Hewlett Packard
Enterprise

Data Protector

ソフト ウェアバージョン: 10.00

インストールガイド

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

ご注意

保証

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

ここに記載する情報は、予告なしに変更されることがあります。

権利の制限

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

著作権について

商標について

Adobe™はAdobe Systems Incorporatedの商標です。

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

UNIX®は、The Open Groupの登録商標です。

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

ドキュメントの更新情報

このマニュアルの表紙には、以下の識別情報が記載されています。

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

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

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

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

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

サポート

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

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

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

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

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

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

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

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

目次

第1章: インストール手順の概要 19
インストール手順の概要 19
リモートインストールの概念 21
Data Protectorインストールメディア 22
Cell Managerシステムの選択 23
Data Protectorユーザーインターフェイスシステムの選択 24
Data Protectorグラフィカルユーザーインターフェイス 24

第2章: Data Protectorのインストール 26
Data Protector Cell Managerおよびインストールサーバーのインストール 26
UNIX Cell Managerのインストール Cell Manager 27
前提条件 27
クラスター対応 Cell Manager 29
推奨事項 29
カーネルパラメーターの設定 29
インストール手順 29
HP-UXおよびLinuxシステムにインストールされるディレクトリの構造 30
自動での起動とシャットダウンの構成 31
環境変数の設定 33
次に行う手順 33
Windows Cell Managerのインストール Cell Manager 34
前提条件 34
Microsoftターミナルサービスクライント 35
推奨事項 36
インストール手順 36
インストール後の処理 40
トラブルシューティング 41
次に行う手順 42
インストールサーバーのインストール 42
UNIXシステム用のインストールサーバーのインストール 42
前提条件 42
推奨事項 43
インストール手順 44
次に行う手順 44
Windowsシステム用のインストールサーバーのインストール 45
前提条件 45
制限事項 46
インストール手順 46

次に行う手順 49
Data Protectorシングルサーバー版のインストール 49
Windows用SSEの制限 49
SSEへのアップグレード(HP-UX)での制限事項 50
パスワードのインストール 50
インストールを確認する 50
前提条件 50
手順 51
Data Protector Inetサービス構成について 51
統合 51
Windowsドメインユーザーアカウントでinetサービスを実行する 51
Data Protector Inetサービスユーザーの偽装のためのユーザーアカウントの設定 52
Data Protector GUIを使用する 52
手順 52
Data Protector CLIを使用する場合 52
Data ProtectorInetアカウントを変更する 53
前提条件 53
Windowsシステムの場合 53

第3章: Data Protectorクライアントのインストール 54
統合 55
Data Protectorコンポーネント 57
Data Protectorサービス 61
Windowsクライアントのインストール 62
前提条件 62
制限事項 62
推奨事項 63
自動ディザスタリカバリ 63
クラスター対応クライアント 63
ローカルインストール 63
ローカルにインストールされたクライアントのインポート 66
インストールサーバーのローカルインストール 68
Windowsシステムへのバックアップデバイスの接続 70
次に行う手順 71
HP-UXクライアントのインストール 71
前提条件 71
リモートインストール 72
ローカルインストール 72
クラスター対応クライアント 72
HP-UXのカーネル構成のチェック 73
バックアップデバイスのHP-UXシステムへの接続 74
Solarisクライアントのインストール 75

前提条件 75
リモートインストール 75
ローカルインストール 76
クラスター対応クライアント 76
インストール後の構成 76
Solarisシステムへのバックアップデバイスの接続 80
次に行う手順 81
Linuxクライアントのインストール 81
前提条件 82
自動ディザスタリカバリ 82
HPE Serviceguardクラスター 83
Novell Open Enterprise Server (OES) 83
リモートインストール 83
ローカルインストール 83
Linuxシステムへのバックアップデバイスの接続 83
次に行う手順 84
ESX Serverクライアントのインストール 84
IBM AIXクライアントのインストール 85
前提条件 85
IBM HACMPクラスター 85
リモートインストール 85
ローカルインストール 86
AIXクライアントへのバックアップデバイスの接続 86
次に行う手順 86
Mac OS Xクライアントのインストール 86
HP OpenVMSクライアントのインストール 89
前提条件 89
インストール手順 89
クラスター環境でのインストール 92
次に行う手順 94
リモートインストール 94
前提条件 94
推奨事項 95
セキュアシェルを使用したリモートインストール 96
OpenSSHのセットアップ 96
keychainのセットアップ 97
次に行う手順 98
クライアントのセルへの追加 98
トラブルシューティング 100
クライアントへのコンポーネントの追加 100
前提条件 100
UNIXおよびMac OS Xシステムでのローカルインストール 102
前提条件 102

インストール手順 102
ハードディスクからのインストール実行 104
次に行う手順 105
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 105
ライブラリドライブの接続 106
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 106
ADIC/GRAUライブラリ用のMedia Agentのインストール 107
前提条件 107
インストール手順 108
次に行う手順 109
StorageTekライブラリを使用するData Protectorクライアントの準備作業 109
前提条件 109
StorageTekライブラリ用のMedia Agentのインストール 111
次に行う手順 111

第4章: Data Protector統合クライアントのインストール 112
前提条件 112
リモートインストール 114
ローカルインストール 114
クラスター対応統合ソフトウェアのインストール 114
次に行う手順 115
Microsoft Exchange Serverクライアント 115
Data Protector Microsoft Exchange Server 2007 integration 115
前提条件 115
手順 115
Data ProtectorのMicrosoft Exchange Server用統合ソフトウェアのインストールの確認 117
Microsoft Exchange Serverの確認 117
Data Protector Microsoft Exchange Server 2010 integration 117
Data Protector Microsoft Exchange Server Single Mailbox用統合ソフトウェア 118
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 118
Data Protector Microsoft Exchange Server用 Granular Recovery Extension 119
前提条件 119
サポートされる環境 120
拡張機能のインストール 121
手順 121
拡張機能の削除 121
Microsoft SQL Serverクライアント 122
Microsoft SharePoint Serverクライアント 122
Data Protector Microsoft SharePoint Server 2007/2010/2013 integration 122
Data Protector Microsoft SharePoint Server VSSベースソリューション 122
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 123
Data Protector Microsoft SharePoint Server用Granular Recovery Extension 123

前提条件 124
GRE環境 125
Microsoftボリュームシャドウコピーサービスクライアント 126
Sybase Serverクライアント 127
Informix Serverクライアント 127
IBM HACMPクラスター 127
SAP R/3クライアント 128
前提条件 128
SAP MaxDBクライアント 128
SAP HANAアプライアンスクライアント 128
Oracle Serverクライアント 129
HP OpenVMS 129
MySQLクライアント 129
PostgreSQLクライアント 130
IBM DB2 UDBクライアント 130
Lotus Notes/Domino Serverクライアント 130
Lotus Domino Cluster 130
VMwareクライアント 131
Data Protector GRE for VMware vSphere 131
GRE環境 131
マウントプロキシシステム 132
VMware vCenter Server (VirtualCenter Server) 134
VMware vCenter Server Appliance (VCSA) 6.0環境 134
VMware vSphere Web Client用Data Protector GREのインストール 135
考慮事項 135
要件 135
新規インストール 135
アップグレード 136
オプション1 137
オプション2 137
拡張GRE Webプラグインのアンインストール 138
VMware vSphere管理対象オブジェクト参照の手動による登録解除 138
Microsoft Hyper-Vクライアント 139
Data Protector仮想環境用統合ソフトウェア 139
Data Protector Microsoft Volume Shadow Copy Service integration 140
NDMP Serverクライアント 140
HPE P4000 SANソリューション clients 140
HPE P6000 EVAディスクアレイファミリ クライアント 141
クラスターへのインストール 141
他のアプリケーションの統合 141
HPE P6000 EVAディスクアレイファミリとOracle Serverの統合 142

前提条件 142
インストール手順 142
HPE P6000 EVAディスクアレイファミリとSAP R/3の統合 143
前提条件 143
インストール手順 145
HPE P6000 EVAディスクアレイファミリとMicrosoft Exchange Serverの統合 146
前提条件 146
インストール手順 146
HPE P6000 EVAディスクアレイファミリとMicrosoft SQL Serverの統合 146
前提条件 146
インストール手順 146
HPE P9000 XPディスクアレイファミリクライアント 147
クラスターへのインストール 147
他のアプリケーションの統合 147
HPE P9000 XPディスクアレイファミリとOracle Serverの統合 148
前提条件 148
インストール手順 148
HPE P9000 XPディスクアレイファミリとSAP R/3の統合 149
前提条件 149
インストール手順 151
HPE P9000 XPディスクアレイファミリとMicrosoft Exchange Serverの統合 152
前提条件 152
インストール手順 152
HPE P9000 XPディスクアレイファミリとMicrosoft SQL Serverの統合 152
前提条件 152
インストール手順 152
HPE 3PAR StoreServ Storage clients 153
EMC Symmetrixクライアント 153
クラスターへのインストール 153
他のアプリケーションの統合 154
EMC Symmetrix用統合ソフトウェアとOracleの組み合わせ 154
前提条件 154
インストール手順 154
EMC Symmetrix用統合ソフトウェアとSAP R/3の組み合わせ 155
前提条件 155
インストール手順 157
EMC Symmetrix用統合ソフトウェアとMicrosoft SQL Serverの組み合わせ 157
前提条件 157
インストール手順 157
non–HPE Storage Arrays 157
他のアプリケーションの統合 158
non–HPE Storage ArrayとVMwareの仮想環境の統合 158
制限事項 158
前提条件 158
インストール手順 158

non–HPE Storage ArrayとOracle Serverの統合 159
制限事項 159
前提条件 159
インストール手順 159
HPE以外のストレージアレイとSAP R/3の統合 160
制限事項 160
前提条件 160
インストール手順 162
HPEストレージアレイとMicrosoft SQL Serverの統合 162
制限事項 162
前提条件 163
インストール手順 163

第5章: クラスターへのData Protectorのインストール 164
HPE ServiceguardへのData Protectorのインストール 164
構成の段階 164
クラスター対応Cell Managerのインストール 164
前提条件 164
プライマリCell Managerの構成 165
手順 165
セカンダリCell Managerの構成 166
手順 166
Cell Managerパッケージの構成 166
前提条件 166
手順 166
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 168
クラスター対応クライアントのインストール 168
次に行う手順 168
ボリュームグループ作成の例 169
プライマリノードの手順 169
セカンダリノードの手順 171
Data Protectorパッケージ制御ファイルの修正 172
Data Protectorパッケージ制御ファイルの修正 174
Symantec Veritas Cluster ServerへのData Protectorのインストール 175
構成の段階 175
クラスター対応Cell Managerのインストール 175
前提条件 175
Data Protector Cell Manager用のクラスターサービスグループの準備 176
プライマリCell Managerの構成 176
手順 176
セカンダリCell Managerの構成 177
手順 177
Cell Managerクラスターサービスグループの構成 177
手順 177
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 177

クラスター対応クライアントのインストール 178
次に行う手順 178
Microsoft Cluster ServerへのData Protectorのインストール 178
クラスター対応Cell Managerのインストール 178
前提条件 178
考慮事項 179
ローカルインストール手順 180
インストールのチェック 185
Data Protector InetサービスとCRSサービス 186
クラスター対応クライアントのインストール 186
前提条件 186
ローカルインストール手順 187
インストールのチェック 187
Data ProtectorのIBM HACMPクラスターへのインストール 189
クラスター対応クライアントのインストール 189
次に行う手順 189
Microsoft Hyper-VクラスターでのData Protectorのインストール 189

第6章: インストールの保守 190
Data Protector保守モード 190
保守モードの開始 190
保守モードの終了 191
セルへのクラスター対応クライアントのインポート 192
前提条件 192
Microsoft Cluster Server 192
その他のクラスター 193
セルからのクライアントのエクスポート 194
前提条件 195
クライアントをエクスポートする 195
Microsoft Cluster Serverクライアント 196
セキュリティの留意事項 196
セキュリティ層 196
クライアントのセキュリティ 196
Data Protectorユーザー 197
Cell Managerの保護 198
その他のセキュリティ保護について 198
厳密なホスト名チェック 198
制限事項 199
ホスト名の解決 199
要件 200
機能を使用可能にする 200
[バックアップ仕様を開始]ユーザー権限 200
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 200

ホストの信頼 201
保護イベントのモニター 201
ユーザー認証とLDAP 202
LDAPログインモジュールを初期化して構成する 202
LDAPログインモジュールを初期化する 203
LDAPログインモジュールの構成 205
Data Protectorパーミッションの LDAPユーザーまたはグループへの付与 207
LDAPユーザーのユーザーグループへの追加 207
LDAPグループのユーザーグループへの追加 208
LDAP資格情報を使用したログイン 208
LDAP構成のチェック 208
証明書生成ユーティリティ 209
構文 209
例 212
ディレクトリ構造 216
既存のキーストアおよび信頼ストアファイル内の証明書の上書き 218
既存のサーバーとクライアントのストアファイルの置換 218
CA証明書の置換 219
識別名(DN)文字列の更新 219
新しいキーストアと信頼ストアファイルを作成して証明書を上書きする 219
既存のサーバーとクライアントのストアファイルの置換 220
CA証明書の置換 220
識別名(DN)文字列の更新 221
ストアパスワードによる構成ファイルの更新 221
Data Protectorパッチの管理 222
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 222
前提条件 222
制限事項 222
GUIを使用したData Protectorパッチの確認 223
CLIを使用したData Protectorパッチの確認 223
Data Protectorで必要なパッチ 224
Windowsシステムのパッチ 224
HP-UXシステムのパッチ 224
HP-UX 11.11 224
HP-UX 11.23 225
HP-UX 11.31 225
SUSE Linux Enterprise Serverシステムのパッチ 226
Red Hat Enterprise Linuxシステムのパッチ 226
パッチのインストール 226
Symantec Veritas Cluster Server上で構成されているCell Managerへのパッチのインストール 226
Data Protectorパッチバンドルのインストールと削除 227
UNIXシステムでData Protectorパッチバンドルをインストールおよび削除する 227
WindowsシステムでのData Protectorパッチバンドルのインストールと削除 227
内部データベースパッチのダウングレード 230

サイト固有のパッチとホットフィクスの管理 230
インストールサーバーあるいはSSPまたはHFのリモートインストールの準備 231
クライアントへのサイト固有のパッチまたはホットフィクスのインストール 231
SSP/HFによって置換されたバイナリを元に戻す 232
インストールされているSSPまたはHFの確認 233
GUIを使用してSSPまたはHFのパッケージを確認 234
CLIを使用してSSPまたはHFを確認 234
Data Protectorソフトウェアコンポーネントの変更 234
Windowsシステムの場合 234
クラスター対応クライアント 235
HP-UXシステムの場合 235
手順 235
Oracle Server固有の問題 235
Linuxシステム 236
手順 236
その他のUNIXシステム 237
インストールを確認する 237
前提条件 237
手順 237
Data Protectorソフトウェアのアンインストール 237
前提条件 238
Data Protectorクライアントのアンインストール 238
クラスタークライアントのアンインストール 239
Cell Managerとインストールサーバーのアンインストール 239
Windowsシステムからのアンインストール 240
HP-UXシステムからのアンインストール 240
HPE Serviceguard上で構成されているCell Managerおよびインストールサーバーのアンインストール 241
Symantec Veritas Cluster Server上で構成されているCell Managerおよびインストールサーバーのアンインストール 243
Linuxシステムからのアンインストール 244
UNIXでのData Protectorソフトウェアの手動による削除 246

第7章: Data Protectorのアップグレード 248
アップグレードの概要 248
前提条件 249
制限事項 249
アップグレード手順 250
MoM環境でのアップグレード 250
旧エージェントバージョンのサポート 250
シングルサーバー版からのアップグレード 251
旧バージョンのSSEからData Protector 10.00 SSEへのアップグレード 251
Data Protector 10.00 SSEからData Protector 10.00へのアップグレード 251
Cell Managerのアップグレード 252

複数のシステムからのアップグレード 252
Cell Managerの異なるプラットフォームへの移行 253
PA-RISC HP-UXシステムからIntel Itanium HP-UXシステムへの移行 253
32ビット/64ビットWindowsから64ビットWindows/Windows Server 2008またはWindows Server 2012への移行 253
SolarisからLinuxへの移行 253
MoM固有の手順 254
インストールサーバー固有の手順 255
Windows Cell Manager内部データベースの異なるサーバーへの移行 255
用語 255
前提条件 255
移行の準備 256
OLD_SERVERでの操作 256
NEW_SERVERでの操作 256
移行作業 257
IDBのインポート 257
復元後の作業 258
Cell ManagerとしてのNEW_SERVERの追加 259
IDB内のCell Managerの名前の変更 259
次に行う手順 260
トラブルシューティング 260
HPE Serviceguard上で構成されているCell Managerのアップグレード 264
前提条件 264
一次ノード 264
二次ノード 265
一次ノード 265
二次ノード 266
一次ノード 266
Symantec Veritas Cluster Server上で構成されているCell Managerのアップグレード 267
前提条件 267
一次ノード 267
二次ノード 267
一次ノード 268
二次ノード 268
一次ノード 268
Microsoft Cluster Server上で構成されているCell Managerのアップグレード 269
前提条件 269
アップグレード手順 269
以前のバージョンからのスケジュールの移行 272

第8章: Data Protector Licensing 274
概要 274
ライセンスの種類 274

機能ベースのライセンス 274
容量ベースのライセンス 282
ライセンスの種類の選択 284
ライセンスの取得 285
新しいライセンスキーの取得 285
パスワードに関する考慮事項 286
恒久パスワードの取得 287
恒久パスワードのインストール 288
パスワードの検証 290
インストール済みライセンスの確認 291
既存のライセンスのアップグレード 291
他のCell Managerシステムへのライセンスの移動 291
集中型ライセンス 293
ライセンスレポート 293
Data Protectorパスワード 294
恒久パスワードの取得とインストール 295
パスワードの検証 297
インストール済みライセンスの確認 298
他のCell Managerシステムへのライセンスの移動 298
集中型ライセンス 299
Data Protector 10.00へのライセンス移行 300
Data Protectorライセンスフォーム 300
Data Protectorの製品構成とライセンス 301
パスワードに関する考慮事項 301
Data Protectorパスワード 302
恒久パスワードの取得とインストール 303
パスワードの検証 305
インストール済みライセンスの確認 305
他のCell Managerシステムへのライセンスの移動 306
集中型ライセンス 307
ライセンスパスワード 307
パスワードに関する考慮事項 307
恒久パスワードの取得 309
恒久パスワードのインストール 309
パスワードの検証 312
インストール済みライセンスの確認 312
他のCell Managerシステムへのライセンスの移動 312
第9章: インストールのトラブルシューティングとアップグレード 314
WindowsのCell Managerをインストールする際の名前解決に関する問題 314
Data Protectorセル内のDNS接続の確認 315
omnicheckコマンドの使用 315

共通の問題のトラブルシューティング 316
UNIXシステムでのインストールのトラブルシューティング 319
Windowsシステムでのインストールのトラブルシューティング 321
Data Protectorクライアントのインストール結果の確認 323
アップグレードのトラブルシューティング 324
Windowsシステムでのリモートアップグレードのトラブルシューティング 330
UNIXシステムでのローカルアップグレードの手動処理 331
ログファイルの使用 331
ローカルインストール 331
リモートインストール 332
Data Protectorログファイル 332
インストール実行トレースの作成 333

付録A: UNIXシステムネイティブツールを使用したインストールとアップグレード 334
ネイティブツールを使用した、HP-UXおよびLinuxシステムへのインストール 334
swinstallを使用したHP-UXシステムでのCell Managerのインストール 334
rpmを使用したLinuxシステムでのCell Managerのインストール 335
swinstallを使用したHP-UXシステムでのインストールサーバーのインストール 336
rpmを使用したLinuxシステムでのインストールサーバーのインストール 337
Linuxへのローカルインストール 337
次に行う手順 340
クライアントのインストール 340
ネイティブツールを使用した、HP-UXおよびLinuxシステムでのアップグレード 340
swinstallを使用したHP-UXシステムでのData Protectorのアップグレード 340
アップグレード手順 341
rpmを使用したLinuxシステムでのData Protectorのアップグレード 341
アップグレード手順 342

付録B: システムの準備と保守作業 343
UNIXシステムでのネットワーク構成 343
TCP/IP設定をチェックする 343
デフォルトのData Protectorポートの変更 345
デフォルトのData Protector Inetポートの変更 345
UNIXシステム 345
Windowsシステム 346
UNIXシステムでデフォルトのData Protector IDBポートおよびユーザーアカウントを変更する 346
Data ProtectorインストールのためのWindows Server 2008またはWindows Server 2012上で実行するMicrosoftサーバークラスターの準備 347
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 349
NISサーバーの準備 349

Cell Manager名の変更 350
ジョブコントロールエンジン(JCE)データベースのホスト名の変更 356
Windows Cell Managerでの大型バックアップセッションの実行 358

付録C: デバイスとメディア関連タスク 359
Windowsシステムでのテープドライバーおよびロボティクスドライバーの使用 359
テープドライバー 359
ロボティクスドライバー 360
Windowsシステム上でのデバイスファイル(SCSIアドレス)の作成 361
Windowsでネイティブテープドライバーを使用している場合 361
光磁気デバイス 362
HP-UXシステム上のSCSIロボティクス構成 362
HP-UXシステム上のデバイスファイルの作成 366
前提条件 366
デバイスファイルの作成 368
SCSIコントローラーのパラメーターの設定 368
HP-UXシステム上の未使用のSCSIアドレスの取得 368
Solarisシステム上の未使用のSCSIターゲットIDの取得 370
Solarisシステム上でのデバイスおよびドライバー構成の更新 370
構成ファイルの更新 370
デバイスファイルの作成とチェック 373
Windowsシステム上の未使用のSCSIターゲットIDの取得 374
HPE 330fxライブラリでのSCSI IDの設定 374
バックアップデバイスの接続 375
ハードウェア圧縮 377
次に行う手順 377
HPE 24スタンドアロンデバイスの接続 378
HP-UXシステムに接続する場合 378
次に行う手順 378
Windowsシステムに接続する場合 378
この次に行う作業 379
HPE DATオートローダーの接続 379
HP-UXシステムに接続する場合 379
次に行う手順 380
Windowsシステムに接続する場合 380
次に行う手順 380
HPE DLTライブラリ28/48スロットの接続 380
HP-UXシステムに接続する場合 381
次に行う手順 381
Solarisシステムに接続する場合 381
この次に行う作業 383
Windowsシステムに接続する場合 383

