。Windows用のオリジナルのData Protector GUIの他に、Data Protectorには、さまざまなプラットフォームで実行できる、外観も操作も変わらないJavaベースのGUIも用意されています。

Holidaysファイル

休日に関する情報を格納するファイル。このファイルは、Data_Protector_program_data¥Config¥Server¥holidaysディレクトリ(Windows Server 2008の場合)、Data_Protector_home¥Config¥Server¥holidaysディレクトリ(その他のWindowsシステムの場合)、または/etc/opt/omni/server/Holidaysディレクトリ(UNIXシステムの場合)のCell ManagerのHolidaysファイルを編集することで、各種の休日を設定できます。

HP Operations Manager

ネットワーク内の多数のシステムとアプリケーションの運用管理を強力な機能でサポートするHP Operations Manager。Data Protectorには、この管理製品を使用するための統合ソフトウェアが用意され

ています。この統合ソフトウェアは、Windows、HP-UX、SolarisおよびLinux上のHP Operations Manager管理サーバー用のSMART Plug-Inとして実装されています。以前のバージョンのHP Operations Managerは、IT/Operation、Operations Center、およびVantage Point Operations、OpenView Operationsと呼ばれていました。

HP Operations Manager SMART Plug-In(SPI)

ドメイン監視機能を強化する完全に統合されたソリューションで、HP Operations Managerに追加するだけですぐに使えます。HP Operations Manager SMART Plug-Inとして実装されるData Protector用統合ソフトウェアを使用して、ユーザーはHP Operations Managerの拡張機能として任意の数のData Protector Cell Managerを監視できます。

HP Continuous Access (CA) P9000 XP

(HP P9000 XPアレイファミリ固有の用語) HP StorageWorks P9000 XPディスクアレイファミリ構成の1つで、データ複製やバックアップ、ディザスタリカバリなどのためにLDEVのリモートコピーの作成および保守を可能にします。HP CA P9000 XPを使用するには、メイン(プライマリ)ディスクアレイユニットとリモート(セカンダリ)ディスクアレイユニットが必要です。メインディスクアレイユニットはアプリケーションシステムに接続され、オリジナルのデータを格納しているプライマリボリューム(P-VOL)を格納します。リモートディスクアレイはバックアップシステムに接続され、セカンダリボリューム(S-VOL)を格納します。
「HP Business Copy (BC) P9000 XP、Main Control Unit、およびLDEV」を参照。

HP Continuous Access + Business Copy (CA+BC) P6000 EVA

(HP P6000 EVAアレイファミリ固有の用語) HP StorageWorks P6000 EVAディスクアレイファミリ構成の1つで、リモートHP P6000 EVAアレイファミリ上にソースボリュームのコピー(複製)を作成および保守し、このリモートアレイでローカル複製を行うときにソースとしてこのコピーを使用できます。
「HP Business Copy (BC) P6000 EVA、複製、およびソースボリューム」を参照。

HP StorageWorks P6000 EVA SMI-S Agent

HP StorageWorks P6000 EVAディスクアレイファミリ統合に必要なすべてのタスクを実行するData Protectorのソフトウェアモジュール。P6000 EVA SMI-S Agentを使用すると、受信した要求とHP StorageWorks CV EVA間のやり取りを制御するHP StorageWorks SMI-S P6000 EVAアレイプロバイダを通じてアレイを制御できます。
「HP StorageWorksCommand View (CV) EVAおよびHP StorageWorks SMI-S P6000 EVAアレイプロバイダ」を参照。

HP StorageWorks P9000 XP Agent

Data Protector HP StorageWorks P9000 XPディスクアレイファミリ統合に必要なすべてのタスクを実行するHP StorageWorks P9000

XPディスクアレイファミリソフトウェアコンポーネント。RAID Manager P9000 XPユーティリティ(WindowsシステムおよびHP-UXシステムの場合)またはRAID Managerライブラリ(Solarisシステムの場合)を介してP9000 XPアレイのストレージシステムと通信します。

HP StorageWorks Command View (CV) EVA

(HP P6000 EVAアレイファミリ固有の用語) P6000 EVAストレージシステムを構成、管理、モニターするためのユーザーインタフェース。さまざまなストレージ管理作業を行うために使用されます。たとえば、仮想ディスクファミリの作成、ストレージシステムハードウェアの管理、仮想ディスクのスナップショットやスナップクローン、ミラークローンの作成などに使用されます。HP StorageWorks Command View EVAソフトウェアはHPストレージマネジメントアプライアンス上で動作し、Webブラウザからアクセスできます。
「HP StorageWorks P6000 EVA SMI-S AgentおよびHP StorageWorks SMI-S P6000 EVAアレイプロバイダ」を参照。

HP StorageWorks SMI-S P6000 EVA アレイプロバイダ

HP StorageWorks P6000 EVAディスクアレイファミリを制御するために使用するインタフェース。SMI-S P6000 EVAアレイプロバイダはHPストレージマネジメントアプライアンスシステム上で個別のサービスとして動作し、受信した要求とHP StorageWorks Command View EVA間のゲートウェイとして機能します。Data Protector HP P6000 EVAファミリ統合を使用すると、SMI-S P6000 EVAアレイプロバイダはP6000 EVA SMI-S Agentからの標準化された要求を受け入れ、HP Command View EVAと通信して情報の取得またはメソッドの起動を行って、標準化された応答を返します。
「HP StorageWorks P6000 EVA SMI-S AgentおよびHP StorageWorks Command View (CV) EVA」を参照。

HP Business Copy (BC) P6000 EVA

(HP P6000 EVAアレイファミリ固有の用語) ローカル複製ソフトウェアソリューションの1つで、P6000 EVAファームウェアのスナップショット機能およびクローン機能を使用して、ソースボリュームの特定時点のコピー(複製)を作成できます。
「複製、ソースボリューム、スナップショット、およびHP Continuous Access + Business Copy (CA+BC) P6000 EVA」を参照。

HP Business Copy (BC) P9000 XP

(HP P9000 XPアレイファミリ固有の用語) HP StorageWorks P9000 XPディスクアレイファミリ構成の1つで、データ複製やバックアップなどのさまざまな目的のためにLDEVの内部コピーの作成および保守を可能にします。これらのコピー(セカンダリボリューム:S-VOL)は、プライマリボリューム(P-VOL)から分離して、別のシステムに接続することができます。Data Protectorゼロダウンタイムバックアップを目的とする場合、アプリケーションシステムでP-VOLを使

用可能にし、S-VOLセットのいずれかをバックアップシステムで使用可能にする必要があります。
「LDEV、HP Continuous Access (CA) P9000 XP、Main Control Unit、アプリケーションシステム、およびバックアップシステム」を参照。

ICDA

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

IDB

Data Protectorの内部データベース。IDBは、Cell Manager上に維持される埋込み型データベースです。どのデータがどのメディアにバックアップされたか、バックアップ、復元などのセッションがどのように実行されたか、どのデバイス、ライブラリ、ディスクアレイが構成されているかなどに関する情報が格納されます。

IDB復旧ファイル

IDBバックアップ、メディア、バックアップ用デバイスに関する情報を含むIDBファイル(obrindex.dat)。この情報により、IDBの復旧を大幅に簡素化できます。IDBトランザクションログと共にこのファイルを他のIDBディレクトリとは別の物理ディスクに移動し、さらにこのファイルのコピーを作成することをお勧めします。

Inet

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

Informix Server

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

Informix Server用のCMDスクリプト

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

インストールサーバー

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

ISQL

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

Java GUIクライアント

Java GUIクライアントはJava GUIコンポーネントの1つで、ユーザーインタフェース関連の機能(Cell Managerグラフィカルユーザーインタフェースおよび Manager-of-Managers(MoM)のグラフィカルユーザーインタフェース)のみで構成されており、機能するためにはJava GUIサーバーと接続する必要があります。

Java GUIサーバー

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

keychain

パスフレーズを手動で入力しなくても秘密キーを復号化できるようにするツールです。セキュアシェルを使用してリモートインストールを実行する場合、このツールをインストールサーバーにインストールして構成する必要があります。

KMS

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

LBO

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

LDEV

(HP P9000 XPアレイファミリ固有の用語) HP StorageWorks P9000 XPディスクアレイファミリのディスクアレイの物理ディスクの論理パーティション。LDEVは、このようなディスクアレイのスプリットミラー機能やスナップショット機能を使用して複製可能なエンティティです。
「HP Business Copy (BC) P9000 XP、HP Continuous Access (CA) P9000 XP、および複製」を参照。

LISTENER.ORA

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

log_fullシェルスクリプト

*(Informix Server UNIX固有の用語)*ON-Barに用意されているスクリプトの1つで、Informix Serverでlogfullイベント警告が発行され

た際に、論理ログファイルのバックアップを開始するために使用できます。Informix ServerのALARMPROGRAM構成パラメータは、デフォルトで、INFORMIXDIR/etc/log_full.shに設定されます。ここで、INFORMIXDIRは、Informix Serverホームディレクトリです。論理ログファイルを継続的にバックアップしたくない場合は、ALARMPROGRAM構成パラメータをINFORMIXDIR/etc/no_log.shに設定してください。

Lotus C API

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

LVM

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

Main Control Unit (MCU)

(HP P9000 XPアレイファミリ固有の用語) HP CA P9000 XPまたはHP CA+BC P9000 XP構成のプライマリボリューム(P-VOL)を含み、マスターデバイスとして機能するHP StorageWorks P9000 XPディスクアレイファミリのユニット。
「HP Business Copy (BC) P9000 XP、HP Continuous Access (CA) P9000 XP、およびLDEV」を参照。

make_net_ recovery

make_net_recoveryは、Ignite-UXのコマンドの1つ。Ignite-UXサーバーまたはその他の指定システム上にネットワーク経由で復旧アーカイブを作成できます。ターゲットシステムは、Ignite-UXのmake_boot_tapeコマンドで作成したブート可能なテープからブートするか、またはIgnite-UXサーバーから直接ブートした後、サブネットを通じて復旧することができます。Ignite-UXサーバーからの直接ブートは、Ignite-UXのbootsysコマンドで自動的に行うか、またはブートコンソールから対話的に指定して行うことができます。

make_tape_ recovery

make_tape_recoveryは、Ignite-UXのコマンドの1つ。システムに応じてカスタマイズしたブート可能テープ(インストールテープ)を作成できます。ターゲットシステムにバックアップデバイスを直接接続し、ブート可能な復旧テープからターゲットシステムをブートすることにより、無人ディザスタリカバリを実行できます。アーカイブ作成時とクライアント復旧時は、バックアップデバイスをクライアントにローカル接続しておく必要があります。

Manager-of-Managers (MoM)

「MoM」を参照。

MAPI

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

MCU

「Main Control Unit (MCU)」を参照。

Media Agent

デバイスに対する読み込み/書き込みを制御するプロセス。制御対象のデバイスはテープなどのメディアに対して読み込み/書き込みを行います。復元またはオブジェクト検証セッション中、Media Agentはバックアップ メディア上のデータを探して、処理するためにDisk Agentに送信します。復元セッションの場合、続いてDisk Agentはデータをディスクに書き込みます。Media Agentは、ライブラリのロボティクス制御も管理します。

Microsoft Exchange Server

多様な通信システムへの透過的接続を提供するクライアント/サーバー型のメッセージング/ワークグループシステム。電子メールシステムの他、個人とグループのスケジュール、オンラインフォーム、ワークフロー自動化ツールなどをユーザーに提供します。また、開発者に対しては、情報共有およびメッセージング サービス用のカスタムアプリケーション開発プラットフォームを提供します。

Microsoft SQL Server

分散型"クライアント/サーバー"コンピューティングのニーズを満たすように設計されたデータベース管理システム。

Microsoftボリュームシャドウコピーサービス(VSS)

VSS対応アプリケーションのバックアップと復元をそのアプリケーションの機能に関係なく統合管理する統一通信インタフェースを提供するソフトウェアサービスです。このサービスは、バックアップアプリケーション、ライター、シャドウコピープロバイダ、およびオペレーティングシステムカーネルと連携して、ボリュームシャドウコピーおよびシャドウコピーセットの管理を実現します。
「シャドウコピー、シャドウコピープロバイダ、複製およびライター」を参照。

Microsoft管理コンソール(MMC)

*(Windows固有の用語)*Windows環境における管理モデル。シンプルで一貫した統合型管理ユーザーインタフェースを提供します。同じGUIを通じて、さまざまなMMC対応アプリケーションを管理できます。

MMD

Media Management Daemon(メディア管理デーモン)の略。MMDプロセス(サービス)は、Data Protector Cell Manager上で稼動し、メディア管理操作およびデバイス操作を制御します。このプロセスは、Data ProtectorをCell Managerにインストールしたときに開始されます。

MMDB

Media Management Database(メディア管理データベース)の略。MMDBは、IDBの一部です。セル内で構成されているメディア、メディアプール、デバイス、ライブラリ、ライブラリデバイス、スロットに関する情報と、バックアップに使用されているData Protectorメディアに関する情報を格納します。エンタープライズバックアップ環境では、データベースをすべてのセル間で共有できます。
「CMMDBおよびCDB」を参照。

MoM

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

MSM

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

obdrindex.dat

「IDB復旧ファイル」を参照。

OBDR対応デバイス

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

ON-Bar

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

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

ONCONFIG

*(Informix Server固有の用語)*アクティブなONCONFIG構成ファイルの名前を指定する環境変数。ONCONFIG環境変数が存在しない場合、Informix ServerがINFORMIXDIR¥etc(Windowsの場合)、またはINFORMIXDIR/etc/(UNIXの場合)ディレクトリのONCONFIGファイルにある構成値を使います。

Oracle Data Guard

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

ORACLE_SID

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

Oracleインスタンス

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

Oracleターゲットデータベースへのログイン情報

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

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

P1Sファイル

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

他のWindowsシステムの場合)、/etc/opt/omni/server/dr/p1sディレクトリ(UNIXシステムの場合)です。ファイル名は以下のとおりです。recovery.p1s.

RAID

Redundant Array of Independent Disksの略。

RAID Manager P9000 XP (RM)

(HP P9000 XPアレイファミリ固有の用語) RAID Manager P9000 XPアプリケーションには、HP CA P9000 XPアプリケーションおよびHP BC P9000 XPアプリケーションのステータスを報告/制御するコマンドが豊富に用意されています。これらのコマンドは、RAID Manager P9000 XPインスタンスを通じて、HP StorageWorks P9000 XPディスクアレイファミリ Disk Control Unitと通信します。このインスタンスは、コマンドを一連の低レベルSCSIコマンドに変換します。

RAID Managerライブラリ

(HP P9000 XPアレイファミリ固有の用語) Solarisシステム上のData Protectorでは、RAID Managerライブラリを内部的に使用して、HP StorageWorks P9000 XPディスクアレイファミリの構成データ、ステータスデータ、およびパフォーマンスデータにアクセスします。さらに、一連の低レベルSCSIコマンドに変換される関数呼び出しを通じて、HP StorageWorks P9000 XPディスクアレイファミリの主要な機能にアクセスします。

rawディスクバックアップ

「ディスクイメージバックアップ」を参照。

RCU

「Remote Control Unit (RCU)」を参照。

RCU Remote Control Unit (RCU)

(HP P9000 XPアレイファミリ固有の用語) HP CA P9000 XPまたはHP StorageWorks P9000 XPディスクアレイファミリ CA+BC HP構成におけるメインコントロールユニット(MCU)に対するスレーブデバイスとして機能するHP StorageWorks P9000 XPディスクアレイファミリユニット。双方向の構成の中では、RCUはMCUとしての役割も果たします。

RDBMS

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

RDF1/RDF2

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

RDS

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

Recovery Manager (RMAN)

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

RecoveryInfo

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

REDOログ

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

RMAN *(Oracle固有の用語)*

「Recovery Manager」を参照。

RSM

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

RSM

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

SAPDBA

(SAP R/3固有の用語) BRBACKUPツール、BRARCHIVEツール、BRRESTOREツールを統合したSAP R/3ユーザーインタフェース。

SIBF

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

SMB

「スプリットミラーバックアップ」を参照。

SMBF

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

sqlhostsファイルまたはレジストリ

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

SRDF

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

SRDファイル

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

SSE Agent (SSEA) ***(HP P9000 XPアレイファミリ固有の用語)***

「HP StorageWorks P9000 XP Agent」を参照。

sst.confファイル

/usr/kernel/drv/sst.confファイルは、マルチドライブライブラリデバイスが接続されているData Protector Sun Solarisクライアントのそれぞれにインストールされていなければならないファイルです。このファイルには、クライアントに接続されている各ライブラリデバイスのロボット機構のSCSIアドレスエントリが記述されていなければなりません。

st.confファイル

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

StorageTek ACSライブラリ	*(StorageTek固有の用語)*ACS (Automated Cartridge System)は、1つのライブラリ管理ユニット(LMU)と、このユニットに接続された1～24個のライブラリ記憶域モジュール(LSM)からなるライブラリシステム(サイロ)です。
Sybase Backup Server API	*(Sybase固有の用語)*Sybase SQL ServerとData Protectorなどのバックアップソリューションの間でのバックアップ情報および復旧情報交換用に開発された業界標準インタフェース。
Sybase SQL Server	*(Sybase固有の用語)*Sybaseの「クライアントサーバー」アーキテクチャ内のサーバー。Sybase SQL Serverは、複数のデータベースと複数のユーザーを管理し、ディスク上のデータの実位置を追跡します。さらに、物理データストレージ域に対する論理データ記述のマッピングを維持し、メモリ内のデータキャッシュとプロシージャキャッシュを維持します。
SYMA *(EMC Symmetrix固有の用語)*	「EMC Symmetrix Agent」を参照。
System Backup to Tape	*(Oracle固有の用語)*Oracleがバックアップ要求または復元要求を発行したときに正しいバックアップデバイスをロード、ラベリング、およびアンロードするために必要なアクションを処理するOracleインタフェース。
SysVol	*(Windows固有の用語)*ドメインのパブリックファイルのサーバーコピーを保存する共有ディレクトリで、ドメイン内のすべてのドメインコントローラ間で複製されます。
TimeFinder	*(EMC Symmetrix固有の用語)*単一または複数のEMC Symmetrix論理デバイス(SLD)のインスタントコピーを作成するBusiness Continuationプロセス。インスタントコピーは、BCVと呼ばれる専用の事前構成SLD上に作成され、システムに対する別個のプロセスを経由してアクセスできます。
TLU	Tape Library Unit (テープライブラリユニット)の略。
TNSNAMES.ORA	*(OracleおよびSAP R/3固有の用語)*サービス名にマッピングされた接続記述子を格納するネットワーク構成ファイル。このファイルは、1か所で集中的に管理してすべてのクライアントで使用することも、また、ローカルに管理して各クライアントで個別に使用することもできます。