次に行う手順 384
Seagate Viper 200 LTO Ultriumテープドライブの接続 384
Solarisシステムに接続する場合 384
この次に行う作業 385
Windowsシステムに接続する場合 385
次に行う手順 385

付録D: 詳細 386
Data Protectorドキュメントを表示するための要件 386
ヘルプ 387
ドキュメントマップ 387
略称 387
統合 390
Data Protectorグラフィカルユーザーインターフェイス 391

フィードバックを送信 393

第1章: インストール手順の概要

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ユーザーインターフェイスについても説明します。

インストール手順の概要

Data Protectorバックアップ環境は、同じタイムゾーンに所属し、同じLAN/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ポリシーが適用されます。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セッションマネージャーを実行します。

IDBには、バックアップしたファイルとセルの構成が記録されます。

インストールサーバーは、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ー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。

ユーザーインターフェイ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、ユーザーインターフェイスを使用して行われます。ユーザーインターフェイ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ーフェイス(GUI)とコマンドラインインターフェイス(CLI)があります。

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。

バックアップが必要なアプリケーションと仮想環境があるクライアントシステムには、適切なData Protector用統合ソフトウェアエージェ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。統合ソフトウェアエージェントでは、アプリケーションまたは仮想環境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(https://softwaresupport.hpe.com/)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。

- ユーザーインターフェイスを介 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、ユーザーインターフェイ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をインストールする1つまたは複 数 のシステム。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 するシステムは、Cell Managerおよびユーザーインターフェイ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 じシステム上 、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。

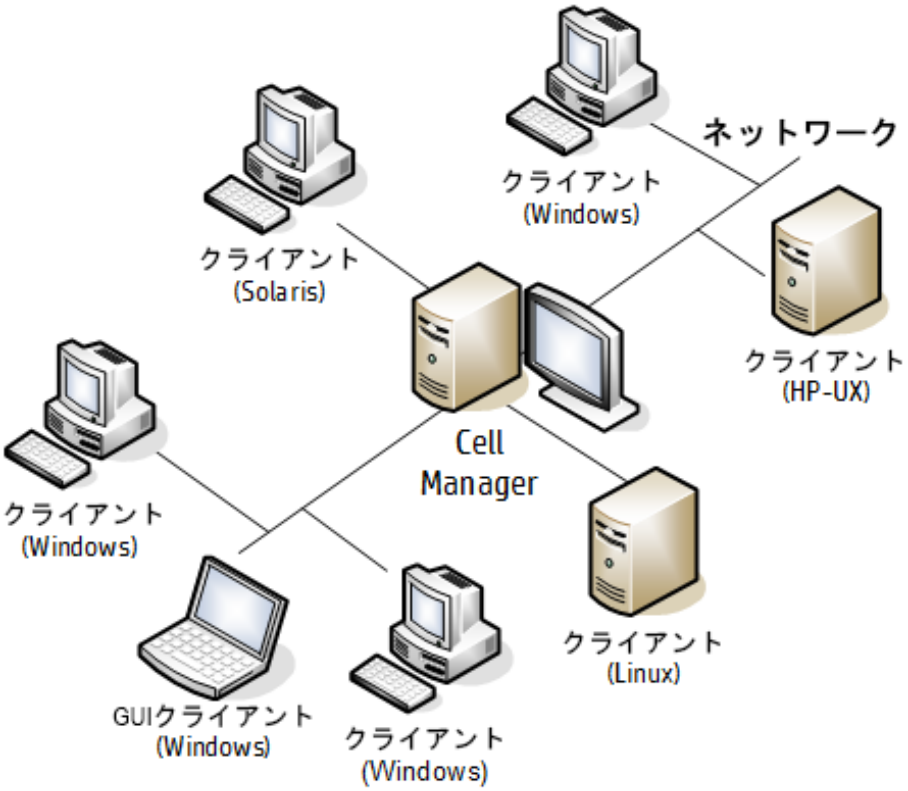
> **重 要 :**
> Data ProtectorクライアントをSolarisシステムにインストールする場 合 は、`/usr/omni`ディレクトリのすべてのファイルを別 のディレクトリに保 存 してください。Data Protectorをインストールすると、`/usr/omni`ディレクトリのすべてのファイルは削 除 されます。

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 インストールは以 下 のとおりです。

1. インストールの前 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ーフェイ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パッケージ(zip/tar)からローカルにインストールします。

> **注 :**
> 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zipパッケージ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、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。

Data Protectorセル



リモート インストールの概 念

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。ユーザーインターフェイ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、ユーザーインターフェイスを複 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システムに配 布 できます。

Windowsシステムは、Data ProtectorのWindowsインストールzipパッケージからローカルにインストールする必 要 があります。

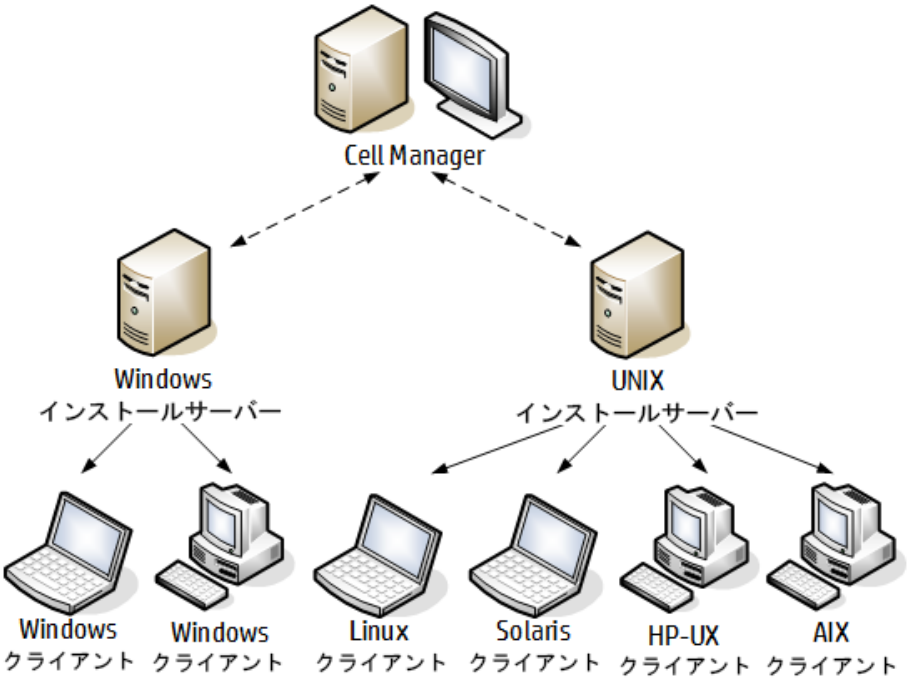
クライアントソフトウェアは、HP-UX、Solaris、Linux、AIX、およびその他 のサポートされているUNIXオペレーティングシステムに、UNIXシステム用 のインストールサーバーからリモートでインストールできます。サポートされるプラットフォームの一 覧 については、『*HPE Data Protectorサポート一 覧*』を参 照 してください。インストールサーバーはクライアントのローカルインストールには必 要 ありませんが、パッチを適 用 してクライアントを最 新 の状 態 を保 つためには必 要 です。

インストール先 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tarパッケージを使 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。

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 については、Data Protectorクライアントのインストール、ページ 54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システムでのローカルインストール、ページ 102を参 照してください。

Data Protectorのインストールの概 念



Data Protectorインストールメディア

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 のプロセッサーアーキテクチャーがサポートされています。ソフトウェアは、zip/tarパッケージで提 供 されます。

> **注:**
> Windows Server 2008およびWindows Server 2012システム用 のData Protectorインストールファイルは、HPEによってデジタル署 名 されています。

次 の表 は、https://softwaresupport.hpe.com/からダウンロード できる各 種 パッケージを示しています。

パッケージ名	目 次
Data Protectorソフトウェア10.00 Windows `DP_A1000_Windows_OVMS.zip`	• Windows 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 • 英 語 版 および各 国 語 版 ガイド ー 式 (電 子 PDFフォーマット)。 • 32/64ビット 版 Windowsクライアント • HP OpenVMSクライアント(AlphaおよびItaniumシステム) • 製 品 情 報 • HPEソフトウェア統 合 パッケージ

パッケージ名	目 次
Data Protectorソフト ウェア10.00 HP-UX DP_A1000_UX11x.tar.gz	• 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 • 英 語 版 および各 国 語 版 ガイド ー 式 (電 子 PDFフォーマッ ト)。 • HPEソフト ウェア統 合 パッケージ
Data Protectorソフト ウェア10.00 Linux DP_A1000_GPLx86_64.tar.gz	• 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 • 英 語 版 および各 国 語 版 ガイド ー 式 (電 子 PDFフォーマッ ト)。 • HPEソフト ウェア統 合 パッケージ

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。セルを集 中 管 理します。Cell Managerの機 能 は次 のとおりです。

- Data Protectorのコアソフト ウェアを実 行します。
- Data Protector内 部 データベース(IDB)サーバーをホストします。
- Data Protectorセッションに関 する情 報 があるデータを収 集 および維 持します。
- Session Managerを実 行します。Session Managerは、各 種 のData Protectorを開 始 および停 止 するほか、関 連 する情 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。

- 対 応 プラット フォーム

  Cell Managerは、Windows、HP-UX、またはLinuxプラット フォームにインスト 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 については、最 新 のサポート ー覧 (https://softwaresupport.hpe.com/)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。

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については、*HPE Data Protectorヘルプ*のキーワード「IDBのサイズ増加とパフォーマンス」で表示される内容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、『HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照してください。

> **注:**
> Cell Managerをユーザーインターフェイ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 Cell ManagerシステムとData Protectorユーザーインターフェイスコンポーネントを、Windowsプラットフォームを使用した別のシステムにインストールできます。

次に行う手順

Data Protector Cell Managerおよびインストールサーバーのインストール、ページ26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ユーザーインターフェイスシステムの選択

Data Protectorには、グラフィカルユーザーインターフェイス(GUI)とコマンドラインインターフェイス(CLI)の2種類のユーザーインターフェイスがあります。GUIはWindowsプラットフォームで使用でき、CLIはWindows、HP-UX、Solaris、およびLinuxプラットフォームで使用できます。両方のユーザーインターフェイスは、単一のData Protectorソフトウェアコンポーネントとして提供され、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ー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ー環境では、複数のシステム上でユーザーインターフェイスを使用できる方が便利です。また、異種混合環境では、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ーフェイスを配置するのが理想的です。

ユーザーインターフェイスに対してサポートされているオペレーティングシステム(リリース、バージョン、エディション)の詳細については、https://softwaresupport.hpe.com/で最新のサポート一覧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文字を使用する方法については、*HPE Data Protectorヘルプ*のキーワード「言語設定、カスタマイズ」で表示される内容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ーフェイ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ーフェイスシステムを使用する必要はありません。

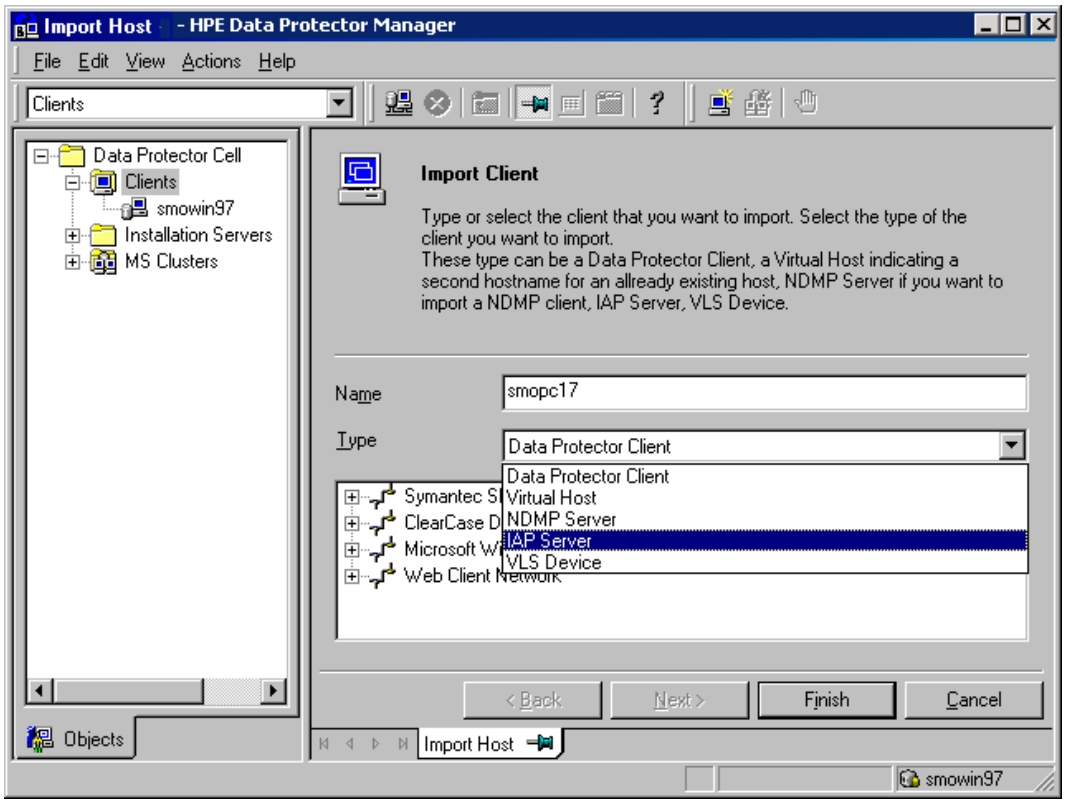
Data Protectorグラフィカルユーザーインターフェイス

Data Protector GUIは高機能ユーザーインターフェイスであり、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、**[クライアント]**、**[ユーザー]**、**[デバイス/メディア]**、**[バックアップ]**、**[復元]**、**[オブジェクト操作]**、**[レポート]**、**[モニター]**、**[インスタントリカバリ]**、**[内部データベース]**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、**[クライアント]**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。

Data Protectorグラフィカルユーザーインターフェイス



Data Protectorグラフィカルユーザーインターフェイス、ページ 391も参 照してください。Data Protector GUIの主 な領 域 について説 明しています。

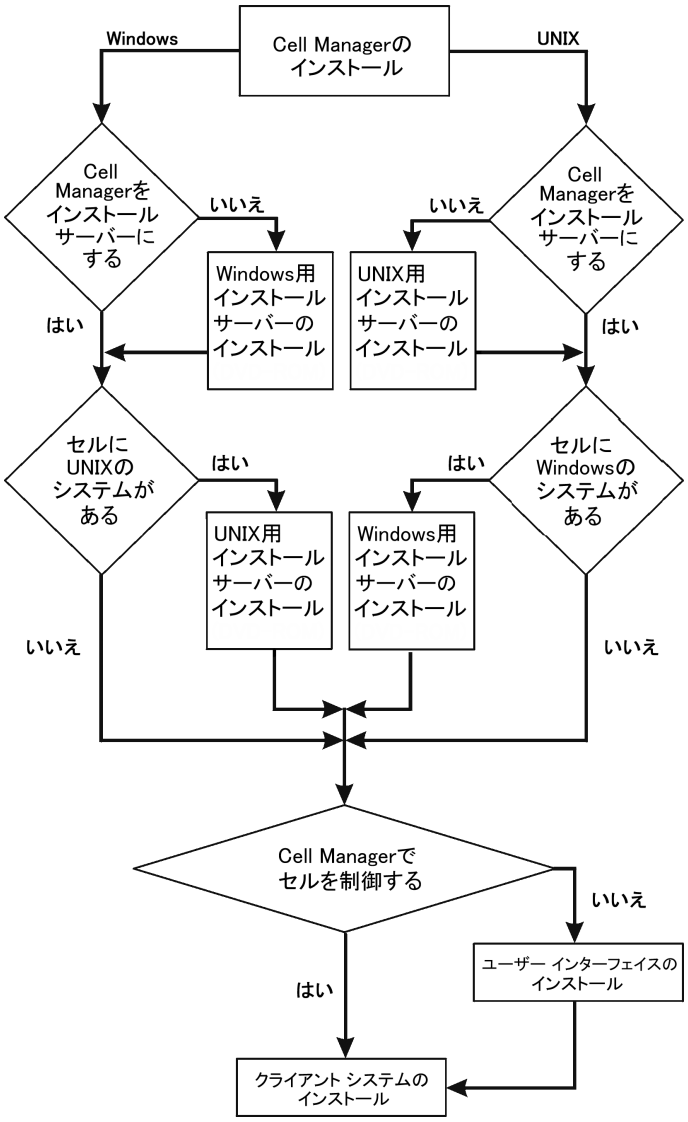
第2章: Data Protectorのインストール

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およびインストールサーバーのインストール
- Data Protectorシングルサーバー版のインストール

Data Protector Cell Managerおよびインストールサーバーのインストール

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。

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

UNIX Cell Managerのインストール Cell Manager

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 Cell Managerのインストール Cell Manager、ページ 34を参照してください。

前提条件

- ホスト名を解決するためのDNS逆引き参照は、Data Protectorセル内のすべてのData Protectorコンポーネントに必要です。
- デフォルトユーザーの`unmask`は、`022`に設定されている必要があります。そうでないと、一部のData Protectorサービスが起動できないことがあります。
- インストールで使用するユーザーアカウントには、選択したターゲットシステムに対する管理者(`root`)権限が付与されている必要があります。
- Cell Managerとなるシステムは、以下の条件を満たしていなければなりません。
  - サポート対象のUNIX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でサポートしているオペレーティングシステムのリストについては、https://softwaresupport.hpe.com/を参照してください。
  - 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。Cell Managerの最小要件は以下のとおりです。
    - Cell Managerでの1プロセスあたりのソフトファイルの上限が、少なくとも1024に設定されていること。
    - ***HP-UXシステムの場合:*** 8 GBの合計RAM。***Linux システムの場合:*** 4 GBの合計RAM。

    並行バックアップを行うセッションには40MBのRAMと5～8 MBのデータセグメントが必要です。たとえば、60の並行バックアップセッションを実行する場合、3GBのRAMと512MBのデータセグメントが必要です。

    Data Protectorをリンクディレクトリにインストールすることで、空きディスク容量不足を解決できます。リンクを作成する場合は、HP-UXおよびLinuxシステムにインストールされるディレクトリの構造、ページ 30を参照してください。
  - Data Protector内部データベース(IDB)用の十分な空きディスクスペースがあること。内部データ

ベースの復旧の場合、合計RAMの2倍が必要です。1.5 GBの空きディスクスペース + IDBが保存される/varディレクトリ内にバックアップファイル(IDB用)ごとに約100バイトが必要です。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。

ディスクボリューム上にストレージ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。

- 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。
- NISサーバーを使用する場合は、Cell Managerシステムを認識するように構成されていること。NISサーバーの準備、ページ 349を参照してください。
- 以下のポートが使用可能であること。
  - 5565 — Data Protectorの新規インストールに必要なポート
  - 5555 — Data Protectorインストールのアップグレード中に必要なポート
  - 7112 — 内部データベースサービスポート
  - 7113 — 内部データベース接続プーラー(IDB CP)ポート
  - 7116 —アプリケーションサーバー(HTTPS AS)ポート
  - 9999 — アプリケーションサーバー管理ポート

  デフォルトの通信ポート番号を変更する場合は、デフォルトのData Protector Inetポートの変更、ページ 345を参照してください。UNIXシステムでデフォルトのData Protector IDBポートおよびユーザーアカウントを変更する、ページ 346デフォルトのIDBポートとアプリケーションサーバーポートを変更する場合は、
を参照してください。
- ロングファイル名をサポートしていること。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 DirectoryPath`コマンドを実行します。
- Basicコマンドラインカリキュレーター(bc)がインストールされていること。
- ユーザーグループhpdpと、このユーザーグループ内の専用ユーザーアカウントhpdpがData Protectorで使用できるように構成されていること。デフォルトのユーザーアカウントを変更するには、UNIXシステムでデフォルトのData Protector IDBポートおよびユーザーアカウントを変更する、ページ 346を参照してください。
- 既存のホームフォルダーがhpdpユーザー用に構成されていること。そうでないと、一部のData Protectorサービスを開始できない可能性があります。
- hpdpユーザーは、システム内にすでに存在する次のパスのあらゆるディレクトリへのアクセス権を持っていること。
  - `/opt/omni/*`
  - `/etc/opt/omni/*`
  - `/var/opt/omni/*`

Linuxシステムの場合：

- 32ビットGNU Cライブラリ(glibc)が64ビットLinuxシステム(x86_64)上にインストールされていること。
- ネットツールがインストールされていること(インストール中に、一部のネットツールユーティリティが必要です)。

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。クラスター対応Cell Managerのインストール、ページ 164を参照してください。

> **注:**
> 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

- HPEでは、Data Protector内部データベースおよび2 GBを超える可能性があるDCバイナリファイルを格納するファイルシステムではラージファイルサポート(LFS)を使用することをお勧めします。

カーネルパラメーターの設定

HP-UXシステムの場合:

- カーネルパラメーターshmmax(共有メモリセグメントの最大サイズ)は、2.5GB以上に設定します。構成をチェックするには、次のコマンドを実行します。

  ```
  kcusage shmmax
  ```

- HPEでは、カーネルパラメーターmaxdsiz(最大データセグメントサイズ)またはmaxdsiz_64を134217728バイト(128MB)以上に設定し、カーネルパラメーターsemmnu(セマフォのアンドゥ構造の数)を4000以上に設定することを推奨します。semmnuパラメーターは、並列バックアップ/復元またはコピーのセッションの最大数(1000)に対応し、データベース照会セッションの最大数(1000)に対応している必要があります。並行セッションを多数実行する予定がない場合、semmnuパラメーターの値を変更する必要はありません。

  上記の変更が完了したら、システムを再起動します。

Linuxシステムの場合:

- カーネルパラメーターshmmax(共有メモリセグメントの最大サイズ)は、2.5GB以上に設定します。構成をチェックするには、次のコマンドを実行します。

  ```
  cat /proc/sys/kernel/shmmax
  ```

  内部データベースの復旧には、カーネルパラメーターを上記の値の2倍に設定する必要があります。

インストール手順

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、tarパッケージに含まれるREADMEファイルか、tarパッケージの/DOCS/C/MANディレクトリにある『*HPE Data Protector Command Line Interface Reference*』を参照してください。

Cell ManagerをHP-UXまたはLinuxシステムにインストールするには

1. ダウンロードしたData Protectorインストールパッケージ(tar)をHP-UXまたはLinuxシステムにコピーし、ファイルをローカルディレクトリに展開します。

   LOCAL_INSTALL

   platform_dir /DP_DEPOT

   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システムの場合
linux_x86_64	Linuxシステムの場合

2. LOCAL_INSTALLディレクトリに移動して、以下のコマンドを実行します。

   ./omnisetup.sh -CM

   omnisetup.shコマンドの詳細については、『*HPE Data Protector Command Line Interface Reference*』を参照してください。

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。必要な手順の詳細については、UNIXシステム用のインストールサーバーのインストール、ページ42を参照してください。

HP-UXおよびLinuxシステムにインストールされるディレクトリの構造

インストールが完了すると、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/
>
> /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。

/opt/omni/bin	ユーザーコマンド
/opt/omni/help/C	ヘルプ
/opt/omni/lbin	管理コマンド、コマンドラインユーティリティ

/opt/omni/sbin	管理コマンド、コマンドラインユーティリティ
/opt/omni/sbin/install	インストール用スクリプト
/etc/opt/omni	構成データ
/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
/var/opt/omni/log /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	manページ
/var/opt/omni/tmp	一時ファイル
/var/opt/omni/server/db80	IDBファイル 詳細については、『*HPE Data Protectorヘルプ*』のキーワード「IDB、ディレクトリの位置」で表示される内容を参照してください。
/opt/omni/AppServer	HPE Data Protectorアプリケーションサーバー。
/opt/omni/idb	HPE Data Protectorの内部データベース。
/opt/omni/jre	Data Protectorで使用するJavaランタイム環境。

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システムの場合:

/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パラメーターが格納されます。このパラメーターは、以下のいずれかの値をとります。 omni=1 システムの再起動時に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

		オプションが適用されます。
	omni=0	システムの再起動時にData Protectorの自動停止および自動起動を行いません。

Linuxシステムの場合：

/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/rc*init_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/rc*init_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。

インストール中には、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システムの場合：

/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。

インストールが完了すると、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	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 Cell Request Server (CRS)サービスが実行されます。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/mmd	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上でData Protector Media Management Daemon (MMD)サービスが実行されます。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/kms	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上でData Protector Key Management Server (KMS)サービスが実行されます。KMSは、Data Protector暗号化機能のキーを管理します。
/opt/omni/idb/bin/postgres	Data ProtectorInternal Database Service (hpdp-idb)は、IDBを実行するサービスです。内部データベースサービスは、内部データベースからの情報を必要とするプロセスによってCell Manager上でローカルにアクセスされます。このサービスは、Cell Manager

/opt/omni/idb/bin/pgbouncer	Data Protector Internal Database Connection Pooler (hpdp-idb-cp)サービスは、hpdb-idbへの開いた接続のプールを提供します。これにより、すべての要求に対して新しい接続が開かれるのではなく要求時に使用できるようになるため、hpdp-idb接続の拡張性が確保されます。このサービスは、Cell Manager上で実行され、ローカルプロセスによってのみアクセスされます。
/opt/omni/AppServer/bin/standalone.sh	Data Protector Application Server (hpdp-as)サービスは、HTTPS接続(Webサービス)を介したIDBへのGUI接続に使用されます。このサービスはCell Manager上で実行され、hpdp-idb-cpサービスへのローカル接続があります。

環境変数の設定

Data Protectorを使用する場合は、事前にお使いHPEのオペレーティングシステム構成の環境変数の値を追加してください。

- Data Protector manページをどこからでも閲覧できるようにするには、/opt/omni/lib/manをMANPATH変数に追加します。
- Data Protectorコマンドをどのディレクトリからでも実行できるようにするには、コマンドの場所をPATH変数に追加します。Data Protectorドキュメントの手順は、変数値が追加されていることを前提とします。コマンドの場所については、『*HPE Data Protector Command Line Interface Reference*』のomniintroのリファレンスページ、およびomniintroのmanページを参照してください。

次に行う手順

この段階で、Cell Manager(および選択した場合はUNIXシステム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 Cell Managerのインストール Cell Manager、ページ 27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する場合は、Windows用のインストールサーバーをインストールします。Windowsシステム用のインストールサーバーのインストール、ページ 45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、ページ 54を参照してください。

Windows Cell Managerのインストール Cell Manager

前提条件

- ホスト名を解決するためのDNS逆引き参照は、Data Protectorセル内のすべてのData Protectorコンポーネントに必要です。
- インストールで使用するユーザーアカウントは、以下の条件を満たす必要があります。
  - 選択したターゲットシステムに対する管理者(`Administrator`)権限が付与されていること。
  - ネットワークアクセスユーザー権限がWindowsローカルセキュリティポリシー内に設定されていること。
- Data Protector Inetサービスはデフォルトで、Windowsローカルユーザーアカウント SYSTEMで実行されます。ただし、さまざまな理由からInetサービスがWindowsドメインユーザーアカウントで実行されている場合は、さらに次のWindowsオペレーティングシステムのセキュリティポリシー特権も付与される必要があります。
  - 認証後にクライアントを偽装
  - プロセスレベルトークンの置き換え

  詳細については、『*HPE Data Protectorヘルプ*』のキーワード「Inetユーザーの偽装」で表示される内容を参照してください。
- Cell Managerとなるシステムは、以下の条件を満たしていなければなりません。
  - 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でサポートしているオペレーティングシステムのリストについては、https://softwaresupport.hpe.com/を参照してください。
  - 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。Cell Managerには合計4 GBのRAMが必要です。

    内部データベースの復旧の場合、合計RAMの2倍が必要です。

    並行バックアップセッションごとに40MBのRAMが必要です。たとえば、60の並行バックアップセッションを実行する場合、3GBのRAMが必要になります。
  - Data Protector 内部データベース(IDB)用の十分な空きディスクスペースがあること。1.5 GBの空きディスクスペース + バックアップされるファイル(IDB用)ごとに約100バイト

    選択したディスクボリューム上に十分なストレージスペースがない場合には、そのディスク上のディレクトリに他のボリュームをマウントすることもできます。ただし、これはインストール前に行っておく必要があります。
  - システムドライブ上のディスクスペース: `2 × size_of_the_biggest_package_to_be_installed + 10 MB`
  - 「リモートサービス管理」(NP)接続(ポート445)を追加で受信するため、ファイアウォールが構築され

ていること。

- 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。コンピューター名とホスト名は同じである必要があります。
- 固定IPアドレスが割り当てられていること。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。
- 以下のポートが使用可能であること。
  - 5565 — Data Protectorの新規インストールに必要なポート
  - 5555 — Data Protectorインストールのアップグレード中に必要なポート
  - 7112 — 内部データベースサービスポート
  - 7113 — 内部データベース接続プーラー(IDB CP)ポート
  - 7116 —アプリケーションサーバー(HTTPS AS)ポート
  - 9999 — アプリケーションサーバー管理ポート

  上記のサービスポートはインストール時に変更できます。デフォルトの通信ポート番号を変更する場合は、デフォルトのData Protector Inetポートの変更、ページ 345を参照してください。

- Windows Cell Manager上で実行するバックアップセッション数が多い場合は、デスクトップヒープの制限を調整してください。各デスクトップヒープの割り当てサイズは、次のレジストリ値によって制御されます。

  ```
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session
  Manager\SubSystems\Windows
  ```

  このレジストリ値のデフォルトデータは、次のようになります。

  ```
  %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
  SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1
  ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4
  ProfileControl=Off MaxRequestThreads=16
  ```

  "SharedSection="に続く数値で、デスクトップヒープがどのように割り当てらレルかが制御されます。これらのSharedSection値は、キロバイト単位で指定します。
  - 1024 - すべてのデスクトップに共通する共有ヒープサイズ。
  - 20480 - 対話型のウィンドウステーションに関連する各デスクトップのデスクトップヒープのサイズ。
  - 768 - 非対話型のウィンドウステーションに関連する各デスクトップのデスクトップヒープのサイズ。

  非対話型ウィンドウステーションに関連付けられるSharedSection値は20480に変更する必要があります。この変更を有効にするには、再起動が必要です。

Microsoftターミナルサービスクライント

- Microsoftターミナルサービスクライントを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

- DCバイナリファイルが2 GBよりも大きくなると思われる場合(DCバイナリファイルのサイズは、ファイルシステムの設定でのみ制限可)は、NTFSファイルシステムの使用をお勧めします。HPE

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。クラスター対応Cell Managerのインストール、ページ 178を参照してください。

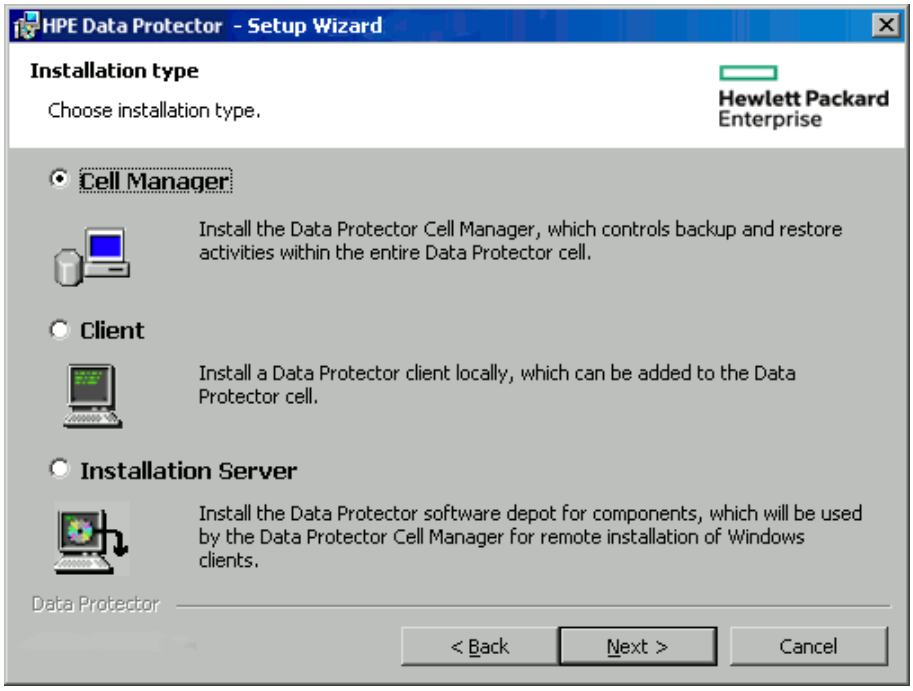
> **注:**
> マルチセル環境(MoM)では、すべてのCell Managerに同じバージョンのData Protectorをインストールする必要があります。

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

1. ダウンロードしたインストールパッケージ(zip)をWindowsシステムにコピーし、ファイルをローカルディレクトリに展開します。ご使用のプラットフォームの該当フォルダーにある`setup.exe`ファイルを実行します。
2. セットアップウィザードに従い、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。
3. [Obsolescence Information]ページで詳細を確認し、Data Protectorでサポートされるハードウェアおよびソフトウェアのバージョンが変更されたこと承認する場合に限り、**[I understand the changes to the supported platforms]**をクリックします。
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。

インストールの種類の選択

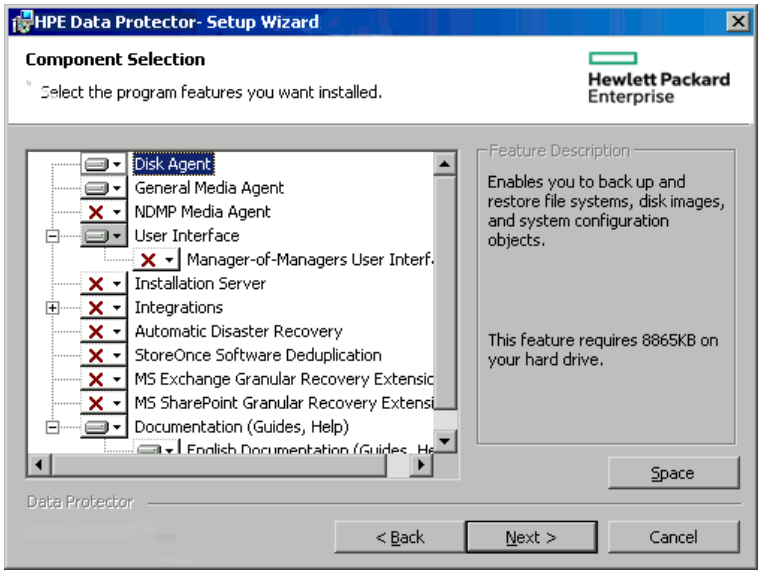


5. Data Protectorサービスを実行するアカウントの、ユーザー名とパスワードを入力します。

   [Next]をクリックし、次に進みます。
6. Data Protectorをデフォルトのフォルダーにインストールする場合は、**[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]または[Change Current Program Data Destination Folder]ダイアログボックスを開き、必要に応じてインストールフォルダーを変更します。プログラムデータインストールフォルダーへのパスは80文字以内に制限されます。
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、ページ 57を参照してください。

ソフトウェアコンポーネントの選択

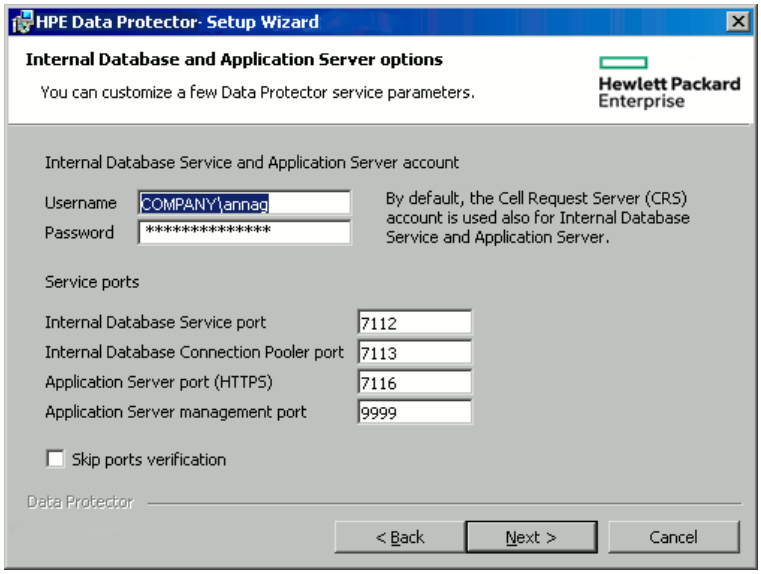


Disk Agent、**General Media Agent**、**ユーザーインターフェイス**、および**インストールサーバー**がデフォルトで選択されています。**[次へ]**をクリックします。

8. 必要に応じて、Data Protector IDBおよびアプリケーションサーバーで使用するユーザーアカウントと、これらのサービスで使用するポートを変更します。

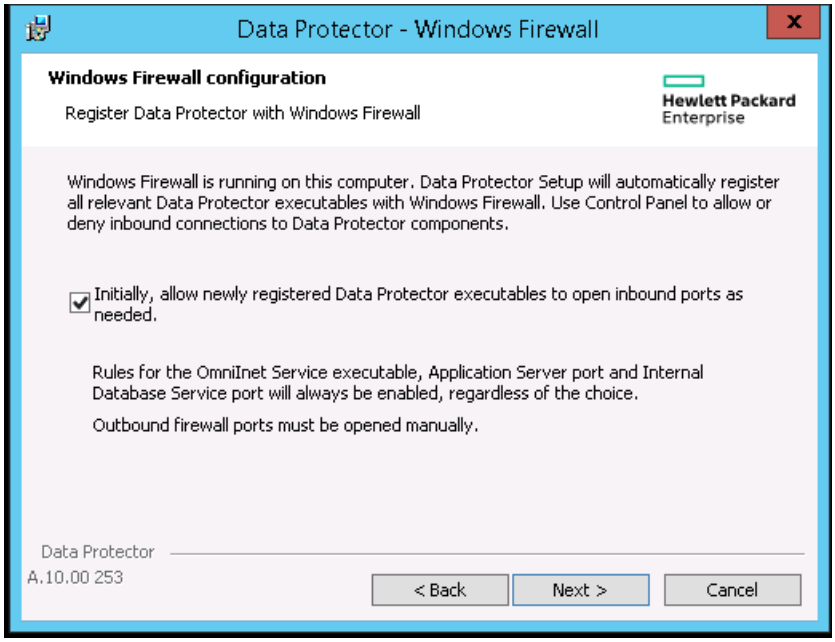
   [次へ]をクリックします。

   IDBおよびアプリケーションサーバーオプションの変更



9. システムにWindows Firewallが検出された場合、Windows Firewallの構成ページが表示されます。必要なData Protector実行可能ファイルはすべて登録されます。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。前バージョンの10.00クライアントでData Protectorが正しく機能するには、Windows FirewallのData Protectorルールを有効にする必要があります。ここでの選択に関

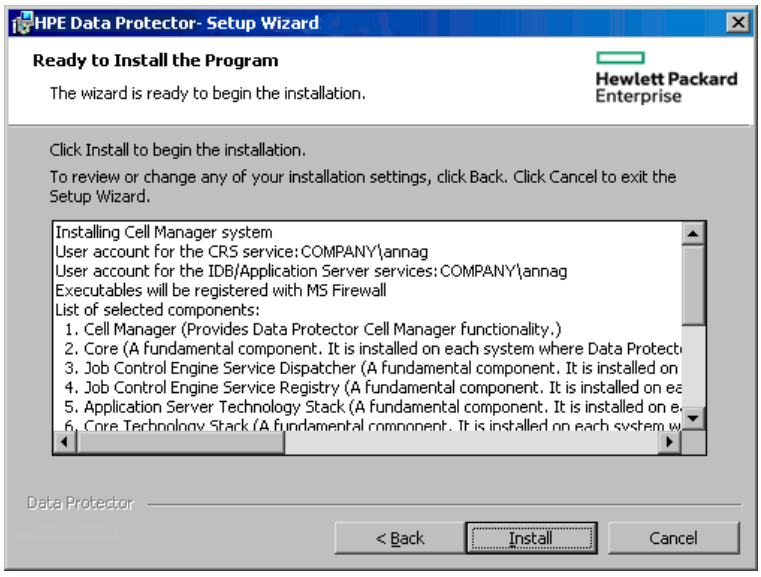
係 なく、OmniInetサービスの実 行 可 能 ファイル、アプリケーションサーバーポート、内 部 データベース サービスポートのルールは常 に有 効 です。



[次 へ]をクリックします。

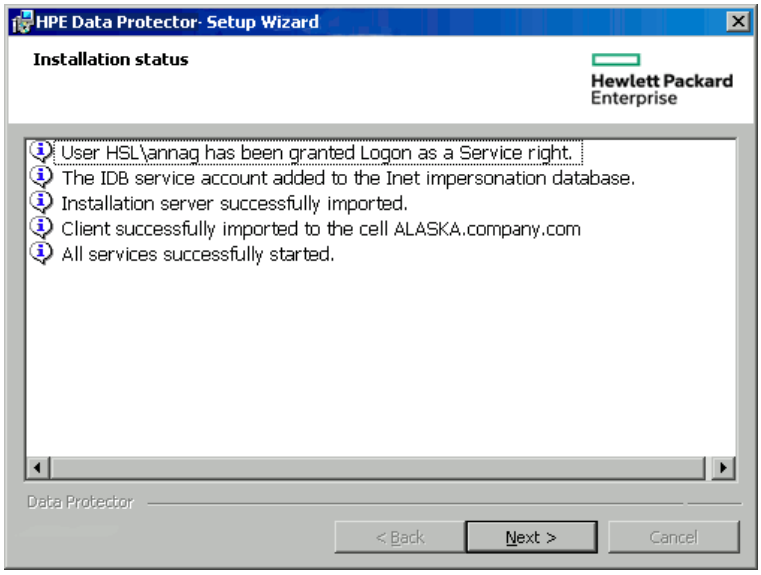
10. コンポーネントのサマリーリストが表 示されます。**[Install]**をクリックして、選 択したコンポーネントのインストールを開 始します。この処 理には、数 分 かかる場 合 があります。

コンポーネントのサマリーリスト



11. **[Installation status]**ページが表 示されます。**[次 へ]**をクリックします。

[Installation status]ページ



12. `User Interface`コンポーネントをインストールした場合に、セットアップ直後にData Protector GUIを使用して操作を開始するには**[Launch Data Protector GUI]**を選択します。

    `English Documentation (Guides, Help)`コンポーネントをインストールした場合に、セットアップ直後にHPE Data Protector製品案内、ソフトウェアノート、およびリファレンスを表示するには、**[Open the Product Announcements, Software Notes, and References]**を選択します。

    [完了]をクリックします。

インストール後の処理

Cell Managerファイルは、*Data_Protector_home*ディレクトリおよび*Data_Protector_program_data*内にあります。

ソフトウェアデポは、*Data_Protector_program_data*\Depotディレクトリ内にあります。

Data Protectorコマンドは、ディレクトリに格納されます。コマンドの場所については、『*HPE Data Protector Command Line Interface Reference*』のomniintroのリファレンスページ、およびomniintroのmanページを参照してください。

> **重要：**
> HPEでは、お使いのオペレーティングシステム構成の適切な環境変数の値にコマンドの場所を追加して、どのディレクトリからでもData Protectorコマンドを実行できるようにすることをお勧めしています。Data Protectorドキュメントの手順は、環境変数の値が追加されていることを前提とします。

以下のプロセスがCell Managerシステムで実行します。

crs.exe	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 Cell Request Server (CRS)サービスが実行されます。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。

mmd.exe	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 Media Management Daemon (MMD)サービスが実行されます。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開始できるようにするData Protectorクライアントサービス。Data Protector Inetサービスは、Data Protectorセル内のすべてのシステム上で実行することが必要です。*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)サービスは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開始します。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。
hpdp-idb	Data Protector Internal Database Service (hpdp-idb)は、IDBを実行するサービスです。内部データベースサービスは、内部データベースからの情報を必要とするプロセスによってCell Manager上でローカルにアクセスされます。このサービスは、Cell Manager上のIDBからManager-of-Manager(MoM)上のIDBへの転送に関するメディア管理情報に対してのみリモートでアクセスされます。
hpdp-idb-cp	Data Protector Internal Database Connection Pooler (hpdp-idb-cp)サービスは、hpdb-idbへの開いた接続のプールを提供します。これにより、すべての要求に対して新しい接続が開かれるのではなく要求時に使用できるようになるため、hpdp-idb接続の拡張性が確保されます。このサービスは、Cell Manager上で実行され、ローカルプロセスによってのみアクセスされます。
hpdp-as	Data Protector Application Server (hpdp-as)サービスは、HTTPS接続(Webサービス)を介したIDBへのGUI接続に使用されます。このサービスはCell Manager上で実行され、hpdp-idb-cpサービスへのローカル接続があります。