TSANDS.CFGファイル

*(Novell NetWare固有の用語)*バックアップを開始するコンテナの名前を指定するファイル。このファイルはテキストファイルで、TSANDS.NLMがロードされるサーバーのSYS:SYSTEM¥TSAディレクトリにあります。

UIProxy

Java GUI Server(UIProxyサービス)はData Protector Cell Managerで実行されます。Java GUI Serverでは、Java GUI ClientとCell Managerとの間の通信を行います。また、ビジネスロジック操作を実行し、重要な情報のみをクライアントに送信する必要があります。このサービスは、Data ProtectorがCell Manager上にインストールされるとすぐに開始されます。

user_restrictions ファイル

割り当てられているユーザー権限に応じてData Protectorのユーザーグループが使用できる特定のユーザーアクションを、Data Protectorセルの特定のシステムでのみ実行されるように制限するファイル。このような制限は、*Admin*および*Operator*以外の Data Protectorのユーザーグループにのみ適用されます。

VMware管理クライアント

*(VMware用統合ソフトウェア固有の用語)*Data Protectorを使用してVMware Virtual Infrastructureと通信するクライアント。VirtualCenter Serverシステム(VirtualCenter環境)、またはESX Serverシステム(スタンドアロンESX Server環境)のどちらかです。

VOLSER

*(ADICおよびSTK固有の用語)*ボリュームシリアル(VOLume SERial)番号は、メディア上のラベルで、大容量ライブラリ内の物理テープの識別に使用されます。VOLSERは、ADIC/GRAUデバイスおよびStorageTekデバイス固有の命名規則です。

VSS

「Microsoftボリュームシャドウコピーサービス(VSS)」を参照。

VSS準拠モード

*(HP P9000 XPアレイファミリVSSプロバイダ固有の用語)*2種類あるP9000 XPアレイVSSハードウェアプロバイダの操作モードの1つ。P9000 XPアレイプロバイダがVSS準拠モードであると、ソースボリューム(P-VOL)とその複製(S-VOL)は、バックアップ後、単純非対状態になります。したがって、ローテーションされる複製数(P-VOL当たりのS-VOL数)に制限はありません。このような構成でのバックアップからの復元は、ディスクの切り替えによってのみ可能となります。
「resyncモード、ソースボリューム、プライマリボリューム(P-VOL)、複製、セカンダリボリューム(S-VOL)、および複製セットローテーション」を参照。

VxFS

Veritas Journal Filesystemの略。

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

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

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

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

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

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

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

ZDB
「ゼロダウンタイムバックアップ(ZDB)」を参照。

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

アーカイブREDOログ
*(Oracle固有の用語)*オフラインREDOログとも呼びます。Oracleデータベースが ARCHIVELOGモードで動作している場合、各オンラインREDOログが最大サイズまで書き込まれると、アーカイブ先にコピーされます。このコピーをアーカイブREDOログと呼びます。各

データベースに対してアーカイブREDOログを作成するかどうかを指定するには、以下の2つのモードのいずれかを指定します。

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

「オンラインREDOログ」を参照。

アーカイブロギング

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

アクセス権限

「ユーザー権限」を参照。

アプリケーションエージェント

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

アプリケーションシステム

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

暗号化KeyID-StoreID

Data Protector Key Management Serverが、Data Protectorで使用される暗号化キーの識別と管理に使用する複合識別子です。KeyIDは、キーストア内のキーを識別します。StoreIDは、Cell Manager上のキーストアを識別します。Data Protectorを暗号化機能付きの旧バージョンからアップグレードした場合、同じCell Manager上で使用されるStoreIDが複数存在する可能性があります。

暗号化キー

256ビットのランダムに生成された数値で、AES 256ビットソフトウェア暗号化またはドライブベースの暗号化が指定されたバックアップの際に、Data Protectorの暗号化アルゴリズムが情報をエンコードするために使用します。これに続く情報の復号化では、同じキーが使用されます。Data Protectorセルの暗号化キーは、Cell Manager上の中央キーストアに保存されます。

暗号化された制御通信

Data Protectorセル内のクライアント間におけるData Protectorのセキュアな通信は、Secure Socket Layer (SSL)をベースにしており、SSLv3アルゴリズムを使用して制御通信が暗号化されます。Data

Protectorセル内の制御通信は、Disk Agent（および統合用ソフトウェア）からMedia Agentへのデータ転送とその逆方向のデータ転送を除く、Data Protectorプロセス間のすべての通信です。

イベントログ

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

インスタントリカバリ

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

インターネットインフォメーションサービス（IIS）

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

インフォメーションストア

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

上書き

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

エクスチェンジャ

SCSIエクスチェンジャとも呼ばれます。
「ライブラリ」を参照。

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

オートチェンジャー
「ライブラリ」を参照。

オートマイグレーション
*(VLS固有の用語)*データのバックアップをまずVLSの仮想テープに作成し、それを物理テープ(1つの仮想テープが1つの物理テープをエミュレート)に移行する操作を、中間バックアップアプリケーションを使用せずに実行する機能。
「仮想ライブラリシステム(VLS)と仮想テープ」を参照。

オートローダ
「ライブラリ」を参照。

オブジェクト
「バックアップオブジェクト」を参照。

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

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

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

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

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

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

オブジェクト検証

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

オブジェクト検証セッション

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

オブジェクト統合

1つのフルバックアップと1つ以上の増分バックアップで構成されたバックアップオブジェクトの復元チェーンを、新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するプロセス。このプロセスは、合成バックアップの一部です。このプロセスの結果、指定のバックアップオブジェクトの合成フルバックアップが出力されます。

オブジェクト統合セッション

1つのフルバックアップと1つ以上の増分バックアップで構成されたバックアップオブジェクトの復元チェーンを、新たな統合されたバージョンのオブジェクトとしてマージするプロセス。

オフラインREDOログ

「アーカイブREDOログ」を参照。

オフラインバックアップ

実行中はアプリケーションデータベースがアプリケーションから使用できなくなるバックアップ。オフラインバックアップセッションでは、一般にデータベースはデータ複製プロセス中に休止状態となり、バックアップシステムからは使用できますが、アプリケーションシステムからは使用できません。たとえばテープへのバックアップの場合、テープへのデータストリーミングが終わるまでの間となります。残りのバックアッププロセスでは、データベースは通常の稼動を再開できます。
「ゼロダウンタイムバックアップ(ZDB)およびオンラインバックアップ」を参照。

オフライン復旧

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

オリジナルシステム
あるシステムに障害が発生する前にData Protectorによってバックアップされたシステム構成データ。

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

オンラインバックアップ
データベースアプリケーションを利用可能な状態に維持したまま行われるバックアップ。データベースは、データ複製プロセスの間、特別なバックアップモードで稼動します。たとえばテープへのバックアップの場合、テープへのデータストリーミングが終わるまでの間となります。この期間中、データベースは完全に機能しますが、パフォーマンスに多少影響が出たり、ログファイルのサイズが急速に増大したりする場合もあります。残りのバックアッププロセスでは、データベースは通常の稼動を再開できます。
場合によっては、データベースを整合性を保って復元するために、トランザクションログもバックアップする必要があります。
「ゼロダウンタイムバックアップ(ZDB)およびオフラインバックアップ」を参照。

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

階層ストレージ管理(HSM)
使用頻度の低いデータを低コストの光磁気プラッタに移動することで、コストの高いハードディスク記憶域を有効利用するための仕組み。移動したデータが必要になった場合は、ハードディスク記憶域に自動的に戻されます。これにより、ハードディスクからの高速読み取りと光磁気プラッタの低コスト性のバランスが維持されます。

拡張増分バックアップ
従来の増分バックアップでは、前回のバックアップより後に変更されたファイルがバックアップされますが、変更検出機能に限界があります。これに対し、拡張増分バックアップでは、名前が変更されたファイルや移動されたファイルのほか、属性が変更されたファイルについても、信頼性のある検出とバックアップが行われます。

確認
指定したメディア上のData Protectorデータが読み取り可能かどうかをチェックする機能。また、CRC(巡回冗長検査)オプションをオンにして実行したバックアップに対しては、各ブロック内の整合性もチェックできます。

仮想コントローラソフトウェア(VCS)

*(HP P6000 EVAアレイファミリ固有の用語)*HSVコントローラを介したHP StorageWorks Command View EVAとの通信など、記憶システムの処理すべてを管理するファームウェア。
「HP StorageWorksCommand View (CV) EVA」を参照。

仮想サーバー

ネットワークIP名およびIPアドレスでドメイン内に定義されるクラスター環境の仮想マシンです。アドレスはクラスターソフトウェアによりキャッシュされ、仮想サーバーリソースを現在実行しているクラスターノードにマップされます。こうして、特定の仮想サーバーに対するすべての要求が特定のクラスターノードにキャッシュされます。

仮想ディスク

(HP P6000 EVAアレイファミリ固有の用語) HP StorageWorks P6000 EVAディスクアレイファミリのディスクアレイのストレージプールから割り当てられるストレージユニット。仮想ディスクは、このようなディスクアレイのスナップショット機能を使用して複製可能なエンティティです。
「ソースボリュームおよびターゲットボリューム」を参照。

仮想テープ

*(VLS固有の用語)*テープに保存された場合と同様にディスクドライブにデータをバックアップするアーカイブ式ストレージテクノロジ。バックアップスピードおよびリカバリスピードの向上、運用コストの削減など仮想テープシステムとしての利点がある。
「仮想ライブラリシステム(VLS)および仮想テープライブラリ(VTL)」を参照。

仮想テープライブラリ(VTL)

*(VLS固有の用語)*従来のテープベースのストレージ機能を提供する、エミュレートされるテープライブラリ。
「仮想ライブラリシステム(VLS)」を参照。

仮想デバイスインタフェース

*(Microsoft SQL Server固有の用語)*Microsoft SQL Serverのプログラミングインタフェースの1つ。大容量のデータベースを高速でバックアップおよび復元できます。

仮想フルバックアップ

コピーするのではなくポインタを使用してデータが統合される、効率の良い合成バックアップ。配布ファイルメディア形式を使用する1つのファイルライブラリにすべてのバックアップ(フルバックアップ、増分バックアップ、およびその結果である仮想フルバックアップ)が書き込まれる場合に実行されます。

仮想ライブラリシステム(VLS)

1つまたは複数の仮想テープライブラリ(VTL)をホストする、ディスクベースのデータストレージデバイス。

カタログ保護

バックアップデータに関する情報(ファイル名やファイルバージョンなど)をIDBに維持する期間を定義します。
「データ保護」を参照。

監査レポート

監査ログファイルに保存されたデータから作成される、ユーザーが判読可能な形式の監査情報出力。

監査ログ

監査情報が保存されるデータファイル。

監査情報

Data Protectorセル全体に対し、ユーザーが定義した拡張期間にわたって実施された、全バックアップセッションに関するデータ。

キーストア

すべての暗号化キーは、Cell Managerのキーストアに集中的に格納され、キー管理サーバー(KMS)により管理されます。

キーマネージメントサービス

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

共有ディスク

あるシステム上に置かれたWindowsのディスクをネットワーク上の他のシステムのユーザーが使用できるように構成したもの。共有ディスクを使用しているシステムは、Data Protector Disk Agentがインストールされていなくてもバックアップ可能です。

緊急ブートファイル

*(Informix Server固有の用語)*Informix Server構成ファイル ixbar.server_id。このファイルは、INFORMIXDIR/etcディレクトリ(Windowsの場合)、またはINFORMIXDIR¥etcディレクトリ(UNIXの場合)に置かれています。INFORMIXDIRはInformix Serverのホームディレクトリ、server_idはSERVERNUM構成パラメータの値です。緊急ブートファイルの各行は、1つのバックアップオブジェクトに対応します。

クライアントバックアップ

Data Protectorクライアントにマウントされているすべてのボリューム(ファイルシステム)のバックアップ。実際に何がバックアップされるかは、バックアップ仕様でどのようにオブジェクトを選択するかによって異なります。

- クライアントシステム名の隣のチェックボックスを選択した場合、[クライアントシステム]の種類の1つのバックアップオブジェクトが作成されます。その結果、バックアップ時にData Protectorは選択されたクライアントにマウントされているすべてのボリュームを最初に検出してから、それらをバックアップします。Windowsクライアントの場合、CONFIGURATIONもバックアップされます。

- クライアントシステムにマウントされているすべてのボリュームを別々に選択する場合、Filesystemタイプの個別バックアップオブジェクトがボリュームごとに作成されます。その結果、バックアップ時に、選択されたボリュームのみがバックアップされます。バックアップ仕様の作成後にクライアントにマウントされたボリュームは、バックアップされません。

クライアントまたはクライアントシステム

セル内でData Protectorの機能を使用できるように構成された任意のシステム。

クラスター対応アプリケーション

クラスターアプリケーションプログラミングインタフェースをサポートしているアプリケーション。クラスター対応アプリケーションごとに、クリティカルリソースが宣言されます。これらのリソースには、ディスクボリューム(Microsoft Cluster Serverの場合)、ボリュームグループ(MC/ServiceGuardの場合)、アプリケーションサービス、IP名およびIPアドレスなどがあります。

クラスター連続レプリケーション

*(Microsoft Exchange Server固有の用語)*クラスター連続レプリケーション(CCR)はクラスター管理とフェイルオーバーオプションを使用して、ストレージグループの完全なコピー(CCRコピー)を作成および維持する高可用性ソリューションです。ストレージグループは個別のサーバーに複製されます。CCRはExchangeバックエンドサーバーで発生した単発箇所の障害を取り除きます。CCRコピーが存在するパッシブExchange ServerノードでVSSを使用してバックアップを実行すれば、アクティブノードの負荷が軽減されます。CCRコピーへの切り替えは数秒で完了するため、CCRコピーはディザスタリカバリに使用されます。複製されたストレージグループは、Exchangeライターの新しいインスタンス(Exchange Replication Service)として表示され、元のストレージグループと同様にVSSを使用してバックアップできます。
「Exchange Replication Serviceおよびローカル連続レプリケーション」を参照。

グループ

*(Microsoft Cluster Server固有の用語)*特定のクラスター対応アプリケーションを実行するために必要なリソース(ディスクボリューム、アプリケーションサービス、IP名およびIPアドレスなど)の集合。

グローバルオプションファイル

Data Protectorをカスタマイズするためのファイル。このファイルでは、Data Protectorのさまざまな設定(特に、タイムアウトや制限)を定義でき、その内容はData Protectorセル全体に適用されます。このファイルは、Data_Protector_program_data¥Config¥Server¥Optionsディレクトリ(Windows Server 2008の場合)、Data_Protector_home¥Config¥Server¥Optionsディレクトリ(その他のWindowsシステム)、

または/etc/opt/omni/server/optionsディレクトリ(HP-UX、Solaris、またはLinuxシステムの場合)のCell Managerに置かれています。

合成バックアップ

データに関しては従来のフルバックアップと同じである合成フルバックアップを、生産サーバーやネットワークに負担をかけずに出力するバックアップソリューション。合成フルバックアップは、前回のフルバックアップと任意の数の増分バックアップを使用して作成されます。

合成フルバックアップ

バックアップオブジェクトの復元チェーンが新たな合成フルバージョンのオブジェクトにマージされる、オブジェクト集約処理の結果。合成フルバックアップは、復元速度の面では従来のフルバックアップと同じです。

コピーセット

*(HP P6000 EVAアレイファミリ固有の用語)*ローカルP6000 EVA上にあるソースボリュームとリモートP6000 EVA上にあるその複製とのペア。
「ソースボリューム、複製、およびHP Continuous Access + Business Copy (CA+BC)P6000 EVA」を参照。

コマンドラインインタフェース(CLI)

CLIには、DOSコマンドやUNIXコマンドと同じようにシェルスクリプト内で使用でできるコマンドが用意されています。これらを使用して、Data Protectorの構成、バックアップ、復元、および管理の各タスクを実行することができます。

コンテナ

*(HP P6000 EVAアレイファミリ固有の用語)*ディスクアレイ上のスペース。後で標準スナップショット、vsnap、またはスナップクローンとして使用するために事前に割り当てられます。

再解析ポイント

*(Windows固有の用語)*任意のディレクトリまたはファイルに関連付けることができるシステム制御属性。再解析属性の値は、ユーザー制御データをとることができます。このデータの形式は、データを保存したアプリケーションによって認識され、データの解釈用にインストールされており、該当ファイルを処理するファイルシステムフィルタによっても認識されます。ファイルシステムは、再解析ポイント付きのファイルを検出すると、そのデータ形式に関連付けられているファイルシステムフィルタを検索します。

再同期モード

*(HP P9000 XPアレイファミリVSSプロバイダ固有の用語)*2種類あるP9000 XPアレイVSSハードウェアプロバイダの操作モードの1つ。P9000 XPアレイプロバイダが再同期モードであると、ソースボリューム(P-VOL)とその複製(S-VOL)は、バックアップ後、中断ミラー関係になります。MU範囲が0-2(つまり、0、1、2)の場合、ローテー

ションされる最大複製数(P-VOL当たりのS-VOL数)は3となります。このような構成でのバックアップからの復元は、S-VOLをそのP-VOLと再同期することによってのみ可能となります。
「VSS準拠モード、ソースボリューム、プライマリボリューム(P-VOL)、複製、セカンダリボリューム(S-VOL)、ミラーユニット(MU)番号、および複製セットローテーション」を参照。

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

差分バックアップ　前回のフルバックアップより後の変更をバックアップする増分バックアップ。このバックアップを実行するには、増分1バックアップを指定します。
「増分バックアップ」を参照。

差分バックアップ　*(Microsoft SQL Server固有の用語)*前回のフルデータベースバックアップ以降にデータベースに対して加えられた変更だけを記録するデータベースバックアップ。
「バックアップの種類」を参照。

差分リストア　*(EMC Symmetrix固有の用語)*BCVまたはSRDF制御操作。BCV制御操作では、差分リストアにより、BCVデバイスがペア内の2番目に利用可能な標準デバイスのミラーとして再割り当てされます。これに対し、標準デバイスの更新時には、オリジナルのペアの分割中にBCVデバイスに書き込まれたデータだけが反映され、分割中に標準デバイスに書き込まれたデータはBCVミラーからのデータで上書きされます。SRDF制御操作では、差分リストアにより、ターゲットデバイス(R2)がペア内の2番目に利用可能なソースデバイス(R1)のミラーとして再割り当てされます。これに対し、ソースデバイス(R1)の更新時には、オリジナルのペアの分割中にターゲットデバイス(R2)に書き込まれたデータだけが反映され、分割中にソースデバイス(R1)に書き込まれたデータはターゲットミラー(R2)からのデータで上書きされます。

差分同期(再同期)　*(EMC Symmetrix固有の用語)*BCVまたはSRDF制御操作。BCV制御操作では、差分同期(Incremental Establish)により、BCVデバイスが増分的に同期化され、EMC Symmetrixミラー化メディアとして機能します。EMC Symmetrixデバイスは、事前にペアにしておく必要があります。SRDF制御操作では、差分同期(Incremental Establish)により、ターゲットデバイス(R2)が増分的に同期化され、

EMC Symmetrixミラー化メディアとして機能します。EMC Symmetrixデバイスは、事前にペアにしておく必要があります。

システムデータベース

*(Sybase固有の用語)*Sybase SQL Server を新規インストールすると、以下の4種類のデータベースが生成されます。

- マスターデータベース(master)
- 一時データベース(tempdb)
- システムプロシージャデータベース(sybsystemprocs)
- モデルデータベース(model)

システムボリューム/ディスク/パーティション

オペレーティングシステムファイルが格納されているボリューム/ディスク/パーティション。ただし、Microsoftの用語では、ブートプロセスの開始に必要なファイルが入っているボリューム/ディスク/パーティションをシステムボリューム/システムディスク/システムパーティションと呼んでいます。

システム復旧データファイル

「SRD file」を参照。

システム状態

*(Windows固有の用語)*システム状態データには、レジストリ、COM+クラス登録データベース、システム起動ファイル、および証明書サービスデータベース(証明書サーバーの場合)が含まれます。サーバーがドメインコントローラの場合は、Active DirectoryサービスとSYSVOLディレクトリもシステム状態データに含まれます。サーバーがクラスターサービスを実行している場合、システム状態データにはリソースレジストリチェックポイントとクォーラムリソースリカバリ ログが含まれ、最新のクラスターデータ情報が格納されます。

シャドウコピー

*(Microsoft VSS固有の用語)*特定の時点におけるオリジナルボリューム(元のボリューム)の複製を表すボリューム。オリジナルボリュームからではなく、シャドウコピーからデータがバックアップされます。オリジナルボリュームはバックアップ処理中も更新が可能ですが、ボリュームのシャドウコピーは同じ内容に維持されます。
「Microsoftボリュームシャドウコピーサービスおよび複製」を参照。

シャドウコピーセット

*(Microsoft VSS固有の用語)*同じ時点で作成されたシャドウコピーのコレクション。
「シャドウコピーおよび複製セット」を参照。

シャドウコピープロバイダ

*(Microsoft VSS固有の用語)*ボリュームシャドウコピーの作成と表現を行うエンティティ。プロバイダは、シャドウコピーデータを所有して、シャドウコピーを公開します。プロバイダは、ソフトウェア(シ

ステムプロバイダなど)で実装することも、ハードウェア(ローカルディスクやディスクアレイ)で実装することもできます。
「シャドウコピー」を参照。

ジュークボックス
「ライブラリ」を参照。

ジュークボックスデバイス
光磁気メディアまたはファイルメディアを格納するために使用する、複数のスロットからなるデバイス。ファイルメディアの格納に使用する場合、ジュークボックスデバイスは「ファイルジュークボックスデバイス」と呼ばれます。

事前割り当てリスト
メディアプール内のメディアのサブセットをバックアップに使用する順に指定したリスト。

実行後
オブジェクトのバックアップ後、またはセッション全体の完了後にコマンドまたはスクリプトを実行するバックアップオプション。実行後コマンドは、Data Protectorで事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows上で動作する実行可能ファイルまたはバッチファイル、UNIX上で動作するシェルスクリプトなどを使用できます。
「実行前」を参照。

実行前
オブジェクトのバックアップ前、またはセッション全体の開始前にコマンドまたはスクリプトを実行するバックアップオプション。実行前コマンドおよび実行後コマンドは、Data Protectorで事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows上で動作する実行可能ファイルまたはバッチファイル、UNIX上で動作するシェルスクリプトなどを使用できます。
「実行後」を参照。

実行前コマンドと実行後コマンド
実行前コマンドおよび実行後コマンドは、バックアップセッションまたは復元セッションの前後に付加的な処理を実行する実行可能ファイルまたはスクリプトです。実行前コマンドおよび実行後コマンドは、Data Protectorで事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows上で動作する実行可能ファイルまたはバッチファイル、UNIX上で動作するシェルスクリプトなどを使用できます。

自動ストレージ管理(ASM)
(Oracle固有の用語) Oracleに統合されるファイルシステムおよびボリュームマネージャで、Oracleデータベースファイルを管理します。データやディスクの管理が簡単になり、ストライピング機能やミラーリング機能によってパフォーマンスが最適化されます。

集中型ライセンス

Data Protectorでは、複数のセルからなるエンタープライズ環境全体にわたってライセンスの集中管理を構成できます。すべてのData Protectorライセンスは、エンタープライズCell Managerシステム上にインストールされます。ライセンスは、実際のニーズに応じてエンタープライズCell Managerシステムから特定のセルに割り当てることができます。
「MoM」を参照。

循環ログ

*(Microsoft Exchange ServerおよびLotus Domino Server固有の用語)*循環ログは、Microsoft Exchange Serverデータベースおよび Lotus Domino Serverデータベースモードの1つ。このモードでは、トランザクションログファイルのコンテンツは、対応するデータがデータベースにコミットされると、定期的に上書きされます。循環ログにより、ディスク記憶領域の要件が軽減されます。

証明書サーバー

Windows Certificate Serverをインストールして構成すると、クライアントに証明書を提供することができます。証明書サーバーは、エンタープライズ用の証明書を発行および管理するためのカスタマイズ可能なサービスを提供します。これらのサービスでは、公開キーベースの暗号化技術で使用されている証明書の発行、取り消し、および管理が可能です。

初期化

「フォーマット」を参照。

所有権

バックアップ所有権は、データを表示および復元するユーザーの機能に影響を与えます。各バックアップセッションとその中でバックアップされたすべてのデータはオーナーに割り当てられます。所有者は、対話型バックアップを開始するユーザー、CRSプロセスを実行するときに使用するアカウント、またはバックアップ仕様オプションで所有者として指定されたユーザーです。
ユーザーが既存のバックアップ仕様を修正せずにそのまま起動した場合、そのバックアップセッションは対話型とみなされません。
ユーザーがバックアップ仕様を修正して起動すると、以下の条件が成立しない限り、そのユーザーがオーナーになります。

- そのユーザーが[セッションの所有権を切り替え]ユーザー権限を持っている。
- バックアップ仕様内でバックアップセッションオーナーを明示的に定義するには、ユーザー名、グループ名またはドメイン名、およびシステム名を指定します。

UNIXCell Manager上でスケジュールしたバックアップの場合、上記の条件が成立しない限り、root: sysがセッションオーナーになります。

Windows Cell Manager上でスケジューリングしたバックアップの場合は、上記の条件が成立していない限り、インストール時に指定されたユーザーがセッションオーナーになります。
オブジェクトのコピーまたは統合を行う場合のオーナーは、コピー仕様や統合仕様で別のオーナーが指定されていない限り、デフォルトでは、その操作を開始するユーザーです。

スイッチオーバー
「フェイルオーバー」を参照。

スキャン
デバイス内のメディアを識別する機能。これにより、MMDBを、選択した位置(たとえば、ライブラリ内のスロット)に実際に存在するメディアと同期させることができます。デバイスに含まれる実際のメディアをスキャンしてチェックすると、第三者がData Protectorを使用せずにメディアを操作(挿入または取り出しなど)していないかどうかなどを確認できます。

スケジューラ
自動バックアップの実行タイミングと頻度を制御する機能。スケジュールを設定することで、バックアップの開始を自動化できます。

スタッカー
メディア記憶用の複数のスロットを備えたデバイス。通常は、1ドライブ構成です。スタッカーは、スタックからシーケンシャルにメディアを選択します。これに対し、ライブラリはレポジトリからメディアをランダムに選択します。

スタンドアロンファイルデバイス
ファイルデバイスとは、ユーザーがデータのバックアップに指定したディレクトリにあるファイルのことです。

拡張可能ストレージエンジン(ESE)
*(Microsoft Exchange Server固有の用語)*Microsoft Exchange Serverで情報交換用の記憶システムとして使用されているデータベーステクノロジ。

ストレージグループ
*(Microsoft Exchange Server固有の用語)*同じログファイルを共有する複数のメールボックスストアとパブリックフォルダストアのコレクション。Exchange Serverでは、各ストレージグループを個別のサーバープロセスで管理します。

ストレージボリューム
*(ZDB固有の用語)*ボリューム管理システム、ファイルシステム、他のオブジェクトなどが存在可能なオペレーティングシステムや他のエンティティ(たとえば、仮想化機構など)に提示できるオブジェクト。ボリューム管理システム、ファイルシステムはこの記憶域に構築されます。これらは通常、ディスクアレイなどの記憶システム内に作成または存在します。

スナップショット

(HP P6000 EVAアレイファミリ、HP P9000 XPアレイファミリ、およびHP StorageWorks P4000 SANソリューション固有の用語) 特定の複製方法で作成されたターゲットボリュームの種類の1つ。ディスクアレイモデルと選択した複製方法に応じて、特性の異なる、さまざまなスナップショットの種類が使用できます。基本的に、各スナップショットは仮想コピー(ソースボリュームの内容に引き続き依存します)、またはソースボリュームから独立した複製(クローン)のどちらかです。
「複製およびスナップショット作成」を参照。

スナップショットバックアップ

「テープへのZDB、ディスクへのZDB、およびディスク+テープへのZDB」を参照。

スナップショット作成

(HP P6000 EVAアレイファミリ、HP P9000 XPアレイファミリ、およびHP StorageWorks P4000 SANソリューション固有の用語) 選択したソースボリュームのコピーをストレージ仮想化技術を使用して作成する複製作成プロセス。スナップショットは、ある特定の時点で作成されたとみなされる複製で、作成後すぐに使用できます。ただし、スナップショットの種類によっては、複製作成後にデータコピープロセスがバックグランドで継続して実行されるものもあります。
「スナップショット」を参照。

スパースファイル

ブロックが空の部分を含むファイル。例として、データの一部または大部分にゼロが含まれるマトリクス、イメージアプリケーションからのファイル、高速データベースなどがあります。スパースファイルの処理を復元中に有効にしておかないと、スパースファイルを復元できなくなる可能性があります。

スプリットミラー

(EMC Symmetrix Disk ArrayおよびHP P9000 XPアレイファミリ固有の用語) 特定の複製方法で作成されたターゲットボリュームの種類の1つ。スプリットミラー複製により、ソースボリュームの独立した複製(クローン)が作成されます。
「複製およびスプリットミラーの作成」を参照。

スプリットミラーの作成

(EMC SymmetrixおよびHP P9000 XPアレイファミリ固有の用語) 事前構成したターゲットボリュームのセット(ミラー)を、ソースボリュームの内容の複製が必要になるまでソースボリュームのセットと同期化し続ける複製技法。その後、同期を停止(ミラーを分割)すると、分割時点でのソースボリュームのスプリットミラー複製はターゲットボリュームに残ります。
「スプリットミラー」を参照。

スプリットミラーバックアップ(*HP P9000 XPアレイファミリ固有の用語*)

「テープへのZDB、ディスクへのZDB、およびディスク+テープへのZDB」を参照。

スプリットミラーバックアップ(*EMC Symmetrix固有の用語*)

「テープへのZDB」を参照。

スプリットミラー復元

*(EMC SymmetrixおよびHP P9000 XPアレイファミリ固有の用語)*テープへのZDBセッションまたはディスク/テープへのZDBセッションでバックアップされたデータを、最初にバックアップメディアから複製に、その後に複製からソースボリュームにコピーするプロセス。この方法では、完全なセッションを復元することも個々のバックアップオブジェクトを復元することも可能です。
「テープへのZDB、ディスク/テープへのZDBおよび複製」を参照。

スマートコピー

*(VLS固有の用語)*仮想テープから物理テープライブラリへ作成されたバックアップデータのコピー。スマートコピーのプロセスによって、Data Protectorではソースメディアとターゲットメディアを区別できるため、メディア管理が可能になります。
「仮想ライブラリシステム(VLS)」を参照。

スマートコピープール

*(VLS固有の用語)*指定されたソース仮想ライブラリに対してどのコピー先ライブラリスロットをスマートコピーターゲットとして使用できるかどうかを定義するプール。
「仮想ライブラリシステム(VLS)およびスマートコピー」を参照。

スレッド

*(Microsoft SQL Server固有の用語)*1つのプロセスのみに属する実行可能なエンティティ。プログラムカウンタ、ユーザーモードスタック、カーネルモードスタック、およびレジスタ値のセットからなります。同じプロセス内で複数のスレッドを同時に実行できます。

スロット

ライブラリ内の機械的位置。各スロットがDLTテープなどのメディアを1つずつ格納できます。Data Protectorでは、各スロットを番号で参照します。メディアを読み取るときには、ロボット機構がメディアをスロットからドライブに移動します。

制御ファイル

*(OracleおよびSAP R/3固有の用語)*データベースの物理構造を指定するエントリが記述されたOracleデータファイル。復旧に使用するデータベース情報の整合性を確保できます。

セカンダリボリューム(S-VOL)

(HP P9000 XPアレイファミリ固有の用語) HP StorageWorks P9000 XPディスクアレイファミリのディスクアレイの内部ディスク(LDEV)で、もう1つのLDEVであるプライマリボリューム(P-VOL)とペアとなっています。プライマリボリューム(P-VOL)セカンダリボリュームは、P-VOLのミラーとして、またP-VOLのスナップショットストレージに使用されるボリュームとして機能することが可能です。S-VOLはP-VOLに使用されるSCSIアドレスとは異なるアドレスに割り当てられます。HP CA P9000 XP構成では、ミラーとして機能するS-VOLをMetroCluster構成のフェイルオーバーデバイスとして使用することができます。
「プライマリボリューム(P-VOL)およびMain Control Unit(MCU)」を参照。

セッション

「バックアップセッション、メディア管理セッションおよび復元セッション」を参照。

セッションID

バックアップ、復元、オブジェクトコピー、オブジェクト統合、オブジェクト検証、またはメディア管理のセッションの識別子で、セッションを実行した日付と一意の番号から構成されます。

セッションキー

実行前スクリプトおよび実行後スクリプト用の環境変数。Data Protectorプレビューセッションを含めたセッションを一意に識別します。セッションキーはデータベースに記録されず、omnimnt, omnistatおよびomniabort コマンドのオプション指定に使用されます。

セル

1台のCell Managerに管理されているシステムの集合。セルは、通常、同じLANまたはSANに接続されている、サイト上または組織エンティティ上のシステムを表します。集中管理によるバックアップおよび復元のポリシーやタスクの管理が可能です。

ゼロダウンタイムバックアップ(ZDB)

ディスクアレイにより実現したデータ複製技術を用いて、アプリケーションシステムのバックアップ処理の影響を最小限に抑えるバックアップアプローチ。バックアップされるデータの複製がまず作成されます。その後のすべてのバックアップ処理は、元のデータではなく複製データを使って実行し、アプリケーションシステムは通常の処理に復帰します。
「ディスクへのZDB、テープへのZDB、ディスク/テープへのZDB、およびインスタントリカバリ」を参照。