注：
複数のプラットフォームにまたがるバックアップや復元をData Protectorユーザーインターフェイスから実行する場合は、『HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照して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。手順の詳細については、オペレーティングシステムのドキュメントを参照してください。

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、Setup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、ページ 34を参照してください。

Setupがチェックする前提条件を以下に示します。

- Service Packのバージョン
- nslookupにより、Data Protectorがホスト名を展開できることが確認されていること
- ディスクスペース
- 管理者権限

次に行う手順

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用インストールサーバーをインストールします。Data Protector Cell Managerおよびインストールサーバーのインストール、ページ 26を参照してください。なお、UNIXシステム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。Data Protectorクライアントのインストール、ページ 54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については、https://softwaresupport.hpe.com/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システム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または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用にサポートされているオペレーティングシステムの詳細は、『HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照してください。
- inetdデーモンまたはxinetdデーモンが実行されていること。
- ホスト名を解決するためのDNS逆引き参照は、Data Protectorセル内のすべてのData Protectorコンポーネントに必要です。
- ポート番号5555/5565 (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、デフォルトのData Protector Inetポートの変更、ページ 345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。最小要件を以下に示します。
  - 512 MBの合計RAM
  - 1.5 GBの空きディスクスペース
- インストールを実行するには、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。
- Data Protectorセル内のCell Managerは、バージョン10.00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/
```

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ます。

注:
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ーにソースディレクトリをマウントします。

推奨事項

UNIXクライアントの場合、UNIX Data Protectorを使用してインストールサーバーをインストールする方法が推奨されます。

Data ProtectorのUNIXクライアントへのローカルインストールも可能ですが、インストールサーバーを使用せずにUNIXにパッチを適用するサポートされる手順がないので推奨されません。

UNIXクライアントにパッチを適用するには、インストールサーバーが必要なので、同じインストールサーバーを使用して最初にData ProtectorをUNIXクライアントにインストールすることが推奨されます。

インストール手順

UNIX用のインストールサーバーをHP-UXシステムまたはLinuxシステムにインストールするには

1. ダウンロードしたData Protectorインストールパッケージ(tar)をHP-UXまたはLinuxシステムにコピーし、ファイルをローカルディレクトリに展開します。

   LOCAL_INSTALL

   platform_dir/DP_DEPOT

   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システムの場合
linux_x86_64	Linuxシステムの場合

2. LOCAL_INSTALLディレクトリに移動して、以下のコマンドを実行します。

   ./omnisetup.sh -IS

   omnisetup.shコマンドの説明については、インストールパッケージ(tar)または*Mount_point*/にあるREADMEファイル、またはインストールパッケージのDOCS/C/MANディレクトリにある『*HPE Data Protector Command Line Interface Reference*』を参照してください。

インストールが終了すると、UNIXのソフトウェアデポは、/opt/omni/databases/vendorディレクトリに置かれます。

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。パッケージのサブセットのみをインストールするには、swinstall (HP-UXの場合)またはrpm (Linuxの場合)を使用する必要があります。ネイティブツールを使用した、HP-UXおよびLinuxシステムへのインストール、ページ 334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、UNIXインストールパッケージ(tar) (HP-UXまたはLinux用)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しなければなりません。さらに、Data Protectorクライアント上のコンポーネントはパッチできなくなります。

次に行う手順

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。UNIXシステム用のインストールサーバーのインストール、ページ 42を参照してください。

   > **注：**
   > 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ッケージ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ッケージを確認できます。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ッケージをインストールまたは削除したときは必ず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。Windowsシステム用のインストールサーバーのインストール、下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、ページ 54を参照してください。

Windowsシステム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については、https://softwaresupport.hpe.com/を参照してください。
- 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。最小要件を以下に示します。
  - 512 MBの合計RAM
  - 2 GBの空きディスクスペース
- ホスト名を解決するためのDNS逆引き参照は、Data Protectorセル内のすべてのData Protectorコンポーネントに必要です。
- TCP/UDP 445。新しいData Protectorクライアントプッシュインストール(クライアント上にData Protectorコンポーネントがない)の場合は、アクセス可能なインストールサーバー共有が必要です。インストールサーバーのデポ共有にアクセスできない場合は、その代わりに最初のData Protectorクライアントインストールをローカルで実行する必要があります。
- 5565 — Data Protectorで新しいインストールに必要なポート。このポート番号がすでに使用されている場合は、「デフォルトのData Protector Inetポートの変更、ページ 345」を参照してください。
- 5555 — Data Protectorのインストールのアップグレードに必要なポート。
- 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。コンピューター名とホスト名は同じである必要があります。

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、以下かの条件のいずれかを満たす必要があります。

- インストールサーバーとクライアントの両方が、同じドメイン内に存在していない。
- インストールサーバーとクライアントの両方が、同じドメイン内に存在している。

重要：
ネットワーク上にWindows用インストールサーバーをインストールしない場合は、インストールパッケージ(zip)からすべての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。

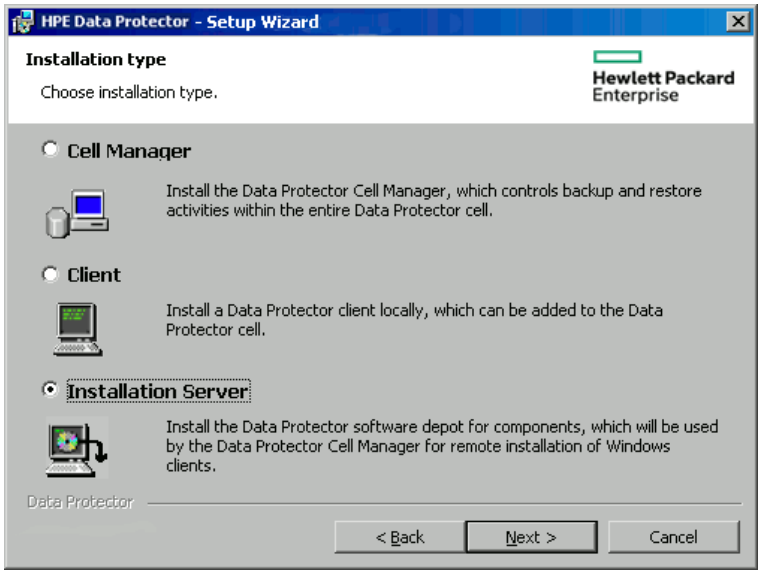
注：
インストールサーバーのインストール後、WindowsシステムにはData Protectorクライアントをリモートでインストールすることはできません。同一システム上にインストールサーバーとクライアントコンポーネントをインストールする場合は、クライアントをローカルにインストールする必要があります。この場合はインストール手順の中で、必要なクライアントコンポーネントとインストールサーバーコンポーネントをすべて選択してください。「Data Protectorクライアントのインストール、ページ 54」を参照してください。

インストール手順

Windowsシステム用のインストールサーバーをインストールするには

1. Windowsシステムにダウンロードしたインストールパッケージ(zip)をコピーし、ローカルディレクトリに展開します。プラットフォームに適用可能なフォルダーから`setup.exe`ファイルを実行します。
2. セットアップウィザードに従い、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。
3. 終了情報ページで詳細を確認し、サポートされているハードウェアおよびソフトウェアバージョンのリストについて、Data Protectorが行った変更を承認する場合のみ、**[I understand the changes to the supported platforms]**をクリックします。
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。

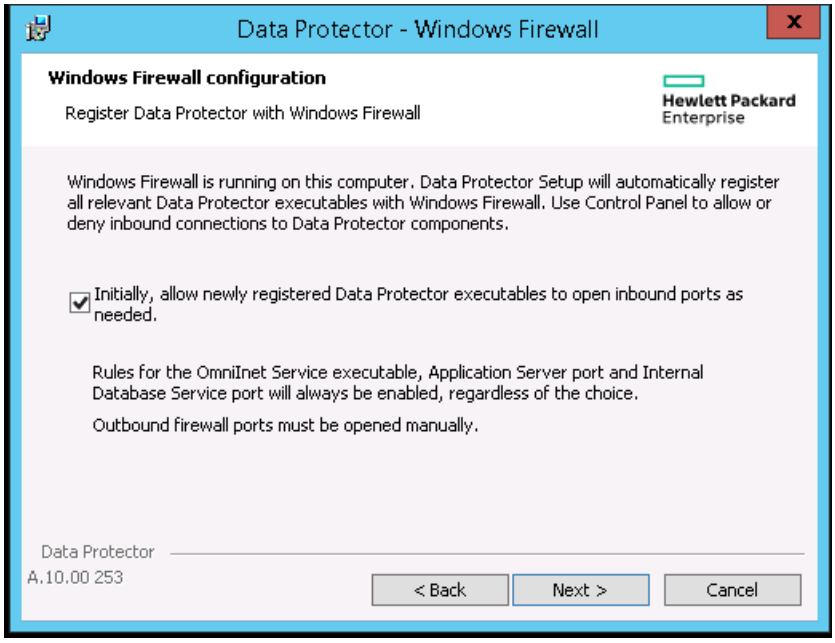
インストールの種類の選択



5. Data Protectorをデフォルトフォルダー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。

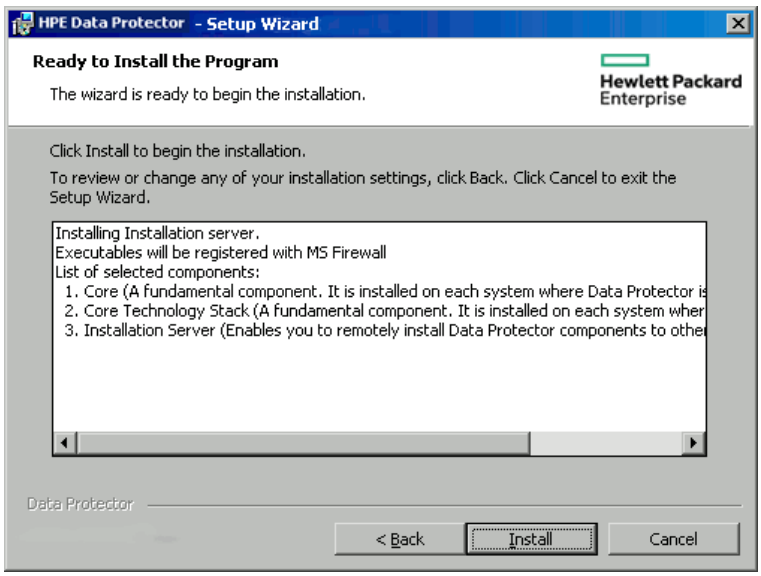
6. システムにWindows Firewallが検出された場合、Windows Firewallの構成ページが表示されます。Data Protectorセットアップでは、すべての必要なData Protector実行可能ファイルが記録されます。デフォルトでは、**[Initially, allow newly registered Data Protector executables to open inbound ports as needed]**オプションが選択されています。この時点で、Data Protectorによってポートがオープンされないようにするには、オプションを選択解除します。Data Protectorが以前のバージョンの10.00クライアントで適切に機能するには、WindowsファイアウォールのData Protectorルールを有効にする必要があります。OmniInetサービス実行可能ファイル、アプリケーションサーバーポート、内部データベースポートのルールは、選択内容にかかわらず常に有効になります。



[次 へ]をクリックします。

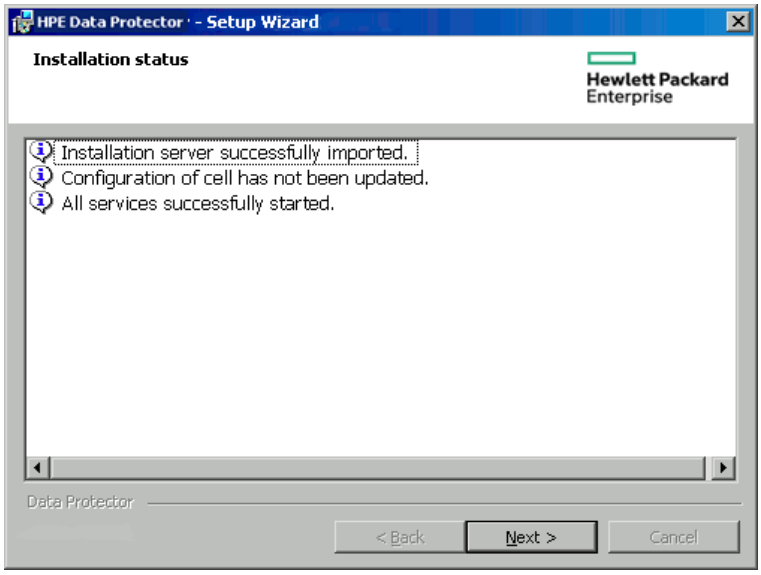
7. コンポーネントのサマリーリストが表 示されます。**[Install]**をクリックして、選 択したコンポーネントのインストールを開 始します。この処 理には、数 分 かかる場 合 があります。

   コンポーネント選 択 サマリーページ



8. インストールステータスのページが表 示されます。**[次 へ]**をクリックします。

   [Installation status]ページ



9. **[完 了]**をクリックします。

インストールが完 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。

インストールサーバーから新 規 クライアントへのコピー中 にインストールファイルが変 更 されないように、インストールサーバーとクライアント間 の通 信 にはネットワークファイルプロトコルのセッション管 理 ブロック(SMB)が使 用 されます。

インストールサーバーは、最初のリモートインストール時に、SMBパケットをセットアップし署名します。以下のポリシーが適用されます。

- Microsoftネットワーククライアント: 常に通信にデジタル署名を行う
- Microsoftネットワークサーバー: 常に通信にデジタル署名を行う

RequireSecuritySignatureパラメーターの次のレジストリ値は、次のキーで1に設定されます。

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanWorkstation\Parameters
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters

リモートインストール時には、次のメッセージが表示されます。

```
Verifying SMB signing at Data Protector Installation server and if necessary
starting it...
```

SMB署名を有効にした後で、ユーザーがSMBを使用してインストールサーバーホストから別のホストに接続する必要がある場合は、接続先のホストでもSMBが有効になっている必要があります。

次に行う手順

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。「UNIXシステム用のインストールサーバーのインストール、ページ 42」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。「UNIXシステム用のインストールサーバーのインストール、ページ 42」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、ページ 54」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およびインストールサーバーのインストール、ページ 26を参照してください。

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オートチェンジャーを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。

- 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。

サポートされているデバイスについては、HPE Data Protector製品案内、ソフトウェアノート、およびリファレンスを参照してください。

SSEへのアップグレード(HP-UX)での制限事項

- 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オートチェンジャーを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、およびSolaris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。

サポートされているデバイスについては、HPE Data Protector製品案内、ソフトウェアノート、およびリファレンスを参照してください。

パスワードのインストール

Cell Managerにパスワードをインストールする詳しい手順は、Data Protectorパスワード、ページ 302を参照してください。

インストールを確認する

Data Protectorソフトウェアコンポーネントが Cell Manager上またはクライアントシステム上で起動して動作しているかどうかを確認する必要がある場合は、Data Protectorグラフィカルユーザーインターフェイスを使って、インストールを確認できます。

前提条件

UNIXシステム用またはWindowsシステム用インストールサーバーなど、選択したクライアントシステムの種類に応じた、適切なインストールサーバーが必要です。

手順

1. コンテキストリストで**[クライアント]**をクリックします。
2. Scopingペインで、**[クライアント]**を展開して、Cell Managerまたはクライアントシステムを右クリックし、**[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. 同じ種類(UNIXシステムまたはWindowsシステム)のすべてのクライアントシステムが表示されます。インストールを確認するクライアントを選択して、**[完了]**をクリックすると、インストールの確認が開始されます。

[インストールチェック]ウィンドウに、インストールの確認結果が表示されます。

Data Protector Inetサービス構成について

Windowsシステムでは、バックアップセッションと復元セッションは、Data Protector Inetサービスによって起動されます。このサービスはデフォルトでWindowsローカルユーザーアカウントSYSTEMで実行されます。したがって、バックアップセッションや復元セッションは同じユーザーアカウントを使って実行されます。

統合

一部のData Protector統合では、バックアップセッションと復元セッションはWindowsドメインユーザーアカウントで起動する必要があります。Windows Server 2003システムでは、Data Protector Inetサービスは別のユーザーアカウントで再起動するだけで、バックアップセッションと復元セッションを起動できます。その他のサポートされているWindowsオペレーティングシステムでは、バックアップセッションと復元セッションはWindowsドメインユーザーアカウントでは開始できません。したがって、Data Protectorでは「ユーザーの偽装」という別の概念を使用します。つまり、Data Protector InetサービスはWindowsローカルユーザーアカウントSYSTEMで実行しますが、このサービスはWindowsドメインユーザーアカウントに偽装することが可能で、これによりこのユーザーアカウントで統合エージェントを開始できるようにします。

Data Protector Inetサービスの偽装を有効にするには、Windowsドメインユーザーアカウントをバックアップ仕様または復元ウィザードで指定して、このユーザーアカント(パスワードも含めて)をWindowsレジストリに保存する必要があります。

Windowsドメインユーザーアカウントでlnetサービスを実行する

場合によっては、Windowsドメインユーザーアカウントでdata Protector Inetサービスを実行する必要があります。

- **クラスター環境**

  クラスターでは、全クラスターノードにData Protector Inetサービスを構成する必要があります。これは、Windowsドメインユーザーアカウントをlnetアカウントとして使用する必要があることを意味します。

Windowsドメインユーザーアカウントでlnetサービスを実行する場合、以下のWindowsオペレーティングシステムセキュリティポリシー権限を与える必要があります。

- `Impersonate a client after authentication`
- `Replace a process level token`

Data Protector Inetサービスユーザーの偽装のためのユーザーアカウントの設定

Data Protector Inetサービスはデフォルトで`Windows`ローカルユーザーアカウント`SYSTEM`で実行されていますが、このサービスがセッションを開始するために別の`Windows`ドメインユーザーアカウントを使用するように指定できます。

- ユーザーアカウントを以下のように構成します。
  - データ(アプリケーションデータなど)にアクセスするための適切な権限をユーザーに付与します。
  - ユーザーを必ずのData Protector`admin`または`operator`ユーザーグループに追加します。

Data Protector GUIを使用する

手順

1. コンテキストリストで**[クライアント]**をクリックします。
2. Scopingペインで**Data Protector[セル]**、**[クライアント]**の順に展開します。
3. クライアントを右クリックし、**[偽装の追加]**をクリックします。

   > **注：**
   > ユーザーを変更または削除するには、**[偽装の変更]**または**[偽装の削除]**をクリックします。

4. [クライアントシステムの選択]ページで、Data Protector Inetサービスのユーザーの偽装を構成するクライアントシステムを選択し、**[次へ]**をクリックします。
5. 偽装の追加、削除、または変更ページで、新しいユーザーアカウントを追加するか、あるいは既存のユーザーアカウントを変更または削除して、**[完了]**をクリックします。

> **重要：**
> Windowsレジストリに保存したユーザーアカウントは、必要に応じてData Protector Inetサービスが使用します。

Data Protector CLIを使用する場合

- 1台のData Protectorクライアントでユーザーの偽装のためにユーザーアカウントを設定するには、`omniinetpasswd`コマンドを使用します。

  クライアントにログインして以下のコマンドを実行します。

  `omniinetpasswd -add User@DomainPassword`
- 複数台のData Protectorクライアントでユーザーの偽装のためにユーザーアカウントを設定するには、`omnicc`コマンドを使用します。

Cell Managerにログインして以下のコマンドを実行します。

```
omnicc -impersonation -add_user -user User@Domain -host ClientName1 -host
ClientName2 -host ClientName3 -passwd Password
```

omniinetpasswdおよびomniccコマンドの詳細については、『*HPE Data Protector Command Line Interface Reference*』を参照してください。

Data ProtectorInetアカウントを変更する

Data Protector Inetサービスが特定のユーザーアカウントでバックアップおよび復元に必要なプロセスを起動するようにするには、そのユーザーアカウントでサービスを再開する必要があります。

前提条件

- Microsoft Cluster Server:Microsoft Cluster Server: アカウントを変更する前に、OBVS_HPDP_AS, OBVS_HPDP_IDB, OBVS_HPDP_IDB_CPおよびOBVS_MCRSクラスターグループをオフラインにします。Data Protector Inetサービスが別のアカウントで再起動されたら、再度クラスターグループをオンラインに戻します。

Windowsシステムの場合

1. [コントロールパネル]で**[管理ツール]**をクリックした後、**[サービス]**をダブルクリックします。
2. **[Data Protector Inet]**をダブルクリックします。
3. [Data Protector Inetのプロパティ]の[全般]タブで、**[停止]**をクリックし、**[ログオン]**タブをクリックします。
4. **[現在のアカウント]**ボタンを選択します。
5. (共有ディスクにアクセスするための)正しいパーミッションを持つアカウントを入力するか、リストをブラウズして選択します。
6. パスワードを入力し、確認のためもう一度パスワードを入力します。
7. **[OK]**をクリックして、これらのプロパティページを閉じます。
8. [Data Protector Inet]を選択したまま右クリックし、**[開始]**をクリックします。
9. このダイアログボックスを終了します。

第3章: 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から配布してリモートでインストールすることも、適切なインストールパッケージ(zip/tar)からローカルにインストールすることもできます。

UNIXクライアントの場合、UNIX Data Protectorを使用してインストールサーバーをインストールする方法が推奨されます。

Data ProtectorのUNIXクライアントへのローカルインストールも可能ですが、インストールサーバーを使用せずにUNIXにパッチを適用するサポートされる手順がないので推奨されません。

UNIXクライアントにパッチを適用するには、インストールサーバーが必要なので、同じインストールサーバーを使用して最初にData ProtectorをUNIXクライアントにインストールすることが推奨されます。

> **注:** リモートインストール時にWindows インストールサーバーがターゲットにするのはクライアントのポート445です。HP-UX/Linux インストールサーバーの場合は、クライアントのポート22 (セキュアなリモートインストール)またはポート512/514 (非セキュアなリモートインストール)です。インストールサーバー側では、エフェメラルポートを使用して、これらのターゲットポートへの接続が行われます。

クライアントのインストールが完了したら、各クライアントの適切な環境変数にコマData Protectorンドの場所を追加して、どのディレクトリからでもHPEコマンドを実行できるようにすることをお勧めします。Data Protectorドキュメントの手順は、変数値が追加されていることを前提とします。コマンドの場所については、『*HPE Data Protector Command Line Interface Reference*』のomniintroのリファレンスページ、およびomniintroのman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、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、ページ 323を参照してください。セキュリティ保護の詳細については、セキュリティの留意事項、ページ 196を参照してください。

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クライアントのインストール、ページ 62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、ページ 71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クライアントのインストール、ページ 75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、ページ 81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、ペー

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
	ジ 84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、ページ 86を参照してください。
IBM AIX	リモートおよびローカルインストール。IBM AIXクライアントのインストール、ページ 85を参照してください。
HP OpenVMS	ローカルインストール。HP OpenVMSクライアントのインストール、ページ 89を参照してください。
その他のUNIXシステム	ローカルインストール。UNIXおよびMac OS Xシステムでのローカルインストール、ページ 102を参照してください。
DAS Media Agent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、ページ 105を参照してください。
ACS Media Agent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、ページ 105を参照してください。

統合

Data Protector用統合ソフトウェアとは、Data Protectorでデータベースアプリケーションをバックアップするソフトウェアコンポーネントです。Microsoft 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や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。

統合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、ページ 115」を参照してください。
Microsoft SQL Server	「Microsoft SQL Serverクライアント、ページ 122」を参照してください。
Microsoft SharePoint Server	「Microsoft SharePoint Serverクライアント、ページ 122」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
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、ページ 126」を参照してください。
Sybase Server	「Sybase Serverクライアント、ページ 127」を参照してください。
Informix Server	「Informix Serverクライアント、ページ 127」を参照してください。
SAP R/3	「SAP R/3クライアント、ページ 128」を参照してください。
SAP MaxDB	「SAP MaxDBクライアント、ページ 128」を参照してください。
SAP HANAアプライアンス	「SAP HANAアプライアンスクライアント、ページ 128」を参照してください。
Oracle Server	「Oracle Serverクライアント、ページ 129」を参照してください。
MySQL	「MySQLクライアント、ページ 129」を参照してください。
PostgreSQL	「PostgreSQLクライアント、ページ 130」を参照してください。
IBM DB2 UDB	「IBM DB2 UDBクライアント、ページ 130」を参照してください。
Lotus Notes/Domino Server	「Lotus Notes/Domino Serverクライアント、ページ 130」を参照してください。
VMware	「VMwareクライアント、ページ 131」を参照してください。
Microsoft Hyper-V	「Microsoft Hyper-Vクライアント、ページ 139」を参照してください。
Network Data Management Protocol (NDMP) Server	「NDMP Serverクライアント、ページ 140」を参照してください。
HPE P4000 SANソリューション	「HPE P4000 SANソリューション clients、ページ 140」を参照してください。
HPE P6000 EVAディスクアレイファミリ	「HPE P6000 EVAディスクアレイファミリ クライアント、ページ 141」を参照してください。
HPE P9000 XPディスクアレイファミリ	「HPE P9000 XPディスクアレイファミリ クライアント、ページ 147」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
HPE 3PAR StoreServ Storage	「HPE 3PAR StoreServ Storage clients、ページ 153」を参照してください。
EMC Symmetrix	「EMC Symmetrixクライアント、ページ 153」を参照してください。
EMC VNXストレージプロバイダー	「non–HPE Storage Arrays、ページ 157」を参照してください。
EMC VMAXストレージプロバイダー	「non–HPE Storage Arrays、ページ 157」を参照してください。
NetAppストレージプロバイダー	「non–HPE Storage Arrays、ページ 157」を参照してください。

他のインストール

インストール	リファレンス
HPE Serviceguard	「HPE ServiceguardへのData Protectorのインストール、ページ 164」を参照してください。
Symantec Veritas Cluster Server	「Symantec Veritas Cluster ServerへのData Protectorのインストール、ページ 175」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、ページ 178」を参照してください。
IBM HACMPクラスター	「Data ProtectorのIBM HACMPクラスターへのインストール、ページ 189」を参照してください。
Microsoft Hyper-Vクラスター	「Microsoft Hyper-VクラスターでのData Protectorのインストール、ページ 189」を参照してください。

Data Protectorコンポーネント

サポート対象プラットフォームの最新情報は、HPE Data Protectorのホームページ (https://softwaresupport.hpe.com/manuals)でご確認ください。

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。

ユーザーインターフェイス	ユーザーインターフェイスコンポーネントには、Data Protectorのグラフィカ

	ルユーザーインターフェイス(Windowsシステム)とコマンドラインインターフェイスの一部(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:** Data Protectorコマンドラインインターフェイ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、『*HPE Data Protector Command Line Interface Reference*』を参照してください。 異種混合環境でData Protectorのユーザーインターフェイスをする前に、『HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照して制限事項を確認してください。
英語版ドキュメント(ガイド、ヘルプ)	Data Protectorの英語版ドキュメントファイルセットです。
フランス語のドキュメント(ガイド、ヘルプ)	Data Protectorのフランス語版ドキュメントファイルセットです。
日本語のドキュメント(ガイド、ヘルプ)	Data Protectorの日本語版ドキュメントファイルセットです。
簡体字中国語のドキュメント(ガイド、ヘルプ)	Data Protectorの簡体字中国語版ドキュメントファイルセットです。
Manager-of-Managersユーザーインターフェイス	Manager-of-Managersユーザーインターフェイスには、Data Protectorのグラフィカルユーザーインターフェイスが含まれます。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ユーザーインターフェイスと Managerユーザーインターフェイスは、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。
自動ディザスタリカバリ	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手法を使用して復旧を行うシステムと、拡張自動ディザスタリカバリ(EADR)またはワンボタンディザスタリカバリ(OBDR)で使用するDR CD ISOイメージを作成することによってディザスタリカバリを自動化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 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 MaxDB用統合ソフトウェア	SAP MaxDB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。
SAP HANA用統合ソフトウェア	SAP HANA用統合ソフトウェアコンポーネントは、Data Protectorによる保護の対象となるSAP HANAアプライアンスを代表または構成す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。
MySQL統合	MySQL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MySQL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。
仮想環境用統合ソフトウェア	仮想環境用統合ソフトウェアのコンポーネントは、Data Protectorの仮想環境用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。
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用統合ソフトウェアコンポーネントは、Data Protector Microsoft Exchange Server 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 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+用統合ソフトウェア	MS Exchange Server 2010+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またはMicrosoft Exchange Server 2013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	MS 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 2007/2010/2013用統合ソフトウェア	MS SharePoint 2007/2010/2013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 2007/2010/2013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システムにインストールする必要があります。
HPE P4000 VSS Agent	HPE P4000 VSS Agentコンポーネントは、HPE 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の両方にインストールする必要があります。
HPE P6000/HPE 3PAR SMI-S Agent	HPE P6000/HPE 3PAR SMI-S Agentコンポーネントは、Data ProtectorをHPE P6000 EVAディスクアレイファミリと統合する場合、またはData ProtectorをHPE 3PAR StoreServ Storageと統合する場合、アプリケーションシステムとバックアップシステムの両方にインストールする必要があります。
HPE P9000 XP Agent	HPE P9000 XP Agentコンポーネントは、Data ProtectorをHPE P9000 XPディスクアレイファミリと統合する場合に、アプリケーションシステムとバックアップシステムの両方にインストールする必要があります。
HPE 3PAR VSS Agent	HPE 3PAR VSS Agentコンポーネントは、アプリケーションシステムとバックアップシステムがWindowsシステムで、ボリュームシャドウコピーサービスを使用してデータをバックアップおよび復元する構成でData ProtectorをHPE 3PAR StoreServ Storageと統合する場合、アプリケーションシステムとバックアップシステムの両方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、Data ProtectorをEMC Symmetrix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の両方にインストールする必要があります。
EMC VNXストレージプロバイダー	EMC VNXストレージプロバイダーコンポーネントは、Data ProtectorをEMC VNX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の両方にインストールする必要があります。EMC VNXストレージプロバイダーコンポーネントは、Data ProtectorSMI-S Agentのプラグインです。
EMC VMAXストレージプロバイダー	EMC VMAXストレージプロバイダーコンポーネントは、Data ProtectorをEMC VMAX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の両方にインストールする必要があります。EMC VMAXストレージプロバイダーコンポーネントは、Data ProtectorSMI-S Agentのプラグインです。
NetAppストレージプロバイダー	NetAppストレージプロバイダーコンポーネントは、Data ProtectorをNetAppストレージと統合する場合に、アプリケーションシステムとバックアップシステムの両方にインストールする必要があります。仮想環境統合の場合は、このコンポーネントをバックアップシステムにのみインストールする必要があります。NetAppストレージプロバイダーコンポーネントは、Data Protector SMI-S Agentのプラグインです。
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。Data Protector
MS Exchange Granular Recovery Extension	Microsoft Exchange Server用Data Protector Granular Recovery Extensionは、Granular Recovery機能を有効化するために、各Microsoft Exchange Serverシステムにインストールする必要があります。Microsoft Exchange Server Database Availability Group (DAG)環境では、DAG内の任意のExchange Server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用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拡張GRE Webプラグイン	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拡張GRE Webプラグインコンポーネントをを VMware Virtual Serverシステムにインストールする必要があります。ファイルの復旧にWebプラグインを使用する前に、Data Protector GRE環境を構成する必要があります。
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:
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サービス

Data Protector以下の形式で指定します。

`Inet`	クライアントバックアップサービス
`CRS`	Cell Managerサービス
`hpdp-idb`	内部データベースサービス
`hpdp-idb-cp`	内部データベース接続プーラー
`hpdp-as`	アプリケーションサーバー

デフォルトでは、`Inet`および`hpdp-*`サービスはローカルシステムアカウント下で実行され、`CRS`は管理者アカウント下で実行されます。

いずれのサービスのアカウント情報も変更可能です。ただし、新しいアカウントは以下の最低条件を満たしている必要があります。

サービス	リソース	サービスによって必要とされる最低限のリソースパーミッション
CRS	*Data_Protector_program_data* HKLM\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII	フルアクセス フルアクセス
Inet	バックアップと復元 所有権の取得	- -

Windowsクライアントのインストール

各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については、https://softwaresupport.hpe.com/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。

- 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、『HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照してください。
- ポート番号5555 (デフォルト)が利用可能であること。
- ホスト名を解決するためのDNS逆引き参照は、Data Protectorセル内のすべてのData Protectorコンポーネントに必要です。
- 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。コンピューター名とホスト名は同じである必要があります。
- 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 Server 2008またはWindows Server 2012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。アカウントを有効にし、*管理承認モード*は無効にする必要があります。

- 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のインストールを開始するにあたって、Microsoft Installer(MSI) 2.0がシステムにインストールされていることを確認してください。これよりも古いバージョンがインストールされている場合は、Data Protectorのインストールを開始する前にバージョン2.0にアップグレードすることをお勧めします。MSIのアップグレードを行わないでインストールを開始すると、Data Protectorセットアップウィザードによって必要なバージョンに自動的にアップグレードされます。この場合、Data Protectorにより、MSIのアップグレードに関する情報が表示されます。

  MSIのアップグレード後は、システムの再起動をお勧めします。

自動ディザスタリカバリ

`Automatic Disaster Recovery`コンポーネントは、拡張自動ディザスタリカバリ(EADR)、ワンボタンディザスタリカバリ(OBDR)、自動システム復旧(ASR)のいずれかを使用して復旧を行うシステムと、EADRまたはOBDRで使用するDR CD ISOイメージを作成するシステム上に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。詳細については、クラスター対応クライアントのインストール、ページ 186を参照してください。

インストール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、ページ 57を参照してください。

ローカルインストール

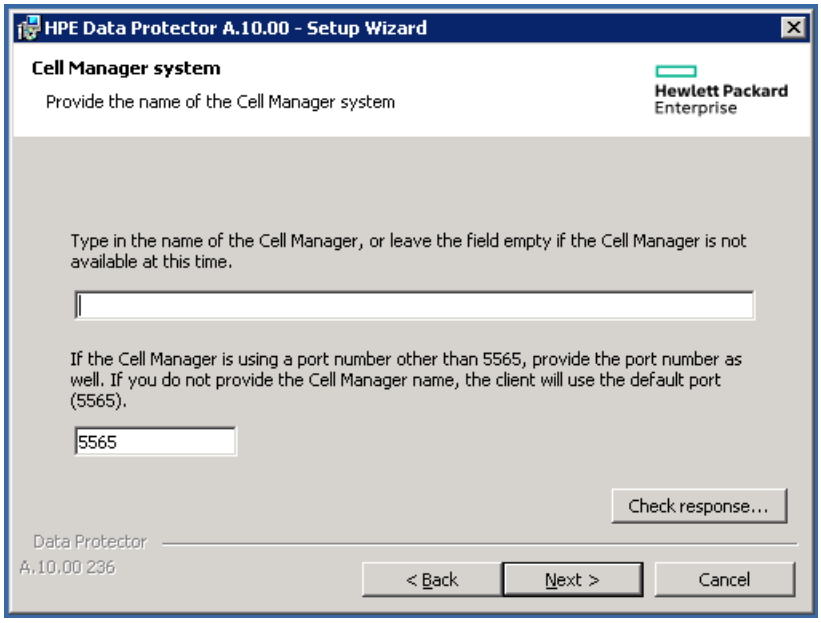
Windowsクライアントは、Windowsインストールパッケージ(zip)を使用して、ローカルにインストールできます。

1. Windowsシステムにダウンロードしたインストールパッケージ(zip)をコピーし、ローカルディレクトリに展開します。プラットフォームに適用可能なフォルダーから`setup.exe`ファイルを実行します。
2. セットアップウィザードに従い、ライセンス契約を十分にお読みください。**[Next]**をクリックし、次に進みます。
3. [Installation 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。
4. Cell Managerの名前を入力します。

   Cell Managerでデフォルトポート番号5565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]**をクリックして、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します。

   [次へ]をクリックします。

Cell Managerの選 択



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

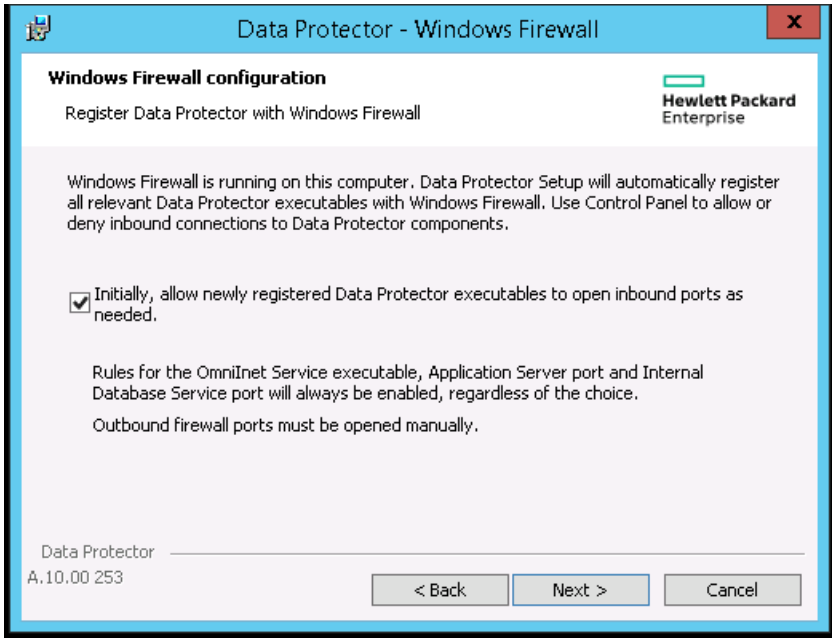
   それ以 外 の場 合 は、**[Change]**をクリックして[Change Current Destination Folder]ページを開き、パスを入 力します。

6. インストール対 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 については、Data Protectorコンポーネント、ページ 57を参 照してください。

   [次 へ]をクリックします。

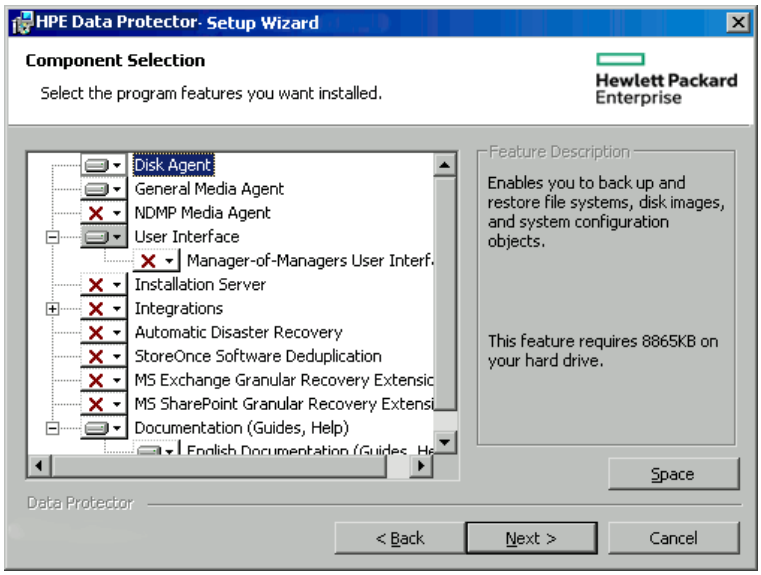
7. システムにWindows Firewallが検 出 された場 合 、Windows Firewallの構 成 ページが表 示 されます。Data Protectorセットアップでは、すべての必 要 なData Protector実 行 可 能 ファイルが記 録 されます。デフォルトでは、**[Initially, allow newly registered Data Protector executables to open inbound ports as needed]**オプションが選 択 されています。この時 点 で、Data Protectorによってポートがオープンされないようにするには、オプションを選 択 解 除 します。Data Protectorが以 前 のバージョンの10.00クライアントで適 切 に機 能 するには、WindowsファイアウォールのData Protectorルールを有 効 にする必 要 があります。OmniInetサービス実 行 可 能 ファイル、アプリケーションサーバーポート、内 部 データベースポートのルールは、選 択 内 容 にかかわらず常 に有 効 になります。



[次 へ]をクリックします。

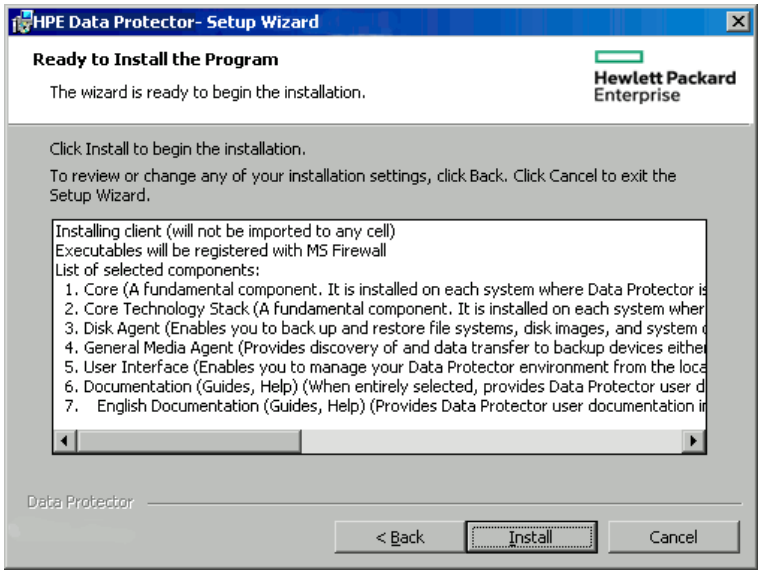
8. 選 択 コンポーネント のサマリーページが表 示 されます。**[Install]**をクリックして、選 択 したコンポーネント をインストールします。

   コンポーネント選 択 サマリーページ



9. インストールステータスのページが表 示 されます。**[次 へ]**をクリックします。

インストールサマリーページ



10. `User Interface`コンポーネントをインストールした場合に、セットアップ直後にData Protector GUIを使用して操作を開始するには**[Launch Data Protector GUI]**を選択します。

    `English Documentation (Guides, Help)`コンポーネントをインストールした場合に、セットアップ直後に『*HPE Data Protector製品案内、ソフトウェアノートおよびリファレンス*』を表示するには、**[Open the Product Announcements, Software Notes, and References]**を選択します。
11. **[完了]**をクリックします。

ローカルにインストールされたクライアントのインポート

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システムを手動で追加することを意味します。システムをData Protectorセルに追加すると、このシステムはData Protectorクライアントとして機能します。

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、ページ 194を参照してください。

インポートするクライアントの構成

この手順は、ローカルインストールの際にCell Managerの名前を指定しなかった場合にのみ適用されます。

ローカルインストールが完了したら、クライアント側で次のコマンドを実行します。

```
omnicc -secure_comm -configure_peer <Cell manager hostname>
```

これにより、クライアントがCell Manager証明書付きで構成されます。ローカルにインストールされるクライアントでは、この手順は必須です。また、このコマンドは、削除したクライアントの再インポートにも必要です。

Cell Managerの証明書の指紋表示に対して**y/n**オプションの選択を要求するコマンドが表示されます。**y**を入力して構成を正常に完了します。

クライアントを検証なしで構成する場合は、`-accept_host`コマンドの末尾にコマンドを追加します。