増分1メールボックスバックアップ

増分1メールボックスバックアップでは、前回のフルバックアップ以降にメールボックスに対して行われた変更をすべてバックアップします。

増分ZDB

ファイルシステムZDBからテープへ、またはZDBからディスク+テープへのセッション。前回の保護されたフルバックアップまたは増分バックアップからの変更のみがテープにストリーミングされます。
「フルZDB」を参照。

増分バックアップ

前回のバックアップ以降に変更があったファイルだけを選択するバックアップ。増分バックアップには複数のレベルがあり、復元チェーンの長さを細かく制御できます。
「バックアップの種類」を参照。

増分バックアップ

*(Microsoft Exchange Server固有の用語)*前回のフルバックアップまたは増分バックアップ以降の変更だけをバックアップするMicrosoft Exchange Serverデータのバックアップ。増分バックアップでは、バックアップ対象はトランザクションログだけです。
「バックアップの種類」を参照。

増分メールボックスバックアップ

増分メールボックスバックアップでは、前回の各種バックアップ以降にメールボックスに対して行われた変更をすべてバックアップします。

ソースデバイス(R1)

*(EMC Symmetrix固有の用語)*ターゲットデバイス(R2)とのSRDF操作に参加するEMC Symmetrixデバイス。このデバイスに対するすべての書き込みは、リモートEMC Symmetrixユニット内のターゲットデバイス(R2)にミラー化されます。R1デバイスは、RDF1グループタイプに割り当てる必要があります。
「ターゲットデバイス(R2)」を参照。

ソースボリューム

*(ZDB固有の用語)*複製されるデータを含むストレージボリューム。

ターゲットシステム

*(ディザスタリカバリ固有の用語)*コンピュータの障害が発生した後のシステム。ターゲットシステムは、ブート不能な状態になっていることが多く、そのような状態のシステムを元のシステム構成に戻すことがディザスタリカバリの目標となります。クラッシュしたシステムがそのままターゲットシステムになるのではなく、正常に機能していないハードウェアをすべて交換することで、クラッシュしたシステムがターゲットシステムになります。

ターゲットデータベース

*(Oracle固有の用語)*RMANでは、バックアップまたは復元対象のデータベースがターゲットデータベースとなります。

ターゲットデバイス(R2)

*(EMC Symmetrix固有の用語)*ターゲットデバイス(R1)とのSRDF操作に参加するEMC Symmetrixデバイス。リモートEMC Symmetrixユニット内に置かれます。ローカルEMC Symmetrixユニット内でソースデバイス(R1)とペアになり、ミラー化ペアから、すべての書き込み

データを受け取ります。このデバイスは、通常のI/O操作ではユーザーアプリケーションからアクセスされません。R2デバイスは、RDF2グループタイプに割り当てる必要があります。
「ソースデバイス(R1)」を参照。

ターゲットボリューム
*(ZDB固有の用語)*複製されるデータを含むストレージボリューム。

ターミナルサービス
*(Windows固有の用語)*Windowsのターミナルサービスは、サーバー上で実行されている仮想Windowsデスクトップセッションと Windowsベースのプログラムにクライアントからアクセスできるマルチセッション環境を提供します。

チャンネル
*(Oracle固有の用語)*Oracle Recovery Managerリソース割り当て。チャンネルが割り当てられるごとに、新しいOracleプロセスが開始され、そのプロセスを通じてバックアップ、復元、および復旧が行われます。割り当てられるチャンネルの種類によって、使用するメディアの種類が決まります。

- diskタイプ
- sbt_tapeタイプ

OracleがData Protectorと統合されており、指定されたチャンネルの種類がsbt_tapeタイプの場合は、上記のサーバー プロセスがData Protectorに対してバックアップの読み取りとデータファイルの書き込みを試行します。

ディザスタリカバリ
クライアントのメインシステムディスクを(フル)バックアップの実行時に近い状態に復元するためのプロセスです。

ディザスタリカバリオペレーティングシステム
「DR OS」を参照。

ディザスタリカバリの段階0
ディザスタリカバリの準備(ディザスタリカバリを成功させるための必須条件)。

ディザスタリカバリの段階1
DR OSのインストールと構成(以前の記憶領域構造の構築)。

ディザスタリカバリの段階2
オペレーティングシステム(環境を定義する各種の構成情報を含む)とData Protectorの復元。

ディザスタリカバリの段階3
ユーザーデータとアプリケーションデータの復元。

ディスク+テープへのZDB

*(ZDB固有の用語)*ゼロダウンタイムバックアップの1つの形式。ディスクへのZDBと同様に、作成された複製が特定の時点でのソースボリュームのバックアップとしてディスクアレイに保持されます。ただし、テープへのZDBと同様、複製データはバックアップメディアにもストリーミングされます。このバックアップ方法を使用した場合、同じセッションでバックアップしたデータは、インスタントリカバリプロセス、Data Protector標準のテープからの復元を使用して復元できます。特定のディスクアレイファミリではスプリットミラー復元が可能です。

「ゼロダウンタイムバックアップ(ZDB)、ディスクへのZDB、テープへのZDB、インスタントリカバリ、複製、および複製セットローテーション」を参照。

ディスクイメージ(rawディスク)のバックアップ

ディスクイメージのバックアップでは、ファイルがビットマップイメージとしてバックアップされるので、高速バックアップが実現します。ディスクイメージ(rawディスク)バックアップでは、ディスク上のファイルおよびディレクトリの構造はバックアップされませんが、ディスクイメージ構造がバイトレベルで保存されます。ディスクイメージバックアップは、ディスク全体か、またはディスク上の特定のセクションを対象にして実行できます。

ディスククォータ

コンピュータシステム上のすべてのユーザーまたはユーザーのサブセットに対してディスクスペースの消費を管理するためのコンセプト。このコンセプトは、いくつかのオペレーティングシステムプラットフォームで採用されています。

ディスクグループ

*(Veritas Volume Manager固有の用語)*VxVMシステムのデータストレージの基本ユニット。ディスクグループは、1つまたは複数の物理ボリュームから作成できます。同じシステム上に複数のディスクグループを置くことができます。

ディスクステージング

データをいくつかの段階に分けてバックアップする処理。これにより、バックアップと復元のパフォーマンスが向上し、バックアップデータの格納費用が節減され、データの可用性と復元時のアクセス性が向上します。バックアップステージは、最初に1種類のメディア(たとえば、ディスク)にデータをバックアップし、その後データを異なる種類のメディア(たとえば、テープ)にコピーすることから構成されます。

ディスクへのZDB

*(ZDB固有の用語)*ゼロダウンタイムバックアップの1つの形式。作成された複製が、特定の時点でのソースボリュームのバックアップとしてディスクアレイに保持されます。同じバックアップ仕様を使って別の時点で作成された複数の複製を、複製セットに保持するこ

とができます。テープにZDBした複製はインスタントリカバリプロセスで復元できます。
「ゼロダウンタイムバックアップ(ZDB)、テープへのZDB、ディスク/テープへのZDB、インスタントリカバリ、および複製セットローテーション」を参照。

ディレクトリ接合

*(Windows固有の用語)*ディレクトリ接合は、Windowsの再解析ポイントのコンセプトに基づいています。NTFS 5ディレクトリ接合では、ディレクトリ/ファイル要求を他の場所にリダイレクトできます。

データストリーム

通信チャンネルを通じて転送されるデータのシーケンス。

データファイル

*(OracleおよびSAP R/3固有の用語)*Oracleによって作成される物理ファイル。表や索引などのデータ構造を格納します。データファイルは、1つのOracleデータベースにのみ所属できます。

データベースサーバー

大規模なデータベース(SAP R/3データベースやMicrosoft SQLデータベースなど)が置かれているコンピュータ。サーバー上のデータベースへは、クライアントからアクセスできます。

データベースの並列処理(数)

十分な台数のデバイスが利用可能で、並列バックアップを実行できる場合には、複数のデータベースが同時にバックアップされます。

データベースの差分バックアップ

前回のフルデータベースバックアップ以降にデータベースに対して加えられた変更だけを記録するデータベースバックアップ。

データベースライブラリ

Data Protectorのルーチンのセット。Oracle Serverのようなオンラインデータベース統合ソフトウェアのサーバーとData Protectorの間でのデータ転送を可能にします。

データ保護

メディア上のバックアップデータを保護する期間を定義します。この期間中は、データが上書きされません。保護期限が切れると、それ以降のバックアップセッションでメディアを再利用できるようになります。
「カタログ保護」を参照。

データ複製(DR)グループ

(HP P6000 EVAアレイファミリ固有の用語) HP P6000 EVAファミリ仮想ディスクの論理グループ。共通の性質を持ち、同じHP CA P6000 EVAログを共有していれば、最大8組のコピーセットを含めることができます。
「コピーセット」を参照。

テープなしのバックアップ(*ZDB固有の用語*)

「ディスクへのZDB」を参照。

テープへのZDB

*(ZDB固有の用語)*ゼロダウンタイムバックアップの1つの形式。作成された複製が、バックアップメディア(通常はテープ)にストリーミングされます。このバックアップ形式ではインスタントリカバリはできませんが、バックアップ終了後にディスクアレイ上に複製を保持する必要がありません。バックアップデータはData Protector標準のテープからの復元を使用して復元できます。特定のディスクアレイファミリでは、スプリットミラー復元が可能です。
「ゼロダウンタイムバックアップ(ZDB)、ディスクへのZDB、ディスク+テープへのZDB、インスタントリカバリ、および複製」を参照。

デバイス

ドライブまたはより複雑な装置(ライブラリなど)を格納する物理装置。

デバイスグループ

*(EMC Symmetrix固有の用語)*複数のEMC Synnetrixデバイスを表す論理ユニット。デバイスは1つのデバイスグループにしか所属できません。デバイスグループのデバイスは、すべて同じEMC Symmetrix装置に取り付けられている必要があります。デバイスグループにより、利用可能なEMC Symmetrixデバイスのサブセットを指定し、使用することができます。

デバイスストリーミング

デバイスがメディアへ十分な量のデータを継続して送信できる場合、デバイスはストリーミングを行います。そうでない場合は、デバイスはテープを止めてデータが到着するのを待ち、テープを少し巻き戻した後、テープへの書込みを再開します。言い換えると、テープにデータを書き込む速度が、コンピュータシステムがデバイスへデータを送信する速度以下の場合、デバイスはストリーミングを行います。ストリーミングは、スペースの使用効率とデバイスのパフォーマンスを大幅に向上します。

デバイスチェーン

デバイスチェーンは、シーケンシャルに使用するように構成された複数のスタンドアロンデバイスからなります。デバイスチェーンに含まれるデバイスのメディアで空き容量がなくなると、自動的に次のデバイスのメディアに切り替えて、バックアップを継続します。

デルタバックアップ

差分バックアップ(delta backup)では、前回の各種バックアップ以降にデータベースに対して加えられたすべての変更がバックアップされます。
「バックアップの種類」を参照。

統合ソフトウェアオブジェクト

OracleまたはSAP DBなどのData Protector統合ソフトウェアのバックアップオブジェクト。

同時処理数

「Disk Agentの同時処理数」を参照。

ドメインコントローラ

ユーザーのセキュリティを保護し、別のサーバーグループ内のパスワードを検証するネットワーク内のサーバー。

ドライブ

コンピュータシステムからデータを受け取って、磁気メディア(テープなど)に書き込む物理装置。データをメディアから読み取って、コンピュータシステムに送信することもできます。

ドライブのインデックス

ライブラリデバイス内のドライブの機械的な位置を識別するための数字。ロボット機構によるドライブアクセスは、この数に基づいて制御されます。

ドライブベースの暗号化

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。バックアップの実行中、ドライブではメディアに書き込まれるデータとメタデータの両方が暗号化されます。

トランザクション

一連のアクションを単一の作業単位として扱えるようにするためのメカニズム。データベースでは、トランザクションを通じて、データベースの変更を追跡します。

トランザクションバックアップ

トランザクションバックアップは、一般に、データベースのバックアップよりも必要とするリソースが少ないため、データベースのバックアップよりもより高い頻度で実行できます。トランザクションバックアップを適用することで、データベースを問題発生以前の特定の時点の状態に復旧することができます。

トランザクションバックアップ

*(SybaseおよびSQL固有の用語)*トランザクションログをバックアップすること。トランザクションログには、前回のフルバックアップまたはトランザクションバックアップ以降に発生した変更が記録されます。

トランザクションログ

*(Data Protector固有の用語)*IDBに対する変更を記録します。IDB復旧に必要なトランザクションログファイル(前回のIDBバックアップ以降に作成されたトランザクションログ)が失われることがないように、トランザクションログのアーカイブを有効化しておく必要があります。

トランザクションログテーブル

*(Sybase固有の用語)*データベースに対するすべての変更が自動的に記録されるシステムテーブル。

トランザクションログバックアップ

トランザクションログバックアップは、一般に、データベースのバックアップよりも必要とするリソースが少ないため、データベースのバックアップよりもより高い頻度で実行できます。トランザクションログバッ

クアップを用いることにより、データベースを特定の時点の状態に復旧できます。

トランザクションログファイル
データベースを変更するトランザクションを記録するファイル。データベースが破損した場合にフォールトトレランスを提供します。

トランスポータブルスナップショット
*(Microsoft VSS固有の用語)*アプリケーションシステム上に作成されるシャドウコピー。このシャドウコピーは、バックアップを実行するバックアップシステムに提供できます。
「Microsoftボリュームシャドウコピーサービス(VSS)」を参照。

ハートビート
特定のクラスターノードの動作ステータスに関する情報を伝達するタイムスタンプ付きのクラスターデータセット。このデータセット(パケット)は、すべてのクラスターノードに配布されます。

ハードリカバリ
*(Microsoft Exchange Server固有の用語)*トランザクションログファイルを使用し、データベースエンジンによる復元後に実行されるMicrosoft Exchange Serverのデータベース復旧。

配布ファイルメディア形式
ファイルライブラリで利用できるメディア形式。仮想フルバックアップと呼ばれる容量効率のいい合成バックアップをサポートしています。この形式を使用することは、仮想フルバックアップにおける前提条件です。
「仮想フルバックアップ」を参照。

バックアップAPI
Oracleのバックアップ/復元ユーティリティとバックアップ/復元メディア管理層の間にあるOracleインタフェース。このインタフェースによってルーチンのセットが定義され、バックアップメディアのデータの読み書き、バックアップファイルの作成や検索、削除が行えるようになります。

バックアップID
統合ソフトウェアオブジェクトの識別子で、統合ソフトウェアオブジェクトのバックアップのセッションIDと一致します。バックアップIDは、オブジェクトのコピー、エクスポート、またはインポート時に保存されます。

バックアップオーナー
IDBの各バックアップオブジェクトにはオーナーが定義されています。デフォルトのオーナーは、バックアップセッションを開始したユーザーです。

バックアップオブジェクト
1つのディスクボリューム(論理ディスクまたはマウントポイント)からバックアップされた項目すべてを含むバックアップ単位。バックアップ項目は、任意の数のファイル、ディレクトリ、ディスク全体またはマウントポイントの場合が考えられます。また、バックアップオブジェク

トはデータベース/アプリケーションエンティティまたはディスクイメージ(rawディスク)の場合もあります。
バックアップオブジェクトは以下のように定義されます。

- クライアント名:バックアップオブジェクトが保存されるData Protectorクライアントのホスト名
- マウントポイント:ファイルシステムオブジェクトを対象とする場合ーバックアップオブジェクトが存在するクライアント(Windowsではドライブ、UNIXではマウントポイント)上のディレクトリ構造におけるアクセスポイント。統合オブジェクトを対象とする場合ーバックアップストリームID。バックアップされたデータベース項目/アプリケーション項目を示します。
- 説明:ファイルシステムオブジェクトを対象とする場合ー同一のクライアント名とマウントポイントを持つオブジェクトを一意に定義します。統合オブジェクトを対象とする場合ー統合の種類を表示します(例: SAPまたはLotus)。
- 種類:バックアップオブジェクトの種類。ファイルシステムオブジェクトを対象とする場合ーファイルシステムの種類(例: WinFS)。統合オブジェクトを対象とする場合ー「Bar」

バックアップシステム

(ZDB固有の用語) 1つ以上のアプリケーションシステムとともにディスクアレイに接続されているシステム。ほとんどの場合、バックアップシステムはターゲットボリューム(複製)を作成するためにディスクアレイに接続されるほか、ターゲットボリューム(複製)のマウント処理に使用されます。
「アプリケーションシステム、ターゲットボリュームおよび複製」を参照。

バックアップセッション

データのコピーを記憶メディア上に作成するプロセス。バックアップ仕様に処理内容を指定することも、対話式に操作を行うこともできます(対話式セッション)。1つのバックアップ仕様の中で複数のクライアントが構成されている場合、すべてのクライアントが同じバックアップの種類を使って、1回のバックアップセッションで同時にバックアップされます。バックアップセッションの結果、1式のメディアにバックアップデータが書き込まれます。これらのメディアは、バックアップセットまたはメディアセットとも呼ばれます。
「バックアップ仕様、フルバックアップ、および増分バックアップ」を参照。

バックアップセット

バックアップに関連したすべての統合ソフトウェアオブジェクトのセットです。

バックアップセット

*(Oracle固有の用語)*RMANバックアップコマンドを使用して作成したバックアップファイルの論理グループ。バックアップセットは、バックアップに関連したすべてのファイルのセットです。これらのファイルはパフォーマンスを向上するため多重化することができます。バックアップセットにはデータファイルまたはアーカイブログのいずれかを含めることができますが、両方同時に使用できません。

バックアップチェーン

「復元チェーン」を参照。

バックアップデバイス

記憶メディアに対するデータの読み書きが可能な物理デバイスをData Protectorで使用できるように構成したもの。たとえば、スタンドアロンDDS/DATドライブやライブラリなどをバックアップデバイスとして使用できます。

バックアップの種類

「増分バックアップ、差分バックアップ、トランザクションバックアップ、フルバックアップおよびデルタバックアップ」を参照。

バックアップビュー

Data Protectorでは、バックアップ仕様のビューを切り替えることができます。
[種類別]を選択すると、バックアップ/テンプレートで利用できるデータの種類に基づいたビューが表示されます。(デフォルト)
[グループ別]を選択すると、バックアップ仕様/テンプレートの所属先のグループに基づいたビューが表示されます。
[名前別]を選択すると、バックアップ仕様/テンプレートの名前に基づいたビューが表示されます。
[Manager別](MoMの実行時のみ有効)を選択すると、バックアップ仕様/テンプレートの所属先のCell Managerに基づいたビューが表示されます。

バックアップ世代

1つのフルバックアップとそれに続く増分バックアップを意味します。次のフルバックアップが行われると、世代が新しくなります。

バックアップ仕様

バックアップ対象オブジェクトを、使用するデバイスまたはドライブのセット、仕様内のすべてのオブジェクトに対するバックアップオプション、およびバックアップを行いたい日時とともに指定したリスト。オブジェクトとなるのは、ディスクやボリューム全体、またはその一部、たとえばファイル、ディレクトリ、Windowsレジストリなどです。インクルードリストおよびエクスクルードリストを使用して、ファイルを選択することもできます。

パッケージ

*(MC/ServiceGuardおよびVeritas Cluster固有の用語)*特定のクラスター対応アプリケーションを実行するために必要なリソース(ボ

リュームグループ、アプリケーションサービス、IP名およびIPアドレスなど)の集合。

パブリック/プライベートバックアップデータ

バックアップを構成する際は、バックアップデータをパブリックまたはプライベートのいずれにするかを選択できます。

- パブリックデータ — すべてのData Protectorユーザーに対してアクセスと復元が許可されます。
- プライベートデータ — バックアップの所有者および管理者に対してのみ表示と復元が許可されます。

パブリックフォルダストア

*(Microsoft Exchange Server固有の用語)*インフォメーションストアのうち、パブリックフォルダ内の情報を維持する部分。パブリックフォルダストアは、バイナリリッチテキスト. edbファイルと、ストリーミングネイティブインターネットコンテンツを格納する. stmファイルから構成されます。

表領域

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

ファーストレベルミラー

(HP P9000 XPアレイファミリ固有の用語) HP StorageWorks P9000 XPディスクアレイファミリのディスクアレイの内部ディスク(LDEV)のミラーで、このミラーをさらにミラー化し、セカンドレベルのミラーを作成できます。Data Protectorゼロダウンタイムバックアップおよびインスタントリカバリ目的には、ファーストレベルミラーのみを使用できます。
「プライマリボリュームおよびミラーユニット(MU)番号」を参照。

ファイバーチャネル

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

ファイルシステム

ハードディスク上に一定の形式で保存されたファイルの集まり。ファイルシステムは、ファイル属性とファイルの内容がバックアップメディアに保存されるようにバックアップされます。

ファイルジュークボックスデバイス

ファイルメディアを格納するために使用する、複数のスロットからなるディスク上に存在するデバイス。

ファイルツリーウォーク

*(Windows固有の用語)*どのオブジェクトが作成、変更、または削除されたかを判断するためにファイルシステムを巡回する処理。

ファイルデポ

バックアップからファイルライブラリデバイスまでのデータを含むファイル。

ファイルバージョン

フルバックアップや増分バックアップでは、ファイルが変更されている場合、同じファイルが複数回バックアップされます。バックアップのロギングレベルとして[すべてログに記録]を選択している場合は、ファイル名自体に対応する1つのエントリとファイルの各バージョンに対応する個別のエントリがIDB内に維持されます。

ファイルライブラリデバイス

複数のメディアからなるライブラリをエミュレートするディスク上に存在するデバイス。ファイルデポと呼ばれる複数のファイルが格納されます。

ファイル複製サービス(FRS)

Windowsサービスの1つ。ドメインコントローラのストアログオンスクリプトとグループポリシーを複製します。また、分散ファイルシステム(DFS)共有をシステム間で複製したり、任意のサーバーから複製作業を実行することもできます。

ブートボリューム/ディスク/パーティション

ブートプロセスの開始に必要なファイルが入っているボリューム/ディスク/パーティション。Microsoftの用語では、オペレーティングシステムファイルが入っているボリューム/ディスク/パーティションをブートボリューム/ブートディスク/ブートパーティションと呼んでいます。

フェイルオーバー

あるクラスターノードから別のクラスターノードに最も重要なクラスターデータ(Windowsの場合はグループ、UNIXの場合はパッケージ)を転送すること。フェイルオーバーは、主に、プライマリノードのソフトウェア/ハードウェア障害発生時や保守時に発生します。

フェイルオーバー

*(HP P6000 EVAアレイファミリ固有の用語)*HP Continuous Access + Business Copy (CA+BC) P6000 EVA構成でソースとあて先の役割を逆にする操作。
「HP Continuous Access + Business Copy (CA+BC) P6000 EVA」を参照。

フォーマット

メディアをData Protectorで使用できるように初期化するプロセス。メディア上の既存データはすべて消去されます。メディアに関する情報(メディアID、説明、場所)は、IDBおよび該当するメディア(メディアヘッダ)に保存されます。Data Protectorのメディアは、保護の期限が切れるか、またはメディアの保護が解除されるかメディアがリサイクルされるまで、フォーマットされません。

復元セッション

バックアップメディアからクライアントシステムにデータをコピーするプロセス。

復元チェーン

特定の時点までのバックアップオブジェクトの復元に必要なバックアップすべて。復元チェーンは、オブジェクトのフルバックアップ1つと、任意の数の増分バックアップで構成されます。

負荷調整

デフォルトでは、デバイスが均等に使用されるように、バックアップ用に選択されたデバイスの負荷(使用率)が自動的に調整されます。負荷調整では、各デバイスに書き込まれるオブジェクトの個数を調整することで、使用率を最適化します。負荷調整はバックアップ時に自動的に実行されるので、データが実際にどのようにバックアップされるかを管理する必要はありません。使用するデバイスを指定する必要があるだけです。負荷調整機能を使用しない場合は、バックアップ仕様に各オブジェクトに使用するデバイスを選択できます。Data Protectorは、指定した順にデバイスにアクセスします。

分散ファイルシステム(DFS)

複数のファイル共有を単一の名前空間に接続するサービス。対象となるファイル共有は、同じコンピュータに置かれていても、異なるコンピュータに置かれていてもかまいません。DFSは、リソースの保存場所の違いに関係なくクライアントがリソースにアクセスできるようにします。

複製

*(ZDB固有の用語)*ユーザー指定のバックアップオブジェクトを含む、特定の時点におけるソースボリュームのデータのイメージ。イメージは、作成するハードウェアまたはソフトウェアによって、物理ディスクレベルでの記憶ブロックの独立した正確な複製(クローン)になる(スプリットミラーやスナップクローンなど)場合もあれば、仮想コピーになる(スナップショットなど)場合もあります。基本的なオペレーティングシステムの観点からすると、バックアップオブジェクトを含む物理ディスク全体が複製されます。しかし、UNIXでボリュームマネージャを使用するときは、バックアップオブジェクトを含むボリュームまたはディスクグループ全体が複製されます。Windowsでパーティションを使用する場合、選択したパーティションを含む物理ボリューム全体が複製されます。
「スナップショット、スナップショット作成、スプリットミラー、およびスプリットミラーの作成」を参照。

複製セット

*(ZDB固有の用語)*同じバックアップ仕様を使って作成される複製のグループ。
「複製および複製セットローテーション」を参照。

複製セットローテーション

*(ZDB固有の用語)*通常のバックアップ作成のために継続的に複製セットを使用すること。複製セットの使用を必要とする同一のバックアップ仕様が実行されるたびに、新規の複製がセットの最大数になるまで作成され、セットに追加されます。その後、セット内の最も

古い複製は置き換えられ、セット内の複製の最大数が維持されます。
「複製および複製セット」を参照。

物理デバイス

ドライブまたはより複雑な装置(ライブラリなど)を格納する物理装置。

プライマリボリューム(P-VOL)

(HP P9000 XPアレイファミリ固有の用語) HP StorageWorks P9000 XPディスクアレイファミリのディスクアレイの内部ディスク(LDEV)で、これに対して、そのミラー、またはスナップショットストレージに使用されるボリュームのいずれかのセカンダリボリューム(S-VOL)が存在します。HP CA P9000 XPおよびHP CA+BC P9000 XP構成では、プライマリボリュームはメインコントロールユニット(MCU)内に配置されています。
「セカンダリボリューム(S-VOL)およびMain Control Unit (MCU)」を参照。

フラッシュリカバリ領域

(Oracle固有の用語) Oracleによって管理されるディレクトリ、ファイルシステム、または自動ストレージ管理(ASM)ディスクグループであり、バックアップ、復元、およびデータベース復旧に関係するファイル(リカバリファイル)用の集中管理ストレージ領域として機能します。
「リカバリファイル」を参照。

フリープール

フリープールは、メディアプール内のすべてのメディアが使用中になっている場合にメディアのソースとして補助的に使用できるプールです。ただし、メディアプールでフリープールを使用するには、明示的にフリープールを使用するように構成する必要があります。

フルZDB

前回のバックアップから変更がない場合でも選択されたすべてのオブジェクトをテープにストリーミングする、テープへのZDBセッションまたはディスク+テープへのZDBセッション。
「増分ZDB」を参照。

フルデータベースバックアップ

最後に(フルまたは増分)バックアップした後に変更されたデータだけではなく、データベース内のすべてのデータのバックアップ。フルデータベースバックアップは、他のバックアップに依存しません。

フルバックアップ

フルバックアップでは、最近変更されたかどうかに関係なく、選択されたオブジェクトをすべてバックアップします。
「バックアップの種類」を参照。

フルメールボックスバックアップ

フルメールボックスバックアップでは、メールボックス全体の内容をバックアップします。

ペアステータス

(HP P9000 XPアレイファミリ固有の用語) HP StorageWorks P9000 XPディスクアレイファミリのディスクアレイのディスクペア(セカンダリボリュームとそれに対応するプライマリボリューム)の状態。状況によってペアのディスクはさまざまな状態になる可能性があります。Data Protector HP StorageWorks P9000 XPエージェントの操作において特に以下の状態が重要となります。

- ペア – セカンダリボリュームがゼロダウンタイムバックアップ用に準備されています。セカンダリボリュームがミラーの場合、完全に同期化されます。セカンダリボリュームがスナップショットストレージ用に使用されるボリュームの場合、空の状態です。
- 中断 – ディスク間のリンクは中断されています。ただし、ペアの関係は維持されたままとなり、後で再度ゼロダウンタイムバックアップを行うためにセカンダリディスクを準備できます。
- コピー – ディスクペアは現在使用中であり、ペア状態に移行中です。セカンダリボリュームがミラーの場合、プライマリボリュームで再同期されています。セカンダリボリュームがスナップショットストレージに使用されるボリュームの場合、その内容はクリアされています。

並列処理

1つのオンラインデータベースから複数のデータストリームを読み取ること。

並行復元

単一のMedia Agentからデータを受信するDisk Agentを複数実行して、バックアップされたデータを同時に複数のディスクに(並行して)復元すること。並行復元を行うには、複数のディスクまたは論理ボリュームに置かれているデータを選択し、同時処理数を2以上に設定してバックアップを開始し、異なるオブジェクトのデータを同じデバイスに送信する必要があります。並行復元中には、復元対象として選択した複数のオブジェクトがメディアから同時に読み取られるので、パフォーマンスが向上します。

保護

「データ保護およびカタログ保護」を参照。

補助ディスク

必要最小限のオペレーティングシステムファイル、ネットワークファイル、およびData Protector Disk Agentがインストールされたブート可能ディスク。 ディスクデリバリーでUNIXクライアントを障害から復旧するときの段階1では、補助ディスクをターゲットシステムのブートに使用することができます。

ホストシステム

Data Protector Disk Agentがインストールされており、ディスクデリバリーによるディザスタリカバリに使用される稼動中のData Protectorクライアント。

ボリュームグループ
LVMシステムにおけるデータストレージ単位。ボリュームグループは、1つまたは複数の物理ボリュームから作成できます。同じシステム上に複数のボリュームグループを置くことができます。

ボリュームシャドウコピーサービス(VSS)
「Microsoftボリュームシャドウコピーサービス(VSS)」を参照。

ボリュームマウントポイント
*(Windows固有の用語)*ボリューム上の空のディレクトリを他のボリュームのマウントに使用できるように構成したもの。ボリュームマウントポイントは、ターゲットボリュームへのゲートウェイとして機能します。ボリュームがマウントされていれば、ユーザーやアプリケーションがそのボリューム上のデータをフル(マージ)ファイルシステムパスで参照できます(両方のボリュームが一体化されている場合)。

マージ
復元中のファイル名競合を解決するモードの1つ。復元するファイルと同じ名前のファイルが復元先に存在する場合、変更日時の新しい方が維持されます。既存のファイルと名前が重複しないファイルは、常に復元されます。
「上書き」を参照。

マウントポイント
ディレクトリ構造内において、ディスクまたは論理ボリュームにアクセスするためのアクセスポイント(/optやd:など)。UNIXでは、bdfコマンドまたはdfコマンドを使ってマウントポイントを表示できます。

マウント要求
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確認することでマウント要求に応答すると、セッションが続行されます。

マジックパケット
「Wake ONLAN」を参照。

マルチスナップ
*(HP P6000 EVAアレイファミリ固有の用語)*個々のターゲットボリュームだけでなく、スナップショットを構成するすべてのボリュームでバックアップデータの整合性が取れるように、複数のターゲットボリュームを同時に作成すること。
「スナップショット」を参照。

ミラー*(EMC Symmetrixおよび HP P9000 XPアレイファミリ固有の用語)*
「ターゲットボリューム」を参照。

ミラークローン

(HP P6000 EVAアレイファミリ固有の用語) ストレージボリュームの動的な複製です。元のストレージボリュームに加えられた変更は、ローカル複製リンクを介して、ミラークローンに反映されます。元のストレージボリュームとそのミラークローン間の複製は中断できます。各ストレージボリュームについてディスクアレイ上に1つのミラークローンを作成できます。

ミラーユニット(MU)番号

(HP P9000 XPアレイファミリ固有の用語) HP StorageWorks P9000 XPディスクアレイファミリのディスクアレイ上にある内部ディスク(LDEV)のセカンダリボリューム(S-VOL)を特定する0以上の整数。
「ファーストレベルミラー」を参照。

ミラーローテーション*(HP P9000 XPアレイファミリ固有の用語)*

「複製セットローテーション」を参照。

無人操作

「lights-out operation」を参照。

無人操作(lights-out operationまたはunattended operation)

オペレータの介在なしで、通常の営業時間外に実行されるバックアップ操作または復元操作。オペレータが手動で操作することなく、バックアップアプリケーションやサービスのマウント要求などが自動的に処理されます。

メールボックス

*(Microsoft Exchange Server固有の用語)*電子メールが配信される場所。管理者がユーザーごとに設定します。電子メールの配信場所として複数の個人用フォルダが指定されている場合は、メールボックスから個人用フォルダに電子メールがルーティングされます。

メールボックスストア

*(Microsoft Exchange Server固有の用語)*インフォメーションストアのうち、ユーザーメールボックス内の情報を維持する部分。メールボックスストアは、バイナリデータを格納するリッチテキスト. edbファイルと、ストリーミングネイティブインターネットコンテンツを格納する. stmファイルからなります。

メディアID

Data Protectorがメディアに割り当てる一意な識別子。

メディア集中管理データベース(CMMDB)

「CMMDB」を参照。

メディア管理セッション
初期化、内容のスキャン、メディア上のデータの確認、メディアのコピーなどのアクションをメディアに対して実行するセッション。

メディア状態要素
使用回数のしきい値と上書きのしきい値。メディアの状態の判定基準となります。

メディアセット
バックアップセッションでは、メディアセットと呼ばれるメディアのグループにデータをバックアップします。メディアの使用法によっては、複数のセッションで同じメディアを共有できます。

メディアの位置
バックアップメディアが物理的に収納されている場所を示すユーザー定義の識別子。"building 4"や"off-site storage"のような文字列です。

メディアのインポート
メディアに書き込まれているバックアップセッションデータをすべて再読み込みして、IDBに取り込むプロセス。これにより、メディア上のデータにすばやく、簡単にアクセスできるようになります。
「メディアのエクスポート」を参照。

メディアのエクスポート
メディアに格納されているすべてのバックアップセッション情報(システム、オブジェクト、ファイル名など)をIDBから削除するプロセス。メディア自体に関する情報やメディアとプールの関係に関する情報もIDBから削除されます。メディア上のデータは影響されません。
「メディアのインポート」を参照。