```
omnicc -secure_comm -configure_peer <Cell manager hostname> -accept_host
```

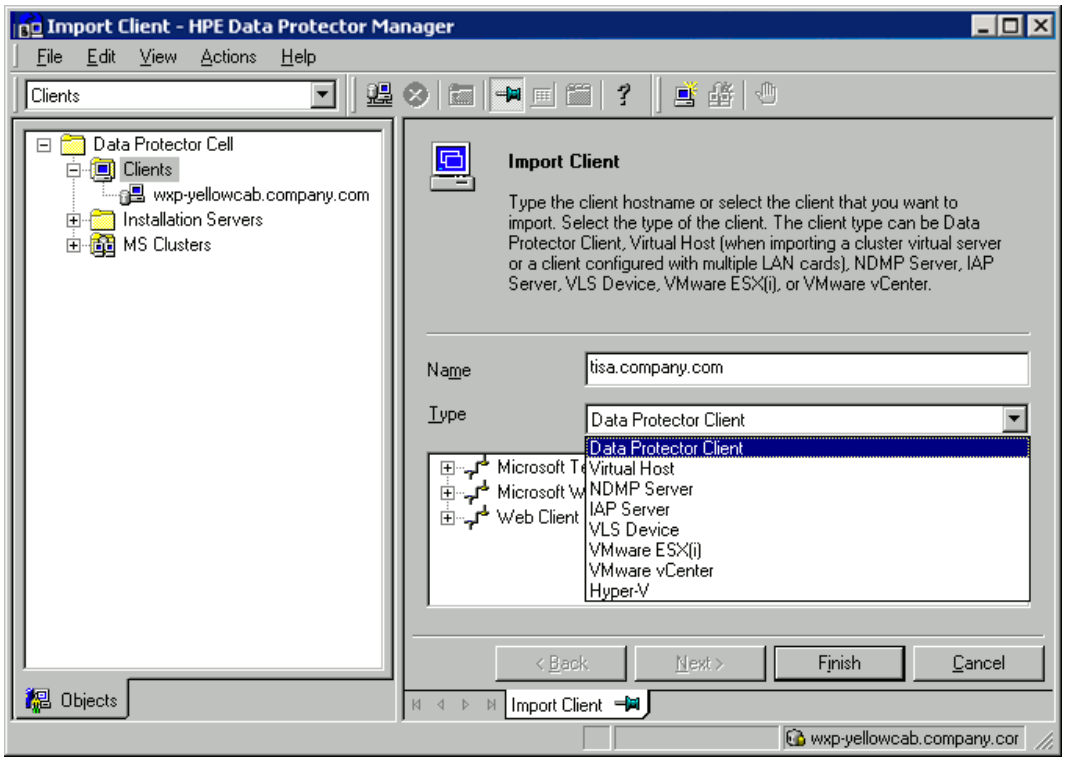
accept_hostコマンドを使用すると、コンソールに**y/n**オプションは表示されません。

GUIを使用してクライアントシステムをインポートするには:

ユーザーが**[フィンガープリントの承認]**オプションを選択した場合は、フィンガープリントウィンドウは表示されず、ホストはユーザーの確認を必要とすることなく承認されます。このオプションが選択されていない場合は、フィンガープリントウィンドウが表示され、ユーザーは手動でフィンガープリントオプションを承認する必要があります。

1. コンテキストリストで**[クライアント]**をクリックします。
2. Scopingペインで**[クライアント]**を右クリックし、**[クライアントのインポート]**をクリックします。
3. インポートするクライアント名を入力します。Windows GUIを使用している場合は、ネットワークを参照して目的のクライアントを選択することもできます。

   セルへのクライアントのインポート



複数のLANカードを持つよう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サーバー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、[Name]テキストボックスにOpenVMSクライアントのTCP/IP名を入力します。

Data ProtectorのMicrosoft Exchange Server 2010用統合ソフトウェアで使用するMicrosoft Exchange Server 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]**をクリックして、ログインの資格情報を指定します。

> **注 :**
> vCD vStorageイメージのバックアップ方法を使用して仮想マシンをバックアップできるようにするには、VMware vCloud Directorが使用するすべてのvCenter ServerシステムをVMware vCenterとしてData Protectorセルにインポートする必要があります。

4. **[次へ]**をクリックします。
5. **[完了]**をクリックしてクライアントをインポートします。

インポートしたクライアントの名前が[結果エリア]に表示されます。

CLIを使用してクライアントシステムをインポートするには:

Data Protectorクライアントをインポートするには`omnicc -import_host`コマンドが使用され、外部のCell Managerをインポートするには`omnicc -import_cs`コマンドが使用されます。仮想クライアントをインポートする場合は、コマンドに`-virtual`を追加します。

Cell Managerの証明書の指紋表示に対して**y/n**オプションの選択を要求するコマンドが表示されます。**y**を入力して構成を正常に完了します。クライアントを検証なしで構成する場合は、コマンドの末尾に`-accept_host`を追加します。

インストール時のCell Managerの指定

インストール時にCell Managerを指定する場合、インストールの一環としてクライアントにCell Manager証明書が構成されますが、インポートは実行されません。

GUIまたはCLIを使用してクライアントシステムをインポートするには、「GUIを使用してクライアントシステムをインポートするには」および「CLIを使用してクライアントシステムをインポートするには」の各項を参照してください。

MOM構成内のCell Manager

MOM構成にCell Managerを含めるには、次の手順を実行する必要があります。

1. 次のコマンドを使用してMOMサーバーでCell Managerを構成する必要があります。

   ```
   omnicc -secure_comm -configure_peer <MOM server>
   ```

   これにより、Cell Manager内にMOMサーバーが構成されます。MOMサーバーのフィンガープリントがプロンプト表示され、ユーザーはこれを承認する必要があります。
2. MOM GUIからCell Managerをインポートします。ユーザーは、Cell Manager証明書のサムプリントを承認するように求められます。

> **注 :**
> 異なるバージョンのCell Managerは、MOM構成には含めることができません。

インストールサーバーのローカルインストール

いつ追加を行うか

次の場合、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、たとえばインストールサーバーとは別 のシステム上 にUNIX Cell Manager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。

インストールサーバーの構 成

以 下 のコマンドを実 行 してインストールサーバーホストを構 成 してください。

```
omnicc -secure_comm -configure_peer <CM host name>
```

インストールサーバーのインポート

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 Protector GUI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インポート]**をクリック して、ウィザードを起 動 します。以 下 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。

Windows/Unix/HP-UX上 でインストールサーバーをCell Managerにインポートする例

hostname1.company.netがCell Managerであり、**hostname2.company.net**がインストールサーバーの 場 合 、インストールサーバーで次 のコマンドを実 行 します。

```
omnicc -secure_comm -configure_peer hostname1.company.net

[root@hostname2 etc]# omnicc -secure_comm -configure_peer hostname1.company.net

- Please use the

fingerprint to validate the certificate manually!

Certificate information:

- Hostname:hostname1.company.net

- Valid: from Sep 24 06:25:52 2016 GMT until Sep 22 06:25:52 2026 GMT

- Fingerprint: e9:2a:3f:ed:af:10:c1:f7:7h:67:69:4b:4d:51:87:25:6h:79:gr:78

Do you want to continue (y/n)?y

Host 'hostname1.company.net' configured for secure configuration successfully.
```

証 明 書 の変 更 と確 認 が必 要 なため、Cell Managerで次 のコマンドを使 用 してインストールサーバーを再 インポートします。

```
omnicc -import_is HostName [-accept_host]
```

```
C:\Program Files\OmniBack\bin>omnicc -import_is hostname2.company.net

- Please use the fingerprint to validate the certificate manually!

Certificate information:

- Hostname:hostname2.company.net

- Valid: from Aug 24 07:26:15 2016 GMT until Aug 22 07:26:15 2026 GMT

- Fingerprint: f5:3b:3h:gb:cf:10:d1:f7:7d:67:60:5b:4d:51:87:76:6h:51:rg:89

Do you want to continue (y/n)?y

Import host successful.
```

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)。
   「Windowsシステム上の未使用のSCSIターゲットIDの取得、ページ 374」を参照してください。
2. まだ使用されていないSCSI Target 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。詳細については、使用するデバイスのドキュメントを参照してください。

   サポート対象デバイスの詳細については、https://softwaresupport.hpe.com/を参照してください。
3. コンピューターの電源を切り、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ー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ー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HPE 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ー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、HPE 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ーをロードまたはアンロードする方法は、Windowsシステムでのテープドライバーおよびロボティクスドライバーの使用、ページ 359を参照してください。
デバイスファイル名の作成の詳細については、Windowsシステム上でのデバイスファイル(SCSIアドレス)の作成、ページ 361を参照してください。

次に行う手順

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。構成タスクに関する情報については、『*HPE Data Protectorヘルプ*』のキーワード「構成、バックアップデバイス」で表示される内容を参照してください。

HP-UXクライアントのインストール

HP-UXクライアントのインストールは、UNIX用インストールサーバーを使用したリモートインストール、またはUNIXインストールパッケージ(tar)を使用したローカルインストールが可能です。

インストール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、ページ 57を参照してください。

前提条件

- 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。インストールが完了していない場合は、Data Protector Cell Managerおよびインストールサーバーのインストール、ページ 26を参照してください。
- インストールを実行するには、*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。
- ホスト名を解決するためのDNS逆引き参照は、Data Protectorセル内のすべてのData Protectorコンポーネントに必要です。
- HP-UX 11.11でインターネットプロトコルのバージョン6(IPv6)を使用するには、IPv6NCF11iバンドルまたはTOUR/IPv6サポートが必要です。

  詳細については、HP-UXシステムのパッチ、ページ 224を参照してください。

  UNIXシステム上のData Protectorクライアントコンポーネントに関するRAMおよびディスクスペースの要件

  UNIXシステム上の各種Data Protectorクライアントコンポーネントにおけるディスクスペースの最小要件は、以下の表のとおりです。

  RAMおよびディスクスペースの要件

クライアントシステムコンポーネント	RAM (MB) [1]	空きディスクスペース(MB) [2]
Disk Agent	各64(128推奨)	各20
Media Agent		
統合コンポーネント		
英語版ドキュメント(ガイド、ヘルプ)	該当なし	100

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ーフェイスを使って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の詳細については、リモートインストール、ページ 94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ー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。

ローカルインストール

インストールサーバーの場合

お使いの環境にUNIX用のインストールサーバーがインストールされていない場合、UNIX用インストールパッケージ(tar)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。ローカルインストールの手順については、インストールサーバーのローカルインストールを参照してください。

クライアントの場合

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。ローカルにインストールされたクライアントのインポート、ページ 66を参照してください。

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。詳細については、『クラスター対応クライアントのインストール、ページ 168』を参照してください。

[1] 表中の数値はコンポーネントのみに関する要件です。オペレーティングシステム、ページングファイル、またはその他のアプリケーションに対するスペースの割り当ては含まれていません。
[2] 表中の数値はコンポーネントのみに関する要件です。オペレーティングシステム、ページングファイル、またはその他のアプリケーションに対するスペースの割り当ては含まれていません。

HP-UXのカーネル構成のチェック

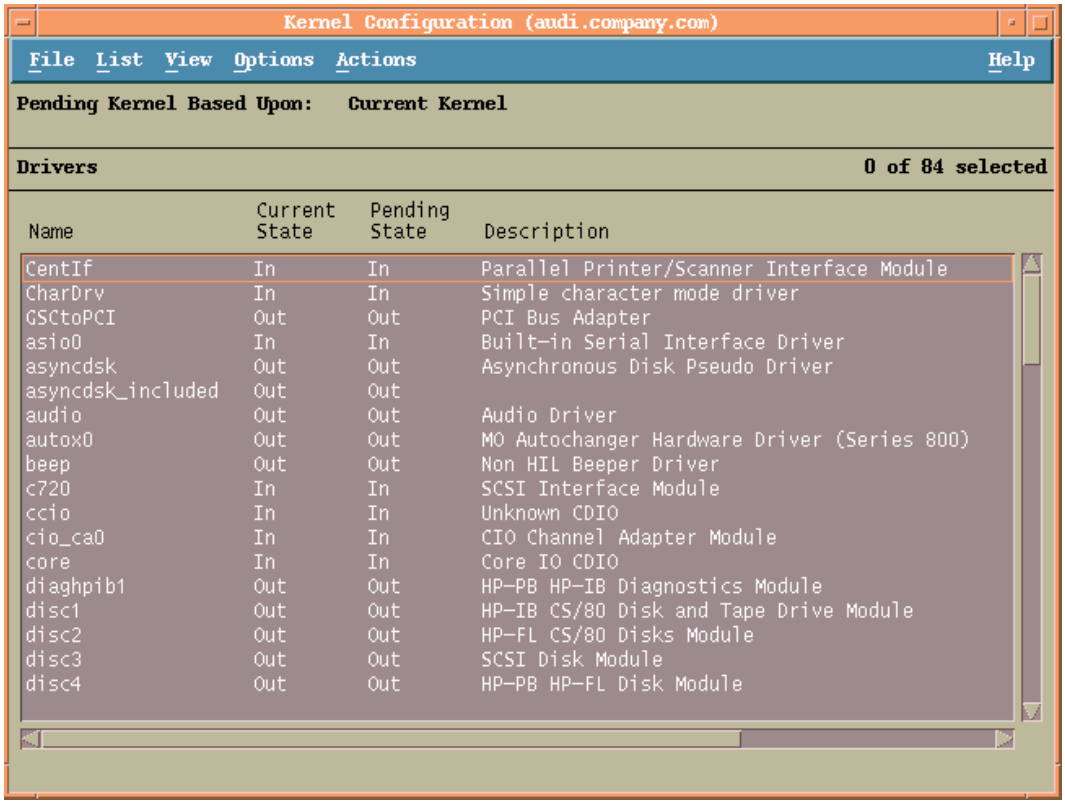
*HPE System Administration Manager (SAM)*ユーティリティを使って、HP-UX 11.x上のカーネルの構成をチェックおよびビルドするには、以下の手順に従ってください。カーネルを手動でビルドする方法の詳細については、HP-UXシステム上のSCSIロボティクス構成、ページ 362を参照してください。

*HPE System Administration Manager (SAM)*ユーティリティを使ってカーネル構成をビルドするには、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ーがインストール済みドライバーのリストに含まれていること。[Kernel Configuration]ウィンドウ、次のページを参照してください。目的のドライバー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。例：
     - テープデバイスにはテープデバイスドライバーが必要です。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ー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`ドライバーはDLTやLTOなどの汎用的なSCSIテープドライブで使用され、`tape2`ドライバーは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ー(`sctl`または`spt`)か、オートチェンジャーロボティクスドライバー(`schgr`)が必要です。

       詳細は、HP-UXシステム上のSCSIロボティクス構成、ページ 362を参照してください。

[Kernel Configuration]ウィンドウ



- **[Current State]**列でドライバーのステータスが**[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。
  a. リスト内のドライバーを選択します。**[Actions]**をクリックして**[Add Driver to Kernel]**を選択します。**[Pending State]**列のステータスが変化します。変更後：`In`.

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

必要なドライバー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ーに接続してください。

バックアップデバイスのHP-UXシステムへの接続

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。
   `/usr/sbin/ioscan -f` システムコマンドを使用します。

   詳細については、HP-UXシステム上の未使用のSCSIアドレスの取得、ページ 368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、通常はデバイス上のスイッチで設定できます。詳細については、使用するデバイスのドキュメントを参照してください。

   サポート対象デバイスの詳細については、https://softwaresupport.hpe.com/を参照してください。

3. デバイスをコンピューターに接続し、デバイスとコンピューター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。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。HP-UXシステム上のデバイスファイルの作成、ページ 366を参照してください。

インストール手順が完了し、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、『*HPE Data Protector ヘルプ*』のキーワード「構成、バックアップデバイス」で表示される内容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クライアントのインストール

Solarisクライアントのインストールは、UNIX用インストールサーバーを使用したリモートインストール、またはUNIXインストールパッケージ(tar)を使用したローカルインストールが可能です。

インストール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、ページ 57を参照してください。

前提条件

- Media Agentをインストールする際には、/etc/systemファイルに次のエントリがあることを確認してください。

  ```
  set semsys:seminfo semmni=100
  ```

- 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およびインストールサーバーのインストール、ページ 26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。
- ホスト名を解決するためのDNS逆引き参照は、Data Protectorセル内のすべてのData Protectorコンポーネントに必要です。

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ーフェイスを使って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の詳細については、リモートインストール、ページ 94を参照してください。

> **注：**
> User Interfaceコンポーネントをインストールする場合は、コンポーネントを使用する前に環境変

> 数を更新する必要があります。詳細については、環境変数の設定、ページ 33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。

> **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/`
>
> 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：**
> リモートからインストールまたはアップグレードする場合、`/tmp`フォルダーおよび`/var/tmp`フォルダーにはインストールするパッケージの最大サイズ以上の空きディスクスペースがなければなりません。

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インストールされていない場合、UNIX用インストールパッケージ(tar)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システムでのローカルインストール、ページ 102を参照してください。

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。詳細については、『クラスター対応クライアントのインストール、ページ 178』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、使用するプラットフォームとデバイスの種類に応じて構成をチェックし、必要な変更作業を確認してください。

- パッチ適用済みのSolaris 9またはSolaris 10システム環境の場合、テープデバイスドライバーはデフォルトでデバイスをサポートしている可能性があります。サポートの有無のチェックには、`strings`コマンドを実行します。

  たとえば、追加で構成作業を行わずにHPE DAT-72デバイスが使用可能かどうかをチェックするには、次のコマンドを実行します。

  Solaris (SPARC)システムの場合：

  ```
  strings /kernel/drv/sparcv9/st | grep HP
  ```

  Solaris (x86、x64)システムの場合：

```
strings /kernel/drv/st | grep HP
```

コマンド出力を確認します。デバイスが存在する場合、追加の手順は必要ありません。存在しない場合、次の手順を実行します。

- HPE 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HPEデータエントリは、HPE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;
```

- HPE 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HPE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：**
> HPE 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。

- 使用する各テープデバイスについて、/kernel/drv/st.confファイルに次の行が存在することを確認し、必要に応じて追加します。*ID*プレースホルダーを、デバイスのアドレスで置換します。

  SCSIデバイス:

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

  ファイバーチャネルデバイス:

  ```
  name="st" parent="fp" target=ID
  ```

  parentパラメーターの値は、テープデバイスによって異なる場合があります。詳細については、テープデバイスのドキュメントを参照してください。

- Solaris 9以前のバージョンでSCSIエクスチェンジャーデバイスを制御する場合は、SCSIパススルードライバーを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. 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。

     32ビット版Solaris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ビット版Solaris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. /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. 制御するSCSIエクスチェンジャーデバイスについて、/kernel/drv/sst.confファイルに次の行が含まれていることを確認し、必要に応じて挿入します。*ID*プレースホルダーを、デバイスのアドレスで置換します。

     SCSIデバイス:

     ```
     name="sst" class="scsi" target=ID lun=0;
     ```

     ファイバーチャネルデバイス:

```
name="sst" parent="lpfc" class="scsi" target=ID lun=0;
```

parentパラメーターの値は、テープデバイスによって異なる場合があります。詳細については、テープデバイスのドキュメントを参照してください。

4. 以下のコマンドを入力して、システムにドライバーをインストールします。

   ```
   add_drv sst
   ```

5. 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ー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、まず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(Solaris (SPARC)専用の手順)。

   ```
   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デバイスを使用する準備として、次の例で示す手順を実行します。

   a. /kernel/drv/st.confを編集し、割り当てられたSCSIポートを使用するためにデバイスパラメーターを設定します。詳細については、デバイスのドキュメントを参照してください。テープデバイスドライバーがデフォルトではデバイスをサポートしない場合のみ、tape-config-listパラメーターを変更します。

   b. /kernel/drv/sgen.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ーを構成します。詳細については、デバイスのドキュメントを参照してください。

   c. /usr/kernel/drv/sgen.conf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 SCSIエクスチェンジャー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;
      ```

- Solaris 10 (SPARC、x86、x64)でSCSIエクスチェンジデバイスを制御するには、付属のsgenドライバーを構成してからSCSIデバイスをインストールします。以下の手順に従ってください。

  1. ファイル/kernel/drv/sgen.confを開きます。

     ファイルでdevice-type-config-listパラメーターが指定されている場合、その行にチェンジャーデバイスの参照を追加します。次に例を示します。

     ```
     device-type-config-list="scanner", "changer";
     ```

     パラメーターが定義されていない場合、次の行を追加します。

     ```
     device-type-config-list="changer";
     ```

  2. 制御するSCSIエクスチェンジャーデバイスについて、/kernel/drv/sgen.confファイルに次の行が含まれていることを確認し、必要に応じて挿入します。*ID*プレースホルダーを、デバイスのアドレスで置換します。

     ```
     name="sgen" class="scsi" target=ID lun=0;
     ```

  3. 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ー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、まず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(SPARCシステム専用の手順)。

```
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デバイスを使用する準備として、次の例で示す手順を実行します。

a. /kernel/drv/st.confを編集し、割り当てられたSCSIポートを使用するためにデバイスパラメーターを設定します。詳細については、デバイスのドキュメントを参照してください。テープデバイスドライバーがデフォルトではデバイスをサポートしない場合のみ、tape-config-listパラメーターを変更します。

b. /kernel/drv/sgen.conf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 SCSIエクスチェンジャードライブに関して以下のデータを/kernel/drv/sgen.confファイルに追加します。

```
name="sgen" 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(Solaris 9以前のバージョン)または/kernel/drv/sgen.confファイル(Solaris 10)の変更が完了したら、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

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、コンピューター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については、https://softwaresupport.hpe.com/manualsを参照してください。

   > **注:**
   > 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。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、テープドライバーは、未定義の状態となり、システムの再起動が必要になります。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. Solaris (SPARC)システムの場合、システムの電源を投入し、Stop-Aキーを押して起動プロセスを中断します。

4. 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。
5. 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:**
   > Solaris 9以前のバージョン(特に64ビット版Solarisの場合)では、SCSI制御デバイス(ピッカー)へのリンクが自動生成されないことがあります。Solaris 10では、このリンクは生成されません。このような場合、シンボリックリンクを作成し、/dev/rsst*Num* (*Num*は任意の数字)にデバイスファイルを追加します。例:
   >
   > ***sstの場合:***
   >
   > ```
   > ln -s /devices/pci@1f,4000/scsi@3,1/sst@4,1:character /dev/rsst4
   > ```
   >
   > ***sgenの場合:***
   >
   > ```
   > ln -s /devices/pci@1e,600000/QLGC,qla@3/sgen@8,2:changer /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エクスチェンジャーデバイス(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、テープドライブには/dev/rmt/0cbnではなく/dev/rmt/0h)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。

次に行う手順

インストール手順が完了し、バックアップデバイスをSolarisクライアントに正しく接続したら、バックアップデバイスやメディアプールの構成、その他構成タスクの追加情報について、『*HPE Data Protectorヘルプ*』のキーワード「構成、デバイスのバックアップ」で表示される内容を参照してください。

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のインストールは、UNIX用インストールサーバーを使用したリモートインストール、またはUNIXインストールパッケージ(tar)を使用したローカルインストールが可能です。

インストール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、ページ 57を参照してください。

前提条件

- 32ビットGNU Cライブラリ(glibc)パッケージが64ビットLinuxシステム(x86_64)上にインストールされている必要があります。
- 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およびインストールサーバーのインストール、ページ 26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。
- 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。
  - クライアントにパスワードなし認証があるか、または`ssh`が構成されている。
- カーネルがSCSIデバイスをサポートしていることを確認してください(`SCSI support`、`SCSI tape support`、`SCSI generic support`モジュール)。パラメーター`Probe all LUNa on each SCSI device`は、省略可能です。

  Linuxカーネルでの SCSIサポートの詳細については、お使いのLinuxディストリビューションまたはLinuxカーネルのドキュメントを参照してください。
- ホスト名を解決するためのDNS逆引き参照は、Data Protectorセル内のすべてのData Protectorコンポーネントに必要です。

> **注 :**
> Data Protectorはデフォルトでポート番号 5555/5565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オペレーティングシステムのディストリビューションでは、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 5555/5565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。デフォルトのData Protector Inetポートの変更、ページ 345を参照してください。

自動ディザスタリカバリ

`Automatic Disaster Recovery`コンポーネントは、拡張自動ディザスタリカバリ(EADR)またはワンボタンディザスタリカバリ(OBDR)を使用して復旧を行うシステムと、EADRまたはOBDRで使用するDR CD ISOイメージを作成するシステム上にインストールする必要があります。

HPE Serviceguardクラスター

HPE 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。

インストールが終了したら、*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。

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ーフェイスを使用します。ソフトウェア配布手順の詳細については、リモートインストール、ページ 94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。

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インストールされていない場合、UNIX用インストールパッケージ(tar)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システム用のインストールサーバーのインストール、ページ 42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 細については、使 用するデバイスのド キュメントを参 照してくださ い。

   サポート対 象 デバイスの詳 細については、https://softwaresupport.hpe.com/を参 照してください。
3. デバイスをコンピューターに接 続し、デバイスとコンピューターの電 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 Enterprise Linuxシステムの場 合 は、コンピューターに新 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 動します。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
   ```