メディアの種類
メディアの物理的な種類(DDSやDLTなど)。

メディアの状態
メディア状態要素から求められるメディアの品質。テープメディアの使用頻度が高く、使用時間が長ければ、読み書きエラーの発生率が高くなります。状態が[不良]になったメディアは交換する必要があります。

メディアの使用法
メディアの使用法は、既に使用されているメディアに対してバックアップをどのように追加するかを制御します。メディアの使用法は、[追加可能]、[追加不可能]、[増分のみ追加可能]のいずれかに設定できます。

メディアのボールティング
メディアを安全な別の場所に収納すること。メディアが復元に必要になった場合や、今後のバックアップにメディアを再使用する場合は、メディアをデータセンターに戻します。ボールティング手順は、会社のバックアップ戦略やデータ保護/信頼性ポリシーに依存します。

メディアプール

同じ種類のメディア(DDSなど)のセット。グループとして追跡されます。フォーマットしたメディアは、メディアプールに割り当てられます。

メディアラベル

メディアに割り当てられるユーザー定義の識別子。

メディア割り当てポリシー

メディアをバックアップに使用する順序を決定します。[厳格]メディア割り当てポリシーでは、特定のメディアに限定されます。[緩和]ポリシーでは、任意の適切なメディアを使用できます。[フォーマットされていないメディアを先に割り当てる]ポリシーでは、ライブラリ内に利用可能な非保護メディアがある場合でも、不明なメディアが優先されます。

ユーザーアカウント(Data Protector ユーザーアカウント)

Data Protectorおよびバックアップデータに対する無許可のアクセスを制限するために、Data Protectorユーザーとして許可を受けたユーザーにしかData Protectorを使用できないようになっています。Data Protector管理者がこのアカウントを作成するときには、ユーザーログオン名、ユーザーのログオン元として有効なシステム、およびData Protectorユーザーグループのメンバーシップを指定します。ユーザーがData Protectorのユーザーインタフェースを起動するか、または特定のタスクを実行するときには、このアカウントが必ずチェックされます。

ユーザーアカウント制御(UAC)

Windows Vista、Windows 7およびWindows Server 2008のセキュリティコンポーネント。管理者が権限レベルを上げるまで、アプリケーションソフトウェアを標準のユーザー権限に限定します。

ユーザーグループ

各Data Protectorユーザーは、ユーザーグループのメンバーです。各ユーザーグループにはユーザー権限のセットがあり、それらの権限がユーザーグループ内のすべてのユーザーに付与されます。ユーザー権限を関連付けるユーザーグループの数は、必要に応じて定義できます。 Data Protectorには、デフォルトでadmin、operator、userという3つのユーザーグループが用意されています。

ユーザーディスク割り当て

NTFSの容量管理サポートを使用すると、共有ストレージボリュームに対して、拡張された追跡メカニズムの使用およびディスク容量に対する制御が行えるようになります。Data Protectorでは、システム全体にわたるユーザーディスク割り当てが、すべてのユーザーに対して一度にバックアップされます。

ユーザープロファイル

*(Windows固有の用語)*ユーザー別に維持される構成情報。この情報には、デスクトップ設定、画面表示色、ネットワーク接続などが含まれます。ユーザーがログオンすると、そのユーザーのプロファイルがロードされ、Windows環境がそれに応じて設定されます。

ユーザー権限

特定のData Protectorタスクの実行に必要なパーミッションをユーザー権限またはアクセス権限と呼びます。主なユーザー権限には、バックアップの構成、バックアップセッションの開始、復元セッションの開始などがあります。ユーザーには、そのユーザーの所属先ユーザーグループに関連付けられているアクセス権限が割り当てられます。

ライター

*(Microsoft VSS固有の用語)*オリジナルボリューム上のデータの変更を開始するプロセス。主に、永続的なデータをボリューム上に書き込むアプリケーションまたはシステムサービスがライターとなります。ライターは、シャドウコピーの同期化プロセスにも参加し、データの整合性を保証します。

ライブラリ

オートチェンジャー、ジュークボックス、オートローダー、またはエクスチェンジャとも呼ばれます。ライブラリには、複数のレポジトリスロットがあり、それらにメディアが格納されます。各スロットがメディア(DDS/DATなど)を1つずつ格納します。スロット/ドライブ間でのメディアの移動は、ロボット機構によって制御され、メディアへのランダムアクセスが可能です。ライブラリには、複数のドライブを格納できます。

リカバリカタログ

*(Oracle固有の用語)*Recovery ManagerがOracleデータベースについての情報を格納するために使用するOracleの表とビューのセット。この情報は、Recovery ManagerがOracleデータベースのバックアップ、復元、および復旧を管理するために使用されます。リカバリカタログには、以下の情報が含まれます。

- Oracleターゲットデータベースの物理スキーマ
- データファイルおよびアーカイブログのバックアップセット
- データファイルのコピー
- アーカイブREDOログ
- ストアドスクリプト

リカバリカタログデータベース

*(Oracle固有の用語)*リカバリカタログスキーマを格納するOracleデータベース。リカバリカタログはターゲットデータベースに保存しないでください。

リカバリカタログデータベースへのログイン情報

*(Oracle固有の用語)*リカバリカタログデータベース(Oracle)へのログイン情報の形式は*<user_name>/<password>@<service>*で、ユーザー名、パスワード、サービス名の説明は、Oracleターゲットデータベースへの Oracle SQL*Net V2ログイン情報と同じです。ただし、この場合の*service*はOracleターゲットデータベースではなく、リカバリカタログデータベースに対するサービス名となります。

ここで指定するOracleユーザーは、Oracleのリカバリカタログのオーナーでなければならないことに注意してください。

リカバリファイル

*(Oracle固有の用語)*リカバリファイルはフラッシュリカバリ領域に存在するOracle固有のファイルで、現在の制御ファイル、オンラインREDOログ、アーカイブREDOログ、フラッシュバックログ、制御ファイル自動バックアップ、データファイルコピー、およびバックアップピースがこれにあたります。
「フラッシュリカバリ領域」を参照。

リサイクルまたは保護解除

メディア上のすべてのバックアップデータのデータ保護を解除して、以降のバックアップで上書きできるようにするプロセス。同じセッションに所属しているデータのうち、他のメディアに置かれているデータも保護解除されます。リサイクルを行っても、メディア上のデータ自体は変更されません。

リムーバブル記憶域の管理データベース

*(Windows固有の用語)*Windowsサービスの1つ。リムーバブルメディア(テープやディスクなど)と記憶デバイス(ライブラリ)の管理に使用されます。リムーバブル記憶域により、複数のアプリケーションが同じメディアリソースを共有できます。

ローカル復旧とリモート復旧

リモート復旧は、SRDファイルで指定されているMedia Agentホストがすべてアクセス可能な場合にのみ実行されます。いずれかのホストがアクセス不能になっていると、ディザスタリカバリプロセスがローカルモードにフェイルオーバーされます。これは、ターゲットシステムにローカルに接続しているデバイスが検索されることを意味します。デバイスが1台しか見つからない場合は、そのデバイスが自動的に使用されます。複数のデバイスが見つかった場合は、デバイスが選択できるプロンプトが表示され、ユーザーが選択したデバイスが復元に使用されます。

ローカル連続レプリケーション

*(Microsoft Exchange Server固有の用語)*ローカル連続レプリケーション(LCR)はストレージグループの完全コピー(LCRコピー)を作成および維持するシングルサーバー ソリューション。LCRコピーは元のストレージグループと同じサーバーに配置されます。LCRコピーが作成されると、変更伝播(ログリプレイ)テクノロジで最新に保たれます。LCRの複製機能では未複製のログが削除されません。この動作の影響により、ログを削除するモードでバックアップを実行しても、コピー中のログと複製に十分な余裕がある場合、実際にはディスクの空き容量が解放されない場合があります。
LCRコピーへの切り替えは数秒で完了するため、LCRコピーはディザスタリカバリに使用されます。元のデータとは異なるディスクに存在するLCRコピーをバックアップに使用すると、プロダクションデータベースの入出力の負荷が最小になります。

複製されたストレージグループは、Exchangeライターの新しいインスタンス(Exchange Replication Service)として表示され、通常のストレージグループのようにVSSを使用してバックアップできます。「クラスター連続レプリケーションおよびExchange Replication Service」を参照。

ロギングレベル

ロギングレベルは、バックアップ、オブジェクトのコピー、またはオブジェクトの集約時にファイルとディレクトリに関する情報をどの程度まで詳細にIDBに記録するかを示します。バックアップ時のロギングレベルに関係なく、データの復元は常に可能です。Data Protectorには、[すべてログに記録]、[ディレクトリレベルまでログに記録]、[ファイルレベルまでログに記録]、および[ログなし]の4つのロギングレベルがあります。ロギングレベル設定によって、IDBのサイズ増加、バックアップ速度、および復元データのブラウザのしやすさが影響を受けます。

ログインID

*(Microsoft SQL Server固有の用語)*Microsoft SQL Serverにログインするためにユーザーが使用する名前。Microsoft SQL Serverのsysloginシステムテーブル内のエントリに対応するログインIDが有効なログインIDとなります。

ロック名

別のデバイス名を使うことで同じ物理デバイスを違う特性で何度も構成することができます。そのようなデバイス(デバイス名)が複数同時に使用された場合に重複を防ぐ目的で、デバイス構成をロックするためにロック名が使用されます。ロック名はユーザーが指定する文字列です。同一の物理デバイスを使用するデバイス定義には、すべて同じロック名を使用します。

論理ログファイル

論理ログファイルは、オンラインデータベースバックアップの場合に使用されます。変更されたデータがディスクにフラッシュされる前に書き込まれるファイルです。障害発生時には、これらの論理ログファイルを使用することで、コミット済みのトランザクションをすべてロールフォワードするとともに、コミットされていないトランザクションをロールバックすることができます。

論理演算子

オンラインヘルプシステムの全文検索には、AND、OR、NOT、NEARの各ブール演算子を使用できます。複数の検索条件をブール演算子で組み合わせて指定することで、検索対象をより正確に絞り込むことができます。複数単語の検索に演算子を指定しなければ、ANDを指定したものとみなされます。たとえば、「manual disaster recovery」という検索条件は、「manual AND disaster AND recovery」と同じ結果になります。

ワイルドカード文字　1文字または複数文字を表すために使用できるキーボード文字。たとえば、通常、アスタリスク(*)は1文字以上の文字を表し、疑問符(?)は1文字を示します。ワイルドカード文字は、名前により複数のファイルを指定するための手段としてオペレーティングシステムで頻繁に使用されます。

索引

A

A.06.00からのアップグレード
　SAPR/3用統合ソフトウェア, 283
ACSクライアント, 122
ADIC/GRAUライブラリ
　Media Agentのインストール, 122
　Media Agentをクライアントにインストール, 124
　クライアントの準備, 123
　ドライブの接続, 123
ADICライブラリ
　「ADIC/GRAUライブラリ」を参照。
AIXクライアント
　インストール, 115
　バックアップデバイスの接続, 117
allow_hostsファイル, 232, 233
Application Recovery Manager
　アップグレード, 289
AutoPassユーティリティ
　アンインストール、HP-UXの場合, 247
　アンインストール、Solarisの場合, 251
　アンインストール、Windowsの場合, 246
　インストール、UNIXの場合, 49
　インストール、Windowsの場合, 60
　ライセンス, 328

C

Cell Manager, 53
Cell Request Server (CRS)サービス, 53, 61
DataProtector A.06.00、A.06.10、およびA.06.11からのアップグレード、HP-UXの場合, 266, 270
KeyManagement Server (KMS), 53
KeyManagement Server (KMS)サービス, 61
MediaManagement Daemon (MMD)サービス, 53, 61
RaimaDatabase Server (RDS)サービス, 53, 61
SSEのアップグレード, 288
UIProxyサービス, 62
Veritas Volume Managerの構成、Microsoft Cluster Server, 393
アップグレード、MC/ServiceGuardの場合, 301
アップグレード、Microsoft Cluster Serverの場合, 305
アンインストール、HP-UXの場合, 247
アンインストール、Linuxの場合, 253
アンインストール、MC/ServiceGuardの場合, 247
アンインストール、Solarisの場合, 250
アンインストール、Windowsの場合, 245
インストール、HP-UX, 47
インストール、HP-UXの場合、ネイティブツールの使用, 362
インストール、Linuxの場合、ネイティブツールの使用, 366
インストール、MC/ServiceGuard, 194
インストール、MicrosoftCluster Server, 195
インストール、Solarisの場合, 47
インストール、Solarisの場合、ネイティブツールの使用, 364
インストール、Windowsの場合, 55
インストール手順, 44
インストールの前提条件、UNIXの場合, 45
インストールの前提条件、Windowsの場合, 55
インストールのトラブルシューティング、UNIXの場合, 54
環境変数の設定、UNIXの場合, 53
概念, 31
機能, 38
構成の変更のチェック, 276
システムの選択, 38, 39
手動でアップグレード、UNIXの場合, 356
自動構成されるファイル、UNIXの場合, 51
準備、NISサーバー, 394
ソフトウェアコンポーネントの変更, 257
ディレクトリ構造、UNIXの場合, 50
トラブルシューティング, 54, 347, 349, 353, 357, 359
名前の変更, 395
保護の概念, 223
Cell Managerのインストール
HP-UXシステムの場合, 47
Linuxシステムの場合, 47
Linuxの場合、ネイティブツールの使用, 366
MC/ServiceGuardシステム, 194
Microsoft Cluster Serverシステム, 195
Solarisシステムの場合, 47
Solarisの場合、ネイティブツールの使用, 364
Windowsシステム, 55
前提条件、UNIXの場合, 45
前提条件、Windowsの場合, 55
ネイティブツールを使用したHP-UXシステムへの, 362
Cell RequestServer (CRS)サービス, 53, 61
cell_infoファイル,
CLI
「コマンドラインインターフェース」を参照。

CRS
「Cell Request Server (CRS)サービス」を参照。

D

DASクライアント, 122
Data Protector 6.20へのアップグレード
P6000 EVAアレイ用統合ソフトウェア, 285
Data Protector A.05.50からのアップグレード
Manager-of-Managers, 286
Data Protector A.06.00、A.06.10、A.06.11からのアップグレード
Oracle用統合ソフトウェア, 282
前提条件, 266
Data Protector A.06.00、A.06.10、およびA.06.11からのアップグレード
Cell Manager、HP-UXの場合, 266, 270
Cell Manager、MC/ServiceGuardの場合, 301
Cell Manager、Microsoft Cluster Serverの場合, 305
omnisvコマンド, 266
Windows用インストールサーバー, 272
インストールサーバー、HP-UXの場合, 266
概要, 266
クライアント, 279
クライアント、MC/ServiceGuardの場合, 281
クライアント、Microsoft Cluster Serverの場合, 307
構成の変更のチェック, 276
Data Protector Java GUI, 110
クライアントのセルへの追加, 87
デフォルトのポート番号の変更, 390
DB2用統合ソフトウェア、インストール, 165
DCBF
「詳細カタログバイナリファイル」を参照。
debugオプション
概要, 359
deny_hostsファイル, 232
Disk Agent
概念, 32
構成、HPOpenVMSの場合, 143
DNS
omnicheckコマンド, 345
セル内の接続の確認, 344
DNSチェックツール, 387
DVD-ROM
インストールDVD-ROM一覧, 36

E

ESX Serverクライアント
インストール, 114

G

General Media Agent
インストールのチェック、NovellNetWare, 431
globalファイル, 276
GRAUライブラリ
「ADIC/GRAUライブラリ」を参照。
GUI
「グラフィカルユーザーインタフェース」を参照。

H

HP
テクニカルサポート, 29
HP OpenVMSクライアント
Disk Agentの構成, 143
Media Agentの構成, 144
アンインストール, 244
インポート, 215
HP P6000 EVAアレイファミリ用統合ソフトウェア
インストール, 167

HP StorageWorks 330fxライブラリ、SCSI IDの設定, 416
HP StorageWorks DAT 24テープドライブ、接続, 421
HP StorageWorks DLTライブラリ24/48スロット、接続, 425
HP StorageWorksP4000 SANソリューション用統合ソフトウェア
　インストール, 181
HP StorageWorksP9000 XPディスクアレイファミリ用統合ソフトウェア
　インストール, 174
HP Surestore 12000eオートローダー、接続, 423
HP-UX 11.23へのアップグレード, 291
HP-UX Cell Manager
　Data Protector A.06.00、A.06.10、A.06.11からのアップグレード, 266
　Data Protector A.06.00、A.06.10、およびA.06.11からのアップグレード, 270
　PA-RISCからIA-64への移行, 291
　アンインストール, 247
　インストール, 47
　インストール、ネイティブツールの使用, 362
　インストールの前提条件, 45
　インストールのトラブルシューティング, 54
　環境変数の設定, 53
　自動構成されるファイル, 51
　ディレクトリ構造, 50
　トラブルシューティング, 54, 353, 357
HP-UX インストールサーバー
　インストール、ネイティブツールの使用, 368
HP-UXクライアント
　インストール, 99
　トラブルシューティング, 349
　バックアップデバイスの接続, 102
HPDEVBRA.NLMファイル, 435
HPUMA.NLMファイル, 435

I

IBM HACMP Cluster
　クライアントのインストール, 210
IDB
　アップグレードのトラブルシューティング, 353
　サイズの増加, 38
inet.conf
　ファイル,
inet.logファイル, 230, 231, 233, 305
Inetサービス, 53, 61
Informix用統合ソフトウェア、インストール, 159
infsコマンド, 406
installation_serversファイル, 67
ioscanコマンド, 403, 406, 408

J

Java GUI Server
　ポート番号の変更, 390
Java GUIクライアント, 240, 244
Java GUIサーバー, 46, 55, 62

K

Key Management Server (KMS), 53, 61
KMS
　「Key Management Server (KMS)サービス」を参照。

L

Linux CellManager
アンインストール, 253
インストール, 47
インストール、ネイティブツールの使用, 366
インストールの前提条件, 45
インストールのトラブルシューティング, 54
環境変数の設定, 53
自動構成されるファイル, 52
ディレクトリ構造, 50
トラブルシューティング, 54
Linux インストールサーバー
インストール、ネイティブツールの使用, 375
Linuxクライアント
インストール, 109
バックアップデバイスの接続, 113
リモートインストールのトラブルシューティング, 112
Lotus用統合ソフトウェア、インストール, 166

M

Mac OS Xクライアント
インストール, 114
Manager-of-Managers
DataProtector A.05.50からのアップグレード, 286
アップグレードの概要, 265
MC/ServiceGuard
CellManagerのアップグレード, 301
CellManagerのアンインストール, 247
CellManagerのインストール, 194
Data Protector A.06.00、A.06.10、およびA.06.11からのクライアントアップグレード, 281
inet.logファイルに大量のログが記録される場合, 233
インストールサーバーのアンインストール, 247
インポート, 219
クライアントのインストール, 194
Media Agent
ADIC/GRAUライブラリ用のインストール, 124
StorageTekACSライブラリ用のインストール, 129
概念, 32
構成、HPOpenVMSの場合, 144
構成、NovellNetWare, 137
タイプ, 32
Media Management Daemon (MMD), 61
Media Management Daemon (MMD)サービス, 53
Microsoft Cluster Server
Cell ManagerとVeritas Volume Managerの構成, 393
Cell Managerのアップグレード, 305
Cell Managerのインストール, 195
インポート, 217
エクスポート, 223
クライアントとVeritas Volume Managerの構成, 393
クライアントのアップグレード, 307
クライアントのインストール, 204
Microsoft ExchangeServer 2003/2007用統合ソフトウェア
インストール, 155
Microsoft ExchangeServer 2010用統合ソフトウェア
インストール, 155

MicrosoftExchange用統合ソフトウェア
HP P6000 EVAアレイファミリを備えたシステムへのインストール, 173
HP StorageWorks P9000 XPディスクアレイファミリを備えたシステムへのインストール, 180
Microsoft Installer, 56, 264, 305, 347
Microsoft SharePointPortal Server用統合ソフトウェア
インストール, 157
Microsoft SharePointServer 2007用統合ソフトウェア
インストール, 158
Microsoft SQL用統合ソフトウェア
EMC Symmetrixディスクアレイを備えたシステムへのインストール, 186
HP P6000 EVAアレイファミリを備えたシステムへのインストール, 173
HP StorageWorks P9000 XPディスクアレイファミリを備えたシステムへのインストール, 181
インストール, 157
Microsoft ボリュームシャドウコピー用統合ソフトウェア、インストール, 166
Microsoftサーバークラスター
インストールのためのWindows Server 2008システムの準備, 390
Microsoftターミナルサービスクライアント, 56
MMD
「Media Management Daemon (MMD) サービス」を参照。
MSI
「Microsoft Installer」を参照。

N

NDMP Media Agent、概念, 32
NDMPクライアント、インポート, 215
NDMP用統合ソフトウェア、インストール, 165
netstat,
NISサーバー、準備, 394
NNM用統合ソフトウェア、インストール, 165
Novell NetWare Cluster Services
インポート, 219
クライアントのインストール, 208
制限、フェイルオーバー, 208
Novell NetWareクライアント
General Media Agentのインストールのチェック, 431
HPDEVBRA.NLMファイル, 435
HPUMA.NLMファイル, 435
Media Agentの構成, 137
インストール, 131
ネットワークトラフィックの最小化, 137
nsswitch.conf
ファイル, 395
nsswitch.confファイル, 395

O

omni_infoファイル, 261
omnicc, 318
omnicheckコマンド, 242, 345
omniinetプロセス
「Inetサービス」を参照。
omnircファイル, 277
omnisetup.sh, 253, 254
omnisetup.shコマンド
アップグレード, 266, 270
インストール, 148, 190
omnisvコマンド, 266
Oracle用統合ソフトウェア
Data Protector A.06.00、A.06.10、A.06.11からのアップグレード, 282
EMC Symmetrixディスクアレイを備えたシステムへのインストール, 182
HP P6000 EVAアレイファミリを備えたシステムへのインストール, 168
HP StorageWorks P9000 XPディスクアレイファミリを備えたシステムへのインストール, 175
アンインストール固有の問題, 259
インストール, 161

P

P6000 EVAアレイ用統合ソフトウェア
Data Protector 6.20へのアップグレード, 285
pkgaddユーティリティ, 251
pkgrmユーティリティ, 250, 251

R

Raima Database Server (RDS)サービス, 53, 61
RDS
「Raima Database Server (RDS)サービス」を参照。
rpmユーティリティ, 253, 254

S

SAP DB用統合ソフトウェア、インストール, 161
SAP R/3用統合ソフトウェア
HP P6000 EVAアレイファミリを備えたシステムへのインストール, 170
SAP R/3用統合ソフトウェア
A.06.00からのアップグレード, 283
EMC Symmetrixディスクアレイを備えたシステムへのインストール, 183
HP StorageWorks P9000 XPディスクアレイファミリを備えたシステムへのインストール, 176
インストール, 160
SCOクライアント
インストール, 119
バックアップデバイスの接続, 120
SCSIアドレス
「SCSIインタフェース」を参照。
SCSIインタフェース
IDの設定、HP StorageWorks 330fxライブラリ, 416
カーネルにロボティクスドライバを追加、HP-UX, 404
コントローラパラメータの設定、Windowsの場合, 408
テープドライバの使用、Windowsの場合, 397
未使用のSCSIアドレス、Windowsの場合, 415
未使用のアドレスの確認、HP-UX, 408
未使用のアドレスの確認、Solarisの場合, 410
ロボティクスドライバの無効化、Windowsの場合, 398
ロボティクスの構成、HP-UX, 401
SCSIコントローラ
「SCSIインタフェース」を参照。
SCSIテープドライバ
「SCSIインタフェース」を参照。
SCSIロボティクス
「SCSIインタフェース」を参照。
SCSIロボディクスドライバの無効化、Windowsの場合, 398
Seagate Viper 200 LTOテープドライブ、接続, 429
servicesファイル,
SolarisCell Manager
アンインストール, 250
インストール, 47
インストール、ネイティブツールの使用, 364
インストールの前提条件, 45
インストールのトラブルシューティング, 54
環境変数の設定, 53
自動構成されるファイル, 52
ディレクトリ構造, 50
トラブルシューティング, 349, 353, 357
Solaris インストールサーバー
インストール、ネイティブツールの使用, 369

Solarisクライアント
インストール, 102
構成、インストール後, 104
トラブルシューティング, 349
バックアップデバイスの接続, 108
SSE, 287
「シングルサーバー版」を参照。
sst.confファイル, 414
st.confファイル, 104, 411
STKACS
「StorageTek ACSライブラリ」を参照。
StorageTek ACSライブラリ
MediaAgentのインストール, 122
Media Agentをクライアントにインストール, 129
クライアントの準備, 128
ドライブの接続, 123
StorageTekライブラリ
「StorageTek ACSライブラリ」を参照。
swagentデーモン,
Sybase用統合ソフトウェア、インストール, 159

T

TCP/IP
設定のチェック、Windowsの場合, 386
Tru64クライアント
インストール, 117
バックアップデバイスの接続, 119

U

UIProxyサービス, 62

V

Veritas Cluster
インポート, 219
クライアントのインストール, 207
制限、フェイルオーバー, 207
Veritas Volume Manager
Cell Managerの構成、Microsoft Cluster Server, 393
クライアントの構成、Microsoft Cluster Server, 393
VLS自動移行
インストール, 186
前提条件, 187
VLSデバイス、インポート, 215
VMware Granular Recovery Extension
インストール, 163
VMware(レガシー)用統合ソフトウェア
インストール, 162
VSS用統合ソフトウェア
アップグレード, 284

W

Web Reporting、インストール, 192
Webサイト
HP,
HPメールニュース配信登録, 30
製品マニュアル, 19
Windows Cell Manager
32ビットから64ビットへの移行, 296
アンインストール, 245
トラブルシューティング, 347
Windows Server 2008
インストールのためのMicrosoftサーバークラスターの準備, 390
WindowsCell Manager
インストール, 55
インストールの前提条件, 55
インストールのトラブルシューティング, 62
トラブルシューティング, 353
Windowsクライアント
アンインストール, 243
インストール, 92
トラブルシューティング, 347, 351, 357
バックアップデバイスの接続, 97

Z

ZDB統合クライアント, 151
「統合」を参照。

あ

アクセス確認を使用可能にする
クライアントの場合, 228
セルで, 231
アクセス権限
rootアカウントへの追加、Linuxの場合, 112
アップグレード
ApplicationPrimary Manager, 289
CLIの変更, 437
globalファイル,
IDBのトラブルシューティング, 353
omnircファイル, 277
omnisetup.sh, 266
omnisetup.shコマンド, 270
omnisvコマンド, 266
SSEからData Protector 6.20, 287, 288
VSS用統合ソフトウェア, 284
アップグレード前の注意点, 263
概要, 263
手動、UNIXの場合, 356
制限事項, 264
手順, 264
トラブルシューティング、UNIXの場合, 353
トラブルシューティング、Windowsの場合, 347, 353
アップグレードのトラブルシューティング
Data Protectorソフトウェア、Windowsの場合, 347
Data Protectorパッチ, 354
IDBが使用できない, 353
MicrosoftInstallerに関する問題, 347
構成ファイルが使用できない, 353
アンインストール
AutoPassユーティリティ、HP-UXの場合, 247
AutoPassユーティリティ、Solarisの場合, 251
AutoPassユーティリティ、Windowsの場合, 246
CellManager、HP-UXの場合, 247
Cell Manager、Linuxの場合, 253
Cell Manager、MC/ServiceGuardの場合, 247
Cell Manager、Solarisの場合, 250
CellManager、Windowsの場合, 245
Oracle用統合ソフトウェア固有の問題, 259
pkgrmユーティリティ, 250, 251
rpmユーティリティ, 253, 254
インストールサーバー、HP-UXの場合, 247
インストールサーバー、Linuxの場合, 254
インストールサーバー、MC/ServiceGuardの場合, 247
インストールサーバー、UNIXの場合, 251
インストールサーバー、Windowsの場合, 245
概要, 242
クライアント、HP OpenVMS, 244
クライアント、リモート, 243
クラスタークライアント, 244
前提条件, 243
暗号化
暗号化キーの自動移行, 265

い

移行
HP-UX用CellManager、PA-RISCからIA-64へ, 291
Windows用CellManager、32ビットから64ビットへ, 296
ライセンス, 339

インストール
ADIC/GRAUライブラリ用のMediaAgent, 122, 124
AutoPassユーティリティ、UNIXの場合, 49
AutoPassユーティリティ、Windowsの場合, 60
Cell Managerのトラブルシューティング、Solarisの場合, 349
DB2用統合ソフトウェア, 165
HP P6000EVAファミリ用統合ソフトウェア, 167
HP StorageWorks P4000 SANソリューション用統合ソフトウェア, 181
HP StorageWorks P9000 XPディスクアレイファミリ用統合ソフトウェア, 174
Informix用統合ソフトウェア, 159
Lotus用統合ソフトウェア, 166
Microsoft Exchange Server 2003/2007用統合ソフトウェア, 155
Microsoft Exchange Server 2010用統合ソフトウェア, 155
Microsoft SharePoint Portal Server用統合ソフトウェア, 157
Microsoft SharePoint Server 2007用統合ソフトウェア, 158
Microsoft SQL用統合ソフトウェア, 157
Microsoftボリュームシャドウコピー用統合ソフトウェア, 166
NDMP用統合ソフトウェア, 165
NNM用統合ソフトウェア, 165
omnisetup.sh, 253, 254
Oracle用統合ソフトウェア, 161
pkgaddユーティリティ, 251
SAP DB用統合ソフトウェア, 161
SAP R/3用統合ソフトウェア, 160
StorageTek ACSライブラリ用のMedia Agent, 122
StorageTekACSライブラリ用のMedia Agent, 129
Sybase用統合ソフトウェア, 159
VLS自動移行クライアント, 186
VMware GranularRecovery Extension, 163
VMware(レガシー)用統合ソフトウェア, 162
WebReporting, 192
WindowsServer 2008でのMicrosoftサーバークラスターの準備, 390
一般的な手順, 33
各国語版ユーザーインタフェース, 189
仮想環境統合ソフトウェア, 162
概要, 31
クライアントのインストール、概要, 72
クライアントの確認, 352
クライアントのトラブルシューティング、UNIXの場合, 349
クライアントのトラブルシューティング、Windowsの場合, 351
クラスター対応Cell Manager, 194
クラスター対応クライアント, 204
クラスター対応Cell Manager, 195
クラスター対応クライアント, 194, 207, 208, 210
クラスター対応統合ソフトウェア, 154
恒久ライセンスパスワード, 328, 333
コンポーネント
「インストールコンポーネント」を参照。
シングルサーバー版, 191
実行トレースファイルの作成, 360
ソフトウェアコンポーネント, 76
ソフトウェアコンポーネントコード, 148
デバッグ, 360
統合, 151
統合ソフトウェア、概要, 151
トラブルシューティング、Windowsの場合, 347
リモートインストール、概要, 82
リモート、概念, 34
ログファイル, 357
ローカルクライアント, 92, 139, 146

インストールコンポーネント
Disk Agent, 32
General Media Agent, 32
MediaAgent, 32
NDMP Media Agent, 32
インストールサーバー, 31
ユーザーインタフェース, 31
インストールサーバー
DataProtector A.06.00、A.06.10、およびA.06.11からのアップグレード、HP-UXの場合, 266
アンインストール、HP-UXの場合, 247
アンインストール、Linuxの場合, 254
アンインストール、MC/ServiceGuardの場合, 247
アンインストール、UNIXの場合, 251
アンインストール、Windowsの場合, 245
インストール、HP-UXの場合、ネイティブツールの使用, 368
インストール、Linuxの場合、ネイティブツールの使用, 375
インストール、Solarisの場合、ネイティブツールの使用, 369
インストール、UNIXの場合, 63
インストール、Windowsの場合, 68
インストール概要, 63
インストール手順, 44
インストールの前提条件、UNIXの場合, 63
インストールの前提条件、Windowsの場合, 68
概念, 31
手動でアップグレード、UNIXの場合, 356
セルへのインポート, 216
ディレクトリ構造、UNIXの場合, 50
インストールサーバー A.06.00、A.06.10、およびA.06.11、Windowsの場合
Data Protectorからのアップグレード, 272
インストールサーバーのインストール
HP-UXシステムの場合、ネイティブツールの使用, 368
Linuxシステムの場合、ネイティブツールの使用, 375
Solarisシステムの場合、ネイティブツールの使用, 369
UNIXシステムの場合, 63
Windowsシステム, 68
概要, 63
前提条件、UNIXの場合, 63
前提条件、Windowsの場合, 68
インストールの準備
WindowsServer 2008上で実行するMicrosoftサーバークラスター, 390
インストールのデバッグ, 360
インストールのトラブルシューティング
Cell Manager、Solarisの場合, 349
Cell Manager、UNIXの場合, 54
Cell Manager、Windowsの場合, 62
Data Protectorソフトウェア、Windowsの場合, 347
debugオプション, 359
Mac OS Xクライアント, 350
Microsoft Installerに関する問題, 347
omnicheckコマンド, 345
swagentデーモン,
各国語版ユーザーインタフェース, 187
クライアント、HP-UXの場合, 350
実行トレースファイル, 359
デバッグ, 360
リモートインストール、Linuxの場合, 112
リモートインストール、UNIXの場合, 349
リモートインストール、Windowsの場合, 351
ログファイル, 357

インポート
HP OpenVMSクライアント, 215
NDMPクライアント, 215
VLSデバイス, 215
インストールサーバー, 216
クライアント, 213
クラスター, 217
複数のLANカードが構成されたクライアント, 215

え

エクスポート
MicrosoftCluster Serverクライアント, 223
クライアント, 221

か

各国語版ユーザーインタフェース, 187
「ユーザーインタフェース」を参照。
各国語版ユーザーインタフェースのトラブルシューティング, 187
確認
インストールされたライセンス, 334
クライアントのインストール, 352
セル内のDNS接続, 344
パッチ, 240
必要なライセンスパスワード, 338
未使用のSCSIアドレス、HP-UX, 408
未使用のSCSIアドレス、Solarisの場合, 410
未使用のアドレスの確認、Windowsの場合, 415
仮想環境統合ソフトウェア
インストール, 162
仮想サーバー、セルへのインポート, 217
仮想テープライブラリ
ライブラリ容量の変更, 278
環境変数、UNIX Cell Managerでの設定, 53
関連ドキュメント, 19
関連ライセンス, 310
カーネル
SCSIロボティクスドライバの追加、HP-UX, 404
再ビルド、HP-UX, 404
カーネルの再ビルド、HP-UX, 404
概念
Cell Manager, 31
Disk Agent, 32
Media Agent, 32
NDMP Media Agent, 32
インストールサーバー, 31
インポート, 214
エクスポート, 220
クライアント, 31
グラフィカルユーザーインタフェース(GUI), 39, 40
セル, 31
バックアップ環境, 31
ユーザーインタフェース, 31
リモートインストール, 34