   例 :

   ```
   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 ティクス用 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。

次 に行う手 順

インストール手 順 が完 了し、Linuxクライアントシステムにバックアップデバイスが正 しく接 続されたら、デバイ スおよびメディアプールを構 成する方 法 やその他 の構 成タスクについて、『*HPE Data Protectorヘルプ*』の キーワード「構 成 、バックアップデバイス」で表 示される内 容を確 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、ページ 81を参 照してくだ

さい。

IBM AIXクライアントのインストール

IBM AIXクライアントのインストールは、UNIX用インストールサーバーを使用したリモートインストール、またはUNIXインストールパッケージ(tar)を使用したローカルインストールが可能です。

インストールプロセスを開始する前に、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、ページ 57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、およびData Protectorコンポーネントについては、『HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照してください。
- 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およびインストールサーバーのインストール、ページ 26を参照してください。
- ホスト名を解決するためのDNS逆引き参照は、Data Protectorセル内のすべてのData Protectorコンポーネントに必要です。
- `Disk Agent`コンポーネントをインストールする前に、選択したシステム上で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クラスター

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、ページ 112を参照してください。

インストールが終了したら、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。

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ーフェイスを使って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の詳細につい

ては、Data Protectorクライアントのインストール、ページ 54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インストールされていない場合、UNIX用インストールパッケージ(tar)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、Data Protectorクライアントのインストール、ページ 54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. コンピューター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用に選択したSCSIアドレスが、他のデバイスで使用されていないことをチェックしてください。

   サポート対象デバイスの詳細については、https://softwaresupport.hpe.com/を参照してください。
2. コンピューターの電源を投入し、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。

次に行う手順

インストール手順が完了し、AIXシステムにバックアップデバイスが正しく接続されたら、デバイスおよびメディアプールを構成する方法やその他のData Protector構成タスクについて、『*HPE Data Protectorヘルプ*』のキーワード「構成、バックアップデバイス」で表示される内容を確認してください。

Mac OS Xクライアントのインストール

Mac OS Xクライアントのインストールは、UNIX用インストールサーバーを使用したリモートインストール、またはUNIXインストールパッケージ(tar)を使用したローカルインストールが可能です。

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のバージョン、Data Protectorコンポーネントについては、『RAMおよびディスクスペースの要件、下』、『Mac OS Xクライアントのインストール、前のページ』および『Mac OS Xクライアントのインストール、前のページ』を参照してください。
- クライアントにおけるWindowsユーザーインターフェイスおよびリモートインストールに関する要件は以下のとおりです。
  - Microsoft Windows XP Professionalシステム(Service Pack 3がインストールされている必要があります)
  - Microsoft Windows Server 2003システム(Service Pack 2がインストールされている必要があります)
- 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およびインストールサーバーのインストール、ページ26を参照してください。
- ホスト名を解決するためのDNS逆引き参照は、Data Protectorセル内のすべてのData Protectorコンポーネントに必要です。

Windowsシステム上のData Protectorクライアントコンポーネントに関するRAMおよびディスクスペースの要件

Windowsシステム上の各種Data Protectorクライアントコンポーネントにおける RAMおよびディスクスペースの最小要件は、以下の表のとおりです。

RAMおよびディスクスペースの要件

クライアントシステムコンポーネント	合計RAM (MB) [1]	空きディスクスペース(MB) [2]
ユーザーインターフェイス	512 [3]	150 [4]

[1] 表中の数値はコンポーネントのみに関する要件です。オペレーティングシステム、ページングファイル、またはその他のアプリケーションに対するスペースの割り当ては含まれていません。
[2] 表中の数値はコンポーネントのみに関する要件です。オペレーティングシステム、ページングファイル、またはその他のアプリケーションに対するスペースの割り当ては含まれていません。
[3] GUIシステムのメモリ要件は、同時に表示する必要がある要素の数によって大幅に異なります。この留意事項については、実際に表示する際の最低限の状況(たとえば1つのディレクトリを展開するなど)を想定します。すべてのディレクトリを展開した状態で表示するのでなければ、クライアント上のディレクトリおよびファイルの名前の合計数について考慮する必要はありません。2MBのメモリがあれば1000の要素(ディレクトリまたはファイルの名前)を表示することができ、基本メモリとしては約50MBが必要であることが確認されています。したがって、最大数のファイル名を表示するためには、512 MBのRAMがあれば十分です。
[4] このディスクスペースに関しては、ページファイルだけは物理メモリの約3倍のサイズまで増加できるようにしなければならないことを留意しておいてください。

クライアントシステムコンポーネント	合計RAM (MB) [1]	空きディスクスペース(MB) [2]
Disk Agent	各64(128推奨)	各20
Media Agent		
統合コンポーネント		
英語版ドキュメント(ガイド、ヘルプ)	該当なし	100

表中の数値はコンポーネントのみに関する要件です。たとえば、「ディスクスペース」欄の数値には、オペレーティングシステム、ページングファイル、またはその他のアプリケーションに割り当てるディスクスペースのサイズは含まれていません。

推奨事項

- デフォルトのブロックサイズを増やす場合は、カーネルパラメーター`kern.sysv.shmmax`(共有メモリセグメントの最大サイズ)を32MBに設定することをお勧めします。

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ーフェイスを使って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については、Data Protectorクライアントのインストール、ページ 54を参照してください。

> **注:**
> リモートインストールの場合、Mac OS Xリモートインストールパッケージ(CoreおよびDisk Agent)に対応するためには、UNIXベースのインストールサーバー(LinuxまたはHP-UX)が必要です。

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インストールされていない場合、UNIXインストールパッケージ(tar)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、「Data Protectorクライアントのインストール、ページ 54」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。

[1] 表中の数値はコンポーネントのみに関する要件です。オペレーティングシステム、ページングファイル、またはその他のアプリケーションに対するスペースの割り当ては含まれていません。
[2] 表中の数値はコンポーネントのみに関する要件です。オペレーティングシステム、ページングファイル、またはその他のアプリケーションに対するスペースの割り当ては含まれていません。

HP OpenVMSクライアントのインストール

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、およびユーザーインターフェイス(コマンドラインインターフェイスのみ)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については、Data Protectorコンポーネント、ページ 57を参照してください。

サポート対象デバイス、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については、『HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照してください。

OpenVMS固有の詳細情報については、OpenVMSのデフォルトのヘルプドキュメントのディレクトリ(SYS$COMMON:[SYSHLP]DPA0800.RELEASE_NOTESなど)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。

- HPE 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コマンドを実行して、システムのTIMEZONE機能を設定します。
- 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。
- HP OpenVMSクライアントのインストールパッケージが格納されているData Protectorインストールパッケージ(zip/tar)にアクセスできること。
- ホスト名を解決するためのDNS逆引き参照は、Data Protectorセル内のすべてのData Protectorコンポーネントに必要です。

インストール手順

このインストール手順は、Data ProtectorのWindows用インストールパッケージ(zip)から実行できます。

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

1. PCSIインストールファイルがすでにある場合は、Data Protectorクライアントのインストール、ページ 54に進みます。PCSIインストールファイルを取得するには、OpenVMSサーバーでインストールパッケージを展開し、ターゲット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. 次のプロンプトにYESと応答して、キットのバージョンを確認します。

例

```
The following product has been selected: HPE AXPVMS DP A08.00-xx Layered
Product Do you want to continue? [YES]
```

4. インストール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ーフェイ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 A08.00-xx: HP OpenVMS IA64 Data Protector V8.00
COPYRIGHT HEWLETT-PACKARD COMPANY 2013
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 X08.00-xx: HP OpenVMS IA64 Data Protector V8.00 [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ージャおよびシャットダウンコマンドプロシージャは、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 これは、このノード上でData Protectorを起動するためのコマンドプロシージャです。
- SYS$STARTUP:OMNI$SYSTARTUP.COM OMNI$ROOTの論理名を定義するためのコマンドプロシージャです。このクライアントに必要な他の論理名も、このコマンドプロシージャに追加できます。
- SYS$STARTUP:OMNI$SHUTDOWN.COM これは、このノード上でData Protectorをシャットダウンするためのコマンドプロシージャです。
- OMNI$ROOT:[BIN]OMNI$STARTUP_INET.COM TCP/IP INETプロセスを起動するのに使用するコマンドプロシージャです。その後、Cell Managerにより送信されたコマンドが実行されます。
- OMNI$ROOT:[BIN]OMNI$CLI_SETUP.COM このコマンドプロシージャは、Data Protector CLIを呼び出すために必要な記号を定義します。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ーに対して、login.comプロシージャからこのコマンドプロシージャを実行してください。このプロシージャには、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. Data Protectorのグラフィカルユーザーインターフェイスを使用して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:**
> 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-A0800
> -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プロシージャは、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

```
$1$DGA100:[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。

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

> **注:**
> 暗黙的なバージョン番号はありません。バージョン番号は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とハードウェアドキュメント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&gt; IO CONNECT gcan/NOADAPTER/DRIVER=SYS$GcDRIVER
```

ここで、

- 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コントローラーのアダプターの文字)
- 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:**
> 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:**
> 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コントローラー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:**
> クラスター内のMSCPにより機能するテープデバイスで、HSxコントローラー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、『*HPE Data Protectorヘルプ*』のキーワード「SAN、デバイスの構成」で表示される内容を参照してください。

コマンドラインインターフェイス

OpenVMSでData Protectorのコマンドラインインターフェイスを使用する前に、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コマンドの説明については、『*HPE 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

『*HPE Data Protectorインテグレーションガイド*』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 9.00
```

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。

次に行う手順

その他の構成タスクに関する情報については、『*HPE Data Protectorヘルプ*』のキーワード「HP OpenVMS」で表示される内容を参照してください。

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ユーザーインターフェイスを使って、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

- インストール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、Data Protectorクライアントシステムのインストール、

ページ54および統合ソフトウェアのインストール、ページ55に示すとおりです。

- サポート対象プラットフォーム、Data Protectorコンポーネント、ディスクスペース要件については、https://softwaresupport.hpe.com/と「リモートインストール、前のページ」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。
- クリーンリモートインストールの場合、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ー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。
- ***Windows 2012の場合:*** Windows 2012システムにリモートでインストールするには、以下のいずれかの手順を実行します。
  インストールサーバーホスト上に、リモートホスト(`omniinetpasswd -inst_srv_user`)の管理者でもあるドメインユーザーを設定します。リモートインストールは、このアカウントの下で開始され、これ以上のユーザーの操作なしでリモートホストへの接続が確立されます。

  または

  リモートホスト上のファイアウォール内の以下のサービスをブロックします。
  - リモートサービス管理(RPC)
  - リモートサービス管理(RPC-EPMAP)

  または

  インストールサーバーホスト上のRPC/TCP (クライアント側)をオフにします。

  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control`

  `DWORD SCMApiConnectionParam = 0x80000000`

  `SCMApiConnectionParam`レジストリ値をマスク値の`0x80000000`と組み合わせます。

  > **注: 注記**: システムの再起動は不要です。

リモートインストールを実行するためのファイアウォールの構成

インストールサーバーを使用して新しいData Protectorクライアントをインストールするときに、インストールエージェントがリモートコンピューターで起動されます。その後、インストールサーバーはData Protectorセルポート(デフォルトで5555/5565)を経由してこのエージェントに接続します。ただし、Microsoft Firewallまたはサードパーティ製のファイアウォールソフトウェアがクライアントで実行されている場合は、接続を確立することができず、インストールが失敗します。この問題を解決するには、以下のいずれかの手順を実行します。

- 特定のポートを経由した接続を許可するようWindows Firewallを設定します。
- Microsoft Firewallの場合: omnircオプション`OB2FWPASSTHRU`がインストールサーバーで設定されている場合には、インストールエージェントが自動的にWindows Firewallに登録され、インストールが正常に続けられます。

推奨事項

- ***UNIXシステム:*** セキュリティ上の理由から、Data Protectorの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。SSHが構成されている場合、パスワードなしの認証が使用されるか、ユーザーに資格情報の提供が求められます。

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。Data Protectorクライアント のインストール、ページ 54を参 照 してください。

> **注：**
> 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。

- ***管 理 者 アカウント：*** UACが有 効 になっているリモート ホスト 上 で管 理 者 グループのメンバーであるローカルユーザーを使 用 するには、**リモート ホスト** 上 で以 下 のいずれかの手 順 を実 行 します。

  ユーザーアカウント制 御 (UAC)の無 効 化

  > **注： 注 記**： システムの再 起 動 が必 要 です。

  または

  以 下 のレジストリ値 の設 定：

  ```
  HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
  DWORD LocalAccountTokenFilterPolicy = 1
  ```

  > **注： 注 記**： システムの再 起 動 は不 要 です。

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 キーと秘 密 キーのペアを使 用 した仕 組 みによって保 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。
- インストールパッケージを暗 号 化 してからネット ワーク上 で転 送 します。

> **注：**
> 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 については、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ド キュメント 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 :**
> 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と秘密キーのペアを生成します。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Data Protectorクライアントのインストール、ページ 54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 :**
   > $HOME/.ssh は通常、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パラメーターの設定を変更します。

   a. ***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。

   b. ***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。

   この2つのファイルは、同期されている必要があります。

   > **注 :**
   > デフォルトのSSHプロトコルのバージョンは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

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.xml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およびSolarisシステムの場合：

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

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

   Linuxシステムの場合：

   /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オプションOB2_ENCRYPT_PVT_KEYを1に設定します。omnircオプションの詳細については、『*HPE Data Protectorトラブルシューティングガイド*』を参照してください。

   コマンド実行の失敗によりセキュアシェルのインストールを実行できない場合、警告が表示されます。この場合でも、インストールは標準のData Protectorリモートインストール方法を使用して続行されます。

次に行う手順

OpenSSHとkeychainのセットアップが終了したら、GUIを使用するか(Data Protectorクライアントのインストール、ページ 54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ーについては、『*HPE Data Protector Command Line Interface Reference*』を参照してください。

> **注：**
> 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

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

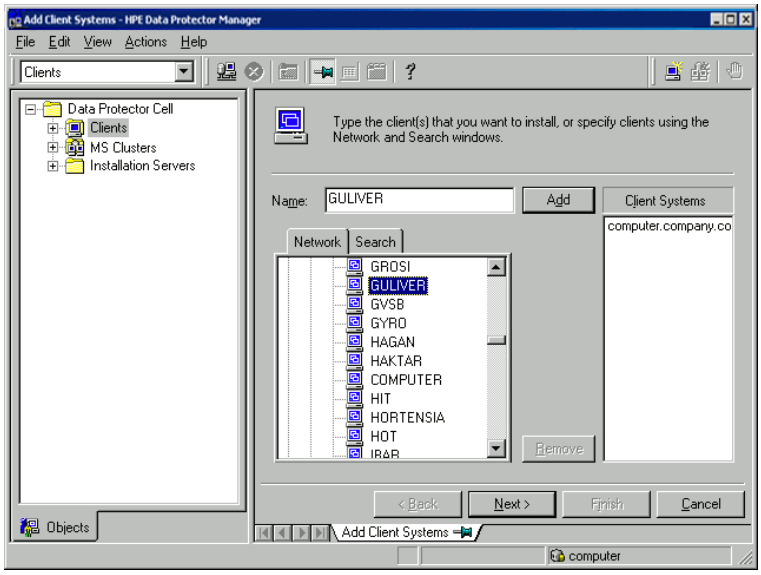
1. **[スタート]** > **[プログラム]** > [**HPE Data Protector**] > **[Data Protector Manager]**を順にクリックして、Data Protector GUIを起動します。

   > **注：**
   > Data Protectorのグラフィカルユーザーインターフェイスの詳細については、Data Protectorグラフィカルユーザーインターフェイス、ページ 24と『*HPE Data Protector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。

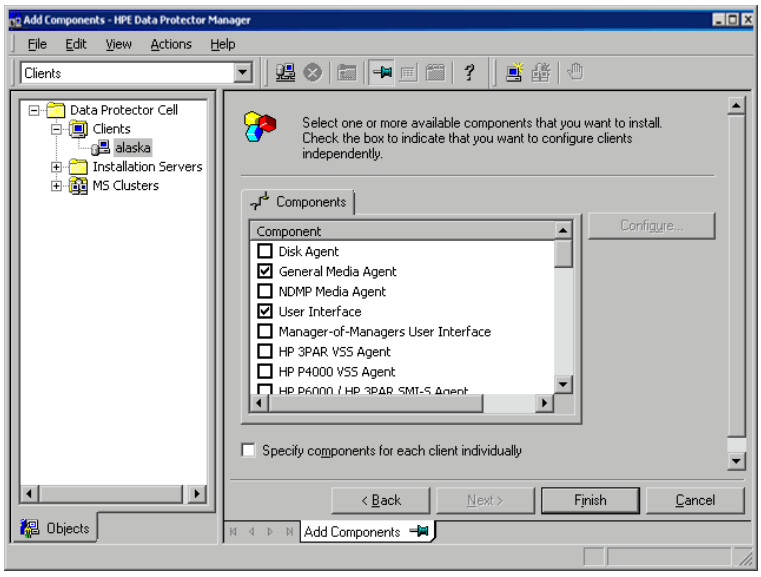
5. クライアントの名前を直接入力するか、Windows GUIを使用している場合はインストールするクライアントを検索することもできます(Data Protectorクライアントのインストール、ページ 54を参照してください)。**[次へ]**をクリックします。

   クライアントの選択



6. Data Protectorクライアントのインストール、ページ 54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、ページ 57を参照してください。

   コンポーネントの選択



7. インストール用のデフォルトアカウントとターゲットディレクトリ(Windows上のみ)を変更するには、**[オプション]**をクリックします。
8. 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、**[各クライアントのコンポーネントを個別に指定]**をクリックし、**[次へ]**をクリックします。クライアントごとにインストールするコンポーネントを個別に選択します。

9. **[次へ]**をクリックします。
10. **[完了]**をクリックしてインストールを開始します。
11. インストール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へのアクセスに必要なデータ(ユーザー名、パスワード。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:**
> 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については、『*HPE Data Protector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、インストールのトラブルシューティングとアップグレード、ページ 314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、ページ 234を参照してください。

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必要があります。

HPE Servicegardクライアント

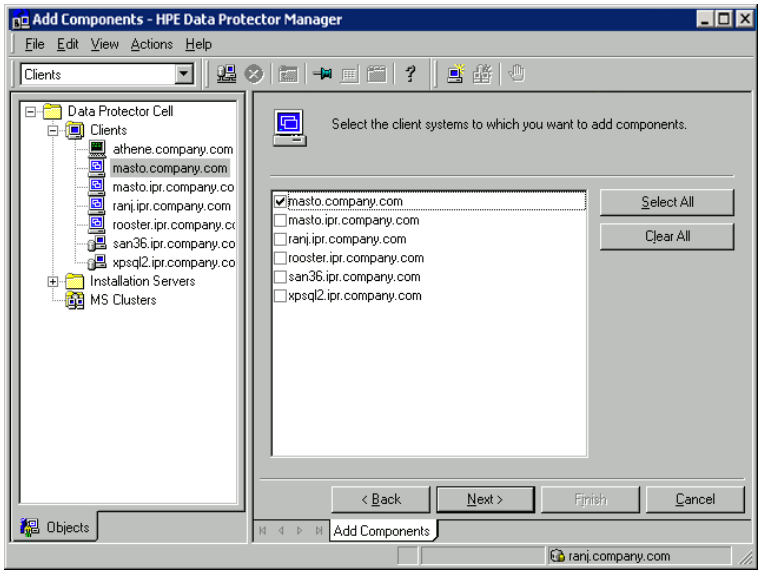
HPE Servicegardクラスター環境では、コンポーネントの追加先のノードがアクティブになっていることを確認してください。

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

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、**[コンポーネントの追加]**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. クライアントの選択、次の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

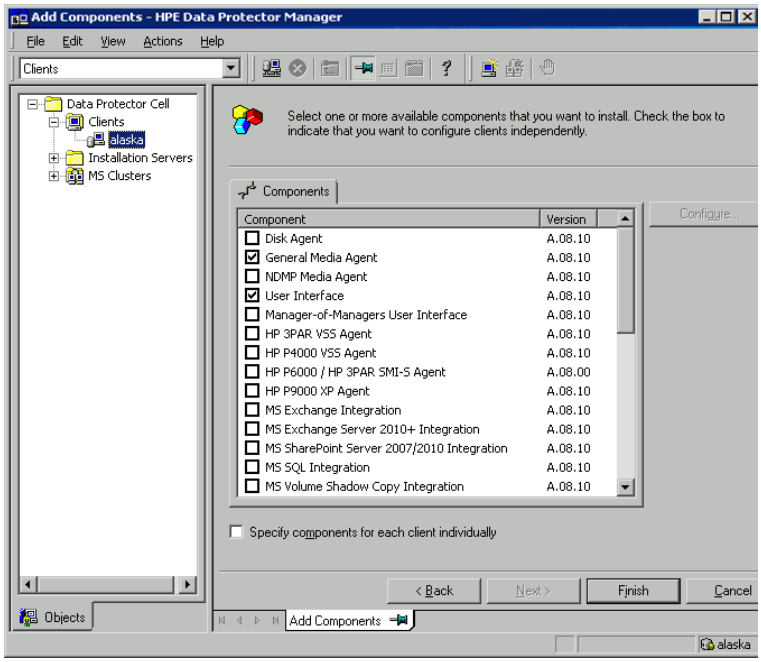
ます。**[次へ]**をクリックします。

クライアントの選択



5. Data Protectorクライアントのインストール、ページ 54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、ページ 57を参照してください。

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、**[各クライアントのコンポーネントを個別に指定]**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。

UNIXおよびMac OS Xシステムで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インストールされていない場 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 、UNIX用 インストールパッケージ(tar)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。

インストール手 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、ページ 57を参 照 してください。

> **注 :**
> Windows XP Home EditionおよびHP OpenVMSのクライアント は、ローカルでインストールできます。リモートインストールはサポートされていません。

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、プロセッサー、およびData Protectorコンポーネントについては、『HPE Data Protector製 品 案 内 、ソフト ウェアノート 、およびリファレンス』を参 照 してください。
- すべてのターゲットシステムで、`root`パーミッションが必 要 です。
- インストールには、POSIXシェル(`sh`)が必 要 です。

> **注 :**
> 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。

インストール手 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

1. ダウンロードしたData Protectorインストールパッケージ(tar)をHP-UXまたはLinuxシステムにコピーし、ファイルをローカルディレクトリに展 開 します。
2. `LOCAL_INSTALL`ディレクトリから、`omnisetup.sh`コマンド を実 行 してください。
   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]
   ```
   ここで、
   - *directory*は、インストールパッケージの展 開 先 です。省 略 すると、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。省略した場合は、クライアントがセルに自動インポートされません。

> **注 :**
> Cell Managerまたはインストールサーバー上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。

- *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。スペース文字は使用できません。`-install`パラメーターを指定しなければ、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 :**
  > クライアントのアップグレードでは、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モデル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、ページ 57を参照してください。

Data Protector component codes

コンポーネントコード	コンポーネント
`cc`	ユーザーインターフェイス
`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
`oracle8`	Oracle用統合ソフトウェア
`mysql`	MySQL統合
`postgresql`	PostgreSQL用統合ソフトウェア
`vepa`	仮想環境用統合ソフトウェア
`sybase`	Sybase用統合ソフトウェア
`sap`	SAP R/3用統合ソフトウェア

コンポーネントコード	コンポーネント
sapdb	SAP MaxDB用統合ソフトウェア
saphana	SAP HANA用統合ソフトウェア
db2	DB2用統合ソフトウェア
emc	EMC Symmetrix Agent
smisa	HPE P6000/HPE 3PAR SMI-S Agent
ssea	HPEP9000 XP Agent
emcvnx	EMC VNXストレージプロバイダー
emcvmax	EMC VMAXストレージプロバイダー
netapp	NetAppストレージプロバイダー
StoreOnceSoftware	StoreOnceソフトウェア重複排除
autodr	自動ディザスタリカバリ
docs	英語版ドキュメント(ガイド、ヘルプ)

例

次の例は、Disk Agent、General Media Agent、User Interface、およびInformix Integrationの各コンポーネントを、Cell Managercomputer.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 -installda,ma,cc,informix
```

3. インストール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

インストールパッケージをコンピューターにコピーして、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します。少なくともhpux/DP_DEPOTディレクトリとLOCAL_INSTALLディレクトリをコピーしてください。

> **注 :**
> 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システムの場 合 もHP-UXデポのコピーが必 要 です。

たとえば、インストールパッケージを/var/dp80にコピーする場 合 、ディレクトリは/var/dp10のサブディレクトリでなければなりません。

```
# pwd

/var/dp80

# 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]
```

例 :

```
./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。

次 に行う手 順

インストール時 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ーフェイスを使 用して、後 からインポートする必 要 があります。手 順 については、を参 照してください。追 加 の構 成 タスクの詳 細 については、『*HPE Data Protectorヘルプ*』を参 照してください。

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 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 のコンピューターに接 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：**
> StorageTekライブラリ内で使用するドライブおよびスロットの数によっては、特殊なライセンスが必要になります。詳細については、Data Protector Licensing、ページ 274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ライブラリの詳細については、https://softwaresupport.hpe.com/を参照してください。

システムにバックアップデバイスを物理的に接続する方法については、Data Protectorクライアントのインストール、ページ 54と、ADIC/GRAUまたはStorageTekライブラリ付属のドキュメントを参照してください。

サポート対象Windowsシステムにバックアップデバイスを物理的に接続する方法については、Data Protectorクライアントのインストール、ページ 54と、ADIC/GRAUまたはStorageTekライブラリ付属のドキュメントを参照してください。

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ー上の`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. Data Protector Media Agentがインストールされ、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各Data Protectorクライアント上で、`omnirc`ファイルを編集して以下のオプションを設定します。

`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。割り当てポリシーのタイプ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オプションを追加する必要があります。

```
OB2_ACIEJECTTOTAL = 0
```

> **注:**
> 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のドキュメント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ライブラリのドキュメント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。手順については、Data Protector Cell Managerおよびインストールサーバーのインストール、ページ 26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ライブラリのドキュメントを参照してください。
- Media Agentをインストールする前に、以下の情報を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`メニューから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。使用可能な挿入/取り出し領域のリストがテキストボックスに表示されます。

     > **注:**
     > 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については、Data Protectorクライアントのインストール、ページ 54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。例: `scsi4:0:1:0`。

  SCSIアドレスの詳細については、Data Protectorクライアントのインストール、ページ 54を参照してください。

インストール手順

インストール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ーフェイ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。Data Protectorクライアントのインストール、ページ 54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`の各ライブラリは*`Data_Protector_home`*`\bin`ディレクトリに含まれています。(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`および`Portmapper service`をDASクライアントにコピーします。なお、これらはADIC/GRAUライブラリとともに出荷されているDASクライアントソフトウェアの要件です。これらのファイルは、インストールメディアに収録されています。
     d. コントロールパネルの[`Administrative Tools, Services`]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. システムを再起動した後、`portmapper`と`rpc services`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ための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ための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。

Data Protectorのデフォルトの管 理 コマンドの場 所 から、`devbra -dev`コマンドを実 行 して、ライブラリドライブがシステムに正 しく接 続 されているかどうかをチェックします。

ライブラリドライブが正 しく接 続 されていると、ライブラリドライブおよび対 応 するデバイスファイルがリストに表 示 されます。

次 に行 う手 順

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、『*HPE Data Protectorヘルプ*』のキーワード「構 成 、*バックアップデバイス*」で表 示 される内 容 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。

StorageTekライブラリを使 用 するData Protectorクライアントの準 備 作 業

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。

- StorageTekライブラリが構 成 済 みで、実 行 されていること。StorageTekライブラリのドキュメントを参 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およびインストールサーバーのインストール、ページ 26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が稼動しているホストの*hostname*。
- Data Protectorで使用するACSドライブIDのリスト。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&gt; 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&gt; 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については、Data Protectorクライアントのインストール、ページ 54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。例: `scsi4:0:1:0`。

  SCSIアドレスの詳細については、Data Protectorクライアントのインストール、ページ 54を参照してください。

- Data Protectorで使用するドライブが`online`状態になっていることを確認します。ドライブが`online`状態になっていない場合は、ACSLSホスト上で次のコマンドを実行して状態を切り替えます。`vary drive drive_id online`
- Data Protectorに使用するCAPが`online`状態になっており、`manual`が手動モードになっていることを確認します。

  CAPが`online`状態になっていない場合は、次のコマンドを実行して状態を切り替えます。

  ```
  vary cap cap_id online
  ```

  CAPが`manual`操作モードになっていない場合は、次のコマンドを実行してモードを切り替えます。

  ```
  set cap manual cap_id
  ```

StorageTekライブラリ用 のMedia Agentのインストール

StorageTekライブラリ用 のMedia Agentをインストールするには

1. Data Protectorグラフィカルユーザーインターフェイスと UNIXシステム用 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。Data Protectorクライアント のインストール、ページ 54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。

   Windowsシステムの場 合 :

   LibAttachサービスをインストールします。詳 細については、ACSのド キュメントを参 照してください。LibAttachサービスの構 成 時 には、必 ず適 切 なACSLSホスト名 を入 力してください。構 成 が正 常 に完 了 すると、LibAttachサービスが自 動 的 に開 始 されます。それ以 降 は、システムを再 起 動 すると、必 ずこのサービスが自 動 的 に開 始 されます。

   HP-UXシステム、Solarisシステム、Linuxシステムの場 合 :

   次 のコマンドを実 行します。

   ```
   /opt/omni/acs/ssi.sh start ACS_LS_Hostname
   ```

   AIXシステムの場 合 :

   次 のコマンドを実 行します。

   ```
   /usr/omni/acs/ssi.sh start ACS_LS_Hostname
   ```

   > **注 :**
   > LibAttachサービスをインストールし終 えたら、libattach\binディレクトリがシステムパスに自 動 的 に追 加 されていることを確 認します。追 加 されていない場 合 は、手 動 で追 加 してください。

   LibAttachサービスの詳 細 は、StorageTekライブラリに付 属 のド キュメントを参 照してください。
3. Data Protectorのデフォルト の管 理 コマンド の場 所 から、devbra -devコマンドを実 行して、ライブラリドライブがシステムに正 しく接 続 されているかどうかをチェックします。

   ライブラリド ライブが正 しく接 続 されていると、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アドレスがリストに表 示 されます。

次 に行う手 順

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、『*HPE Data Protectorヘルプ*』のキーワード「構 成 、*バックアップデバイス*」で表 示 される内 容 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。

第4章: 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 ZDB用統合ソフトウェアは、HPE 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システム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、Microsoft 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、HPE P6000 EVAディスクアレイファミリまたはHPE StoreServ StorageによるZDBおよびIRには`HPE P6000 / HPE 3PAR 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、プロセッサー、およびData Protectorコンポーネントについては、『HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照してください。
- 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(VSS用統合ソフトウェアを除く)。ライセンスの詳細はData Protectorの製品構成とライセンス、ページ 301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。

  その手順については、Data Protector Cell Managerおよびインストールサーバーのインストール、ページ 26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、ページ 57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です。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Microsoft 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。
  - ファイルシステムまたはディスクイメージのゼロダウンタイムバックアップを実行する。

  - 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、`User Interface`コンポーネントが必要です。
- 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です。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。

統合ソフトウェアクライアントのインストールは、Windows用またはUNIX用インストールサーバーを使用したリモートインストール、WindowsまたはUNIX用インストールパッケージ(zip/tar)を使用したローカルインストールが可能です。

個々の統合クライアントに関するその他の詳細については、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、ページ 115
- Microsoft SQL Serverクライアント、ページ 122
- Microsoft SharePoint Serverクライアント、ページ 122
- Microsoftボリュームシャドウコピーサービスクライアント、ページ 126
- Sybase Serverクライアント、ページ 127
- Informix Serverクライアント、ページ 127
- SAP R/3クライアント、ページ 128
- SAP MaxDBクライアント、ページ 128
- SAP HANAアプライアンスクライアント、ページ 128
- Oracle Serverクライアント、ページ 129
- MySQLクライアント、ページ 129
- PostgreSQLクライアント、ページ 130
- IBM DB2 UDBクライアント、ページ 130
- Lotus Notes/Domino Serverクライアント、ページ 130
- VMwareクライアント、ページ 131
- Microsoft Hyper-Vクライアント、ページ 139
- NDMP Serverクライアント、ページ 140
- HPE P4000 SANソリューション clients、ページ 140
- HPE P6000 EVAディスクアレイファミリ クライアント、ページ 141
- HPE P9000 XPディスクアレイファミリ クライアント、ページ 147
- HPE 3PAR StoreServ Storage clients、ページ 153
- EMC Symmetrixクライアント、ページ 153
- non–HPE Storage Arrays、ページ 157

統合クライアントのインストールが完了したら、各クライアントの適切な環境変数にコマンドの場所を追加して、どのディレクトリからでもHPEコマンドを実行できるようにすることをお勧めします。Data Protectorドキュメントの手順は、変数値が追加されていることを前提とします。コマンドの場所については、『*HPE Data Protector Command Line Interface Reference*』の`omniintro`のリファレンスページ、および`omniintro`のmanページを参照してください。

インストール後にData Protector統合クライアントを構成する場合は、『*HPE Data Protectorインテグレーションガイド*』、『*HPE Data Protector Zero Downtime Backup Administrator's Guide*』、または『*HPE Data Protector Zero Downtime Backup Integration Guide*』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ーフェイ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の詳細については、リモートインストール、ページ 94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。

ローカルインストール

ユーザー環境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用またはUNIX用のインストールパッケージ(zip/tar)でローカルインストールを行う必要があります。

インストールする際に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。「ローカルにインストールされたクライアントのインポート、ページ 66」を参照してください。

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、インストールパッケージ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`HPE P6000 / HPE 3PAR 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。

インストール手順は、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。

- HPE ServiceguardへのData Protectorのインストール、ページ 164
- Symantec Veritas Cluster ServerへのData Protectorのインストール、ページ 175
- Microsoft Cluster ServerへのData Protectorのインストール、ページ 178
- Microsoft Hyper-VクラスターでのData Protectorのインストール、ページ 189
- Data ProtectorのIBM HACMPクラスターへのインストール、ページ 189

クラスタリングの詳細については、『*HPE Data Protectorヘルプ*』のキーワード「クラスター、HPE Serviceguard」で表示される内容、および『HPE Data Protectorコンセプトガイド』を参照してください。

次に行う手順

インストールの完了後に統合ソフトウェアを構成する方法は、『*HPE Data Protectorインテグレーションガイド*』を参照してください。

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。次のソリューションから選択することができます。

- Data Protector Microsoft Exchange Server 2007 integration、下
- Data Protector Microsoft Exchange Server 2010 integration、ページ 117
- Data Protector Microsoft Exchange Server Single Mailbox用統合ソフトウェア、ページ 118
- 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、ページ 118
- Data Protector Microsoft Exchange Server用 Granular Recovery Extension、ページ 119

Data Protector Microsoft Exchange Server 2007 integration

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 Integration`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用統合ソフトウェアコンポーネントの一部としてインストールされます。

前提条件

- 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の基本的なアーキテクチャーに関する知識が必要です。Microsoft Exchange Serverについては、*Microsoft Exchange Serverのオンラインヘルプ*を参照してください。
- Data ProtectorのMicrosoft Exchange Server用統合ソフトウェアを使用するには、適切なData Protectorのオンライン拡張使用ライセンス(LTU)が必要です。
- ディスクアレイ上でMicrosoft Exchange Server用統合ソフトウェアを使用する場合は、Exchange Serverのサービス(インフォメーションストア、キーマネージメントサービス(省略可能)、およびサイト複製サービス(省略可能))をアプリケーションシステムのディスクアレイのソースボリュームにインストールします。

手順

1. Exchange Serverシステムで、システムパスに*Exchange_Server_home*`\bin`ディレクトリを追加します。

a. Windowsデスクトップで、**[マイ コンピューター]**を右クリックし、**[プロパティ]**をクリックします。
b. [システムのプロパティ]ウィンドウで、**[詳細設定]**をクリックし、**[環境変数]**をクリックします。
c. [システム環境変数]グループボックスの変数の一覧で、**[Path]**エントリを選択し、**[編集]**をクリックします。
d. [システム変数の編集]ウィンドウの[変数値]テキストボックスで、*Exchange_Server_home*\bin ディレクトリを追加します。**[OK]**をクリックします。

> **重要:**
> Exchange Serverがクラスター対応の場合は、すべてのクラスターノードでシステムパスにこのディレクトリを追加します。

2. Microsoft Exchange Server用統合ソフトウェアをExchange Serverシステム(Data Protectorクライアント)にインストールします。インストールパッケージを使ってローカルにインストールするか、Data Protector GUIを使ってリモートからインストールしてください。

> **重要:**
> Exchange Serverがクラスター対応の場合は、ローカルでインストールパッケージからすべてのクラスターノードにこのソフトウェアコンポーネントをインストールします。

既にExchange ServerシステムにData Protectorがインストールされている場合、または、まだData ProtectorがインストールされていないExchange Serverシステムにリモートインストールを実行する場合は、Data Protector GUIを使って必要なソフトウェアコンポーネントをインストールします。

まだExchange ServerシステムにData Protectorがインストールされておらず、ローカルインストールを実行する場合は、Data Protectorセットアップウィザードを起動します。セットアップウィザードの指示に従ってインストールを実行します。インストール処理はData Protector Cell Managerをインストールする場合と、Data Protectorクライアントをインストールする場合とで異なります。

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する必要があります。

- MS Exchange用統合ソフトウェア
- General Media Agent (Exchange Serverクライアントシステムに接続しているデバイスがある場合)

以下のコンポーネントもインストールすることをお勧めします。

- ユーザーインターフェイス
- Disk Agent (テスト用にExchange Serverクライアントシステムのファイルシステムバックアップを実行する場合)

3. Exchange Serverがクラスター対応の場合は、すべてのクラスターノードでData Protector Inetサービスにクラスターサービスのアカウントを割り当てます。
a. Windowsデスクトップで、**[マイ コンピューター]**を右クリックし、**[管理]**をクリックします。
b. [コンピューターの管理]ウィンドウで、**[サービスとアプリケーション]**を展開し、**[サービス]**をクリックします。
c. サービスの一覧で、**[Data Protector Inet]**を選択して右クリックし、**[プロパティ]**をクリックします。[Data Protector Inetのプロパティ]ウィンドウが表示されます。
d. [ログオン]プロパティページで、**[アカウント]**をクリックします。
e. [アカウント]テキストボックスに、クラスターサービスアカウントの名前を入力します。必要に応じて、**[参照]**をクリックして、目的の名前を探すこともできます。

f. [パスワード]と[パスワードの確認]のテキストボックスに、クラスターサービスアカウントのパスワードを入力します。
g. **[OK]**をクリックします。
h. [ファイル]メニューの**[終了]**をクリックします。

Data ProtectorのMicrosoft Exchange Server用統合ソフトウェアのインストールの確認

- 環境変数Pathに、*Exchange_Server_home*\binディレクトリも設定されているかどうかを確認します。設定されていない場合は、Path変数にこのディレクトリの絶対パスを追加します。
- Data ProtectorのクライアントシステムにCell Manager名が正しく設定されているかどうかを確認します。以下の手順を実行します。
  1. 次のレジストリキーを探します。

     HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\Site
  2. レジストリキーの名前がCellServer、データが*Cell_Manager_host_name*になっているかどうかを確認します。なっていない場合は、このクライアントにData Protectorを再インストールします。

Microsoft Exchange Serverの確認

- 以下のMicrosoft Exchange Serverのサービスが稼動しているかどうかを確認します。
  - Microsoft Exchange System Attendant (MSExchangeSA)
  - Microsoft Exchangeインフォメーションストア(MSExchangeIS)

  稼動していない場合は、Exchange Serverを再起動します。
- Data Protectorの代わりに、Windows用バックアップユーティリティ(Microsoft Windowsバックアップ)を使って、Exchange Serverインフォメーションストアのバックアップと復元を実行してみます。エラーが発生した場合は、Exchange Serverのインストールと構成を確認して問題を特定します。

Data Protector Microsoft Exchange Server 2010 integration

ここでは、Microsoft Exchange Server環境が正しく動作していることが前提となります。

Microsoft Exchange Server 2010データベースまたはMicrosoft Exchange Server 2013データベースをバックアップできるようにするには、すべてのMicrosoft Exchange Serverシステムに次のData Protectorコンポーネントをインストールします。

- MS Exchange Server 2010+ Integration
- MS Volume Shadow Copy Integration
- 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:**
> 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 Volume Shadow Copy Integration`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、『*HPE Data Protectorヘルプ*』のキーワード「インポート、クライアントシステム」で表示される内容を参照してください。

> **注:**
> - 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+ Integration`コンポーネントのインストール時に、自動的に`MS Volume Shadow Copy Integration`コンポーネントがインストールされます。`MS Volume Shadow Copy Integration`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。
> - システムから`MS Exchange Server 2010+ Integration`コンポーネントを削除しても、`MS Volume Shadow Copy Integration`コンポーネントは自動的に削除されません。また、`MS Exchange Server 2010+ Integration`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は`MS Volume Shadow Copy Integration`コンポーネントを削除できません。

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ーとパブリックフォルダー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 Integration`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ウェブサイト 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、ページ 126を参照)。

Data Protector Microsoft Exchange Server用 Granular Recovery Extension

Microsoft Exchange Serverメールボックス項目を復元できるようにするには、Data Protector拡張を使用します。Microsoft Exchange Server環境の構成に応じて、対応するData Protectorコンポーネントを以下のシステムにインストールしてください。

- 単一のMicrosoft Exchange Serverシステム:本システム
- 複数のMicrosoft Exchange Serverシステム:メールボックスサーバーロールが構成されている各Exchange Serverシステム
- Microsoft Exchange Server Database Availability Group (DAG)環境:DAG内の任意のExchange Serverシステム

前提条件

- 選択したMicrosoft Exchange Serverシステムに次のコンポーネントをインストールします。
  - Data Protector`MS Exchange Server 2010+ Integration`コンポーネント
  - Data Protector`User Interface`コンポーネント
  - Data Protector以外の必要なコンポーネントすべて
- 選択したMicrosoft Exchange Serverシステム上のTCP/IPポート60000 (デフォルト)を空きポートにしておきます。

Microsoft Exchange Serverソフトウェア

以下をインストールします。

- Microsoft Exchange Server

  Microsoft Exchange Server環境がインストール済みで、正しく構成されていることを確認してください。

  サポートされているバージョン、プラットフォーム、デバイスなどの情報については、最新のサポート一覧(https://softwaresupport.hpe.com/manuals)を参照してください。

  Microsoft Exchange Serverのインストール、構成、および使用方法については、Microsoft Exchange Serverのドキュメントを参照してください。
- Microsoft管理コンソール(MMC) 3.0以降
- .NET Framework 3.5.1以降
- Internet Information Services (IIS) 6.0以降

Data Protector ソフトウェア

以下のData Protectorコンポーネントをインストールします。

- Data