概要
Data Protector A.06.10およびA.06.11からのアップグレード, 266
debugオプション, 359
アップグレード, 263
アプリケーションクラスターパッケージのインポート, 217
アンインストール, 242
インストールサーバーのインストール, 63
クライアントのインストール, 72
クライアントのリモートインストール, 82
クラスター対応クライアントのインポート, 217
クラスター対応統合ソフトウェアのインストール, 154
実行トレースファイル, 359
製品構成, 309
ソフトウェアコンポーネント, 76
ソフトウェアコンポーネントの変更, 257
統合, 151
統合ソフトウェアのインストール, 151
バックアップデバイスの接続, 417
ライセンス, 336

き

規則
ドキュメント, 27
起動
GUI、UNIX, 40
機能拡張、ライセンス, 309

く

クライアント, 386
ADIC/GRAUライブラリの準備, 123
DataProtector A.06.00、A.06.10、およびA.06.11からのアップグレード, 279
Data Protector A.06.00、A.06.10、およびA.06.11からのアップグレード、MC/ServiceGuardの場合, 281
MicrosoftCluster Server、セルからエクスポート, 223
rootアクセス権限の追加、Linuxの場合, 112
StorageTekACSライブラリの準備, 128
Veritas Volume Managerの構成、Microsoft Cluster Server, 393
アクセス確認を解除する, 232
アクセス確認を使用可能にする, 228
アップグレード、Microsoft Cluster Serverの場合, 307
インストール、概要, 72
インストール後の構成、Solarisの場合, 104
インストールの確認, 352
概念, 31
クラスター対応、セルへのインポート, 217
クラスター対応統合ソフトウェアのインストール、概要, 154
セルからのエクスポート, 220
セルへのインポート, 213
ソフトウェアコンポーネントの変更, 257
デバイスファイルの作成、HP-UX, 406
デバイスファイルの作成、Solarisの場合, 414
統合ソフトウェアのインストール、概要, 151
トラブルシューティング, 347, 349, 351, 357, 359
バックアップデバイスを使用できるように構成、Solarisの場合, 411
保護, 228
保護の概念, 223
ホストからのアクセスの拒否, 232
リモートアンインストール, 243
リモートインストール、概要, 82
ローカルインストール、HP OpenVMS, 139
ローカルインストール、Novell NetWare, 131

クライアント、インストール
ADIC/GRAUライブラリ用のMedia Agent, 124
AIXシステムの場合, 115
DB2用統合ソフトウェア, 165
ESXServerシステムの場合, 114
HPOpenVMSシステム, 139
HP P6000 EVAアレイファミリ用統合ソフトウェア, 167
HP StorageWorks P4000 SANソリューション用統合ソフトウェア, 181
HP StorageWorks P9000 XPディスクアレイファミリ用統合ソフトウェア, 174
HP-UXシステムの場合, 99
IBM HACMPクラスターシステムの場合, 210
Informix用統合ソフトウェア, 159
Linuxシステムの場合, 109
Lotus用統合ソフトウェア, 166
MacOS Xシステム, 114
MC/ServiceGuardシステム, 194
MicrosoftCluster Serverシステム, 204
Microsoft Exchange Server 2003/2007用統合ソフトウェア, 155
Microsoft Exchange Server 2010用統合ソフトウェア, 155
Microsoft SharePoint Portal Server用統合ソフトウェア, 157
Microsoft SharePoint Server 2007用統合ソフトウェア, 158
MicrosoftSQL用統合ソフトウェア, 157
Microsoft ボリュームシャドウコピー用統合ソフトウェア, 166
NDMP用統合ソフトウェア, 165
NNM用統合ソフトウェア, 165
NovellNetWare Cluster Servicesシステム, 208
NovellNetWareシステム, 131
Oracle用統合ソフトウェア, 161
SAPDB用統合ソフトウェア, 161
SAPR/3用統合ソフトウェア, 160
SCOシステム, 119
Solarisシステムの場合, 102
StorageTek ACSライブラリ用のMedia Agent, 129
Sybase用統合ソフトウェア, 159
Tru64システム, 117
UNIXシステムの場合, 146
Veritas Clusterシステム, 207
VLS自動移行, 186
VMwareGranular Recovery Extension, 163
VMware(レガシー)用統合ソフトウェア, 162
Windowsシステム, 92
仮想環境統合ソフトウェア, 162
シングルサーバー版, 191
クライアントのインストール
AIXシステムの場合, 115
ESX Serverシステムの場合, 114
HP OpenVMSシステム, 139
HP-UXシステムの場合, 99
IBM HACMPクラスターシステムの場合, 210
Linuxシステムの場合, 109
Mac OS Xシステム, 114
MC/ServiceGuardシステム, 194
Microsoft Cluster Serverシステム, 204
Novell NetWare Cluster Servicesシステム, 208
Novell NetWareシステム, 131
SCOシステム, 119
Solarisシステムの場合, 102
Tru64システム, 117
UNIXシステムの場合, 146
Veritas Clusterシステム, 207
Windowsシステム, 92
クライアントのセルへの追加
DataProtector GUI,
Data Protector Java GUI, 87

クライアント、バックアップデバイスの接続
ADIC/GRAUライブラリドライブ, 123
AIXクライアント, 117
HP-UXクライアント, 102
Linuxクライアント, 113
SCOクライアント, 120
Solarisクライアント, 108
Tru64クライアント, 119
Windowsクライアント, 97
クラスター
Cell Managerのインストール, 195
MicrosoftCluster Server、セルからエクスポート, 223
アンインストール, 244
クライアントのインストール, 204, 207, 208
セルへのインポート, 217
ソフトウェアコンポーネントの変更, 257
統合ソフトウェアのインストール, 154
グラフィカルユーザーインタフェース(GUI)
Data Protector Java GUI, 40, 77
Data ProtectorJava GUI,
概念, 39, 40
起動、UNIX, 40
ビュー, 40

け

権限を認められたシステムのリスト、保護, 227
検証
ライセンスパスワード, 333

こ

恒久ライセンスパスワードの取得, 333
恒久ライセンスパスワードの取得, 328
構成
CellManagerとVeritas Volume Manager、MSCS, 393
DiskAgent、HP OpenVMSの場合, 143
MediaAgent, on HP OpenVMS, 144
MediaAgent、Novell NetWare, 137
SCSIロボティクス、HP-UX, 401
Solarisクライアント、インストール後, 104
Solarisクライアント、バックアップデバイスの使用前, 411
sst.confファイル, 414
st.confファイル, 104, 411
クライアントとVeritasVolume Manager、Microsoft Cluster Server, 393
構成ファイル
cell_info,
DataProtector A.06.00、A.06.10、A.06.11からのアップグレード後の変更のチェック, 276
inet.conf,
installation_servers, 67
nsswitch.conf, 395
omni_info, 261
omnirc, 277
sst.conf, 414
st.conf, 411
st.confファイル, 104
アップグレードに関する問題, 353
グローバル, 276
自動構成されるファイル、UNIXCell Managerの場合, 51
変更、Solarisクライアントのインストール, 104

コマンド, 266, 318
CLIの変更、アップグレード後, 437
infs, 406
ioscan, 403, 406, 408
netstat,
omnicc, 318
omnicheck, 242, 345
omnikeymigrate, 265
omnisetup.sh, 148, 190, 266, 270
omnisetup.sh ,
omnisv, 266
コマンドラインインタフェース(CLI), 32, 39

さ

削除
DataProtectorソフトウェアを手動で、UNIXの場合, 256
クライアントのアクセス確認, 232
ソフトウェアコンポーネント、UNIXの場合, 258, 261
ソフトウェアコンポーネント、Windowsの場合, 257
ソフトウェアコンポーネント、概要, 257
作成
実行トレースファイル、インストール, 359
デバイスファイル、HP-UX, 406
デバイスファイル、Solarisの場合, 414
デバイスファイル、Windowsの場合, 400

し

詳細カタログバイナリファイル
デフォルトの最大サイズの手動による変更, 277
使用
SCSIテープドライバ、Windowsの場合, 397
ライセンス, 263, 266
ログファイル, 357
使用権, 336
シングルサーバー版
DataProtector 6.20へのアップグレード, 287, 288
インストール, 191
制限事項, 191
製品概要、ライセンス, 337
複数のシステムからのアップグレード, 288
実行トレースファイル
debugオプション, 359
作成, 360
準備、NISサーバー, 394

す

スターターパック、ライセンス, 309

せ

制限事項
Manager-of-Managersのアップグレード, 265
Windowsシステム, 68, 93
アップグレード, 264
シングルサーバー版, 191
セキュリティ
allow_hostsファイル, 232, 233
deny_hostsファイル, 232
inet.logファイルに大量のログが記録される場合, 233
クライアントのアクセス確認を解除する, 232
クライアントの保護を使用可能にする, 228
権限を認められたシステムのリスト, 227
セルの保護を使用可能にする, 231
潜在的な問題点, 227
ホストからのアクセスの拒否, 232

設定
SCSIID、HP StorageWorks 330fxライブラリ, 416
SCSIコントローラパラメータ、Windowsの場合, 408
環境変数、UNIX CellManagerの場合, 53
セル
DNS接続の確認, 344
Microsoft ClusterServerクライアントのエクスポート, 223
アップグレード、概要, 264
インストールサーバーのインポート, 216
概念, 31
クライアントのインポート, 213
クライアントのエクスポート, 220
クライアントの保護設定, 228
クラスターのインポート, 217
保護を使用可能にする, 231
ライセンス, 309, 310
前提条件
Cell Managerのインストール、UNIXの場合, 45
Cell Managerのインストール、Windowsの場合, 55
Data Protector A.06.00、A.06.10、およびA.06.11からのアップグレード, 266
VLS自動移行, 187
インストールサーバーのインストール、UNIXの場合, 63
インストールサーバーのインストール、Windowsの場合, 68

そ

ソフトウェアコンポーネント
依存関係、HP-UXの場合, 258
依存関係、Solarisの場合, 260, 261
概要, 76
コンポーネントコード, 148
削除、UNIXの場合, 258, 261
削除、Windowsの場合, 257
追加、HP-UXの場合, 258
追加、Linuxへの, 260
追加、Solarisの場合, 259
追加、Windowsの場合, 257
変更、概要, 257
変更、クラスタークライアントの場合, 257
ソフトウェアコンポーネントの追加
Solarisシステムの場合, 259
ソフトウェアコンポーネントの追加
Linuxシステムへの, 260
Windowsシステムの場合, 257
概要, 257
ソフトウェアコンポーネントの追加
HP-UXシステムの場合, 258

た

対象読者, 19
大量のログ, 233
ターミナルサービスクライアント, 56

ち

チェック
GeneralMedia Agentのインストール、Novell NetWare, 431
TCP/IPの設定、Windowsの場合, 386
クライアントのインストール, 352
ライセンス, 310
ログファイル、インストール, 357

つ

追加
アクセス権限、Linuxの場合, 112
カーネルのSCSIロボティクスドライバ、HP-UX, 404

て

テクニカルサポート
HP, 29
サービスロケータWebサイト, 30
テープドライバ
「SCSIインタフェース」を参照。
デバイスファイル
作成、HP-UX, 406
作成、Solarisの場合, 414
作成、Windowsの場合, 400
デフォルトポート、変更, 388
データベースのサイズの増加
「IDB」を参照。

と

統合
Oracle、UNIXの場合, 282
Oracleのアップグレード、Windowsの場合, 282
P6000 EVAアレイ, 285
P6000 EVAアレイのアップグレード, 285
SAP R/3、UNIXの場合, 283
SAPR/3のアップグレード、Windowsの場合, 283
VSSのアップグレード,
概要, 151
クラスター対応、インストール, 154
リモートインストール, 154
ローカルインストール, 153
統合クライアント, 151
「統合」を参照。
統合ソフトウェア、インストール
DB2用統合ソフトウェア, 165
HP P6000 EVAアレイファミリ用統合ソフトウェア, 167
HP StorageWorks P4000 SANソリューション用統合ソフトウェア, 181
HP StorageWorks P9000 XPディスクアレイファミリ用統合ソフトウェア, 174
Informix用統合ソフトウェア, 159
Lotus用統合ソフトウェア, 166
Microsoft Exchange 2003/2007用統合ソフトウェア, 155
Microsoft Exchange Server 2010用統合ソフトウェア, 155
Microsoft SharePoint Portal Server用統合ソフトウェア, 157
Microsoft SharePoint Server 2007用統合ソフトウェア, 158
Microsoft SQL用統合ソフトウェア, 157
Microsoftボリュームシャドウコピー用統合ソフトウェア, 166
NDMP用統合ソフトウェア, 165
NNM用統合ソフトウェア, 165
Oracle用統合ソフトウェア, 161
SAP DB用統合ソフトウェア, 161
SAP R/3用統合ソフトウェア, 160
Sybase用統合ソフトウェア, 159
VMware(レガシー)用統合ソフトウェア, 162
VMware統合ソフトウェア, 163
仮想環境統合ソフトウェア, 162
トレースファイル
「実行トレースファイル」を参照。
ドキュメント
HP Webサイト, 19
意見の送付, 30
関連ドキュメント, 19
規則, 27
ドメインネームシステム
「DNS」を参照。
ドライブライセンス, 309

ね

ネットワークトラフィックの最小化、Novell NetWareクライアント, 137

は

バックアップ環境の概念, 31
バックアップデバイス
SCSIIDの設定、HP StorageWorks 330fxライブラリ, 416
バックアップデバイス、接続
ADIC/GRAUライブラリドライブ, 123
AIXクライアント, 117
HPStorageWorks DAT 24テープドライブ, 421
HPStorageWorks DLTライブラリ24/48スロット, 425
HPSurestore 12000eオートローダー, 423
HP-UXクライアント, 102
Linuxクライアント, 113
SCOクライアント, 120
Seagate Viper 200 LTOテープドライブ, 429
Solarisクライアント, 108
Tru64クライアント, 119
Windowsクライアント, 97
概要, 417
バックアップデバイスの接続
ADIC/GRAUライブラリドライブ, 123
AIXクライアント, 117
HP StorageWorks DAT 24テープドライブ, 421
HP StorageWorks DLTライブラリ24/48スロット, 425
HP Surestore 12000eオートローダー, 423
HP-UXクライアント, 102
Linuxクライアント, 113
SCOクライアント, 120
Seagate Viper 200 LTOテープドライブ, 429
Solarisクライアント, 108
Tru64クライアント, 119
Windowsクライアント, 97
概要, 417
パッチ
omnicheckコマンド, 242
確認, 240

ひ

ビュー、グラフィカルユーザーインタフェース, 40

ふ

ファイル
allow_hosts,
HPDEVBRA.NLM,
allow_hosts, 232, 233
deny_hosts, 232
HPUMA.NLM, 435
services,
複数のLANカードが構成されたクライアント、インポート, 215

プロセス
Cell Request Server (CRS)サービス, 53, 61
Inetサービス, 53, 61
Key Management Server (KMS), 53, 61
Media Management Daemon (MMD), 61
Media Management Daemon (MMD) サービス, 53
Raima Database Server (RDS)サービス, 53, 61
UIProxyサービス, 62

へ

ヘルプ
取得, 29
変更
Cell Manager名, 395
ソフトウェアコンポーネント, 257
デフォルトポート, 388

ほ

保護
クライアント, 228
セル, 231
ホストからのアクセスの拒否, 232

み

未使用のSCSIアドレス
「SCSIインタフェース」を参照。

め

メールニュース配信登録、HP, 30

ゆ

ユーザーインタフェース
「コマンドラインインタフェース(CLI)、グラフィカルユーザーインタフェース(GUI)」を参照。
各国語版ユーザーインタフェースのインストール, 189
各国語版ユーザーインタフェースのインストールのトラブルシューティング, 187
概念, 31
システムの選択, 39

ら

ライセンス, 336
AutoPassユーティリティ, 328
CellManager, 310
DataProtector A.06.00、A.06.10、およびA.06.11からのアップグレード, 266
SSEからのアップグレード, 288
一時パスワード, 327
インストールされたライセンスの確認, 334
エンティティーベースのライセンス, 310
概要, 336
機能拡張, 309
緊急用パスワード, 327
恒久パスワード, 327
恒久パスワード、取得とインストール, 328, 333
恒久パスワードの取得とインストール, 333
恒久パスワードの取得とインストール, 328
集中型ライセンス、構成, 335
スターターパック, 309
製品構成, 309, 336, 337
ディスクへのアドバンストバックアップ, 278
ドライブライセンス, 309
パスワードの検証, 333
パスワードのタイプ, 327
必要なパスワードの確認, 338
容量ベースのライセンス, 311, 315, 318
ライセンスの移行, 339
ライセンスの移動, 334
ライセンスの使用、アップグレード後, 266, 288
ライセンスのチェックとレポート, 310
ライセンスフォーム, 340
ライセンスレポートの作成, 318
ライセンスの移動, 334
ライセンスのレポート, 310
ライセンスフォーム, 340

り

リモートインストール
クライアント, 82
統合, 154
トラブルシューティング、Linuxの場合, 112

ろ

ログファイル
inet.log, 230, 231, 233, 305
説明, 358
チェック、インストール, 357
場所, 358
ロボティクス
「SCSIインタフェース」を参照。
ローカルインストール、クライアント, 92, 139, 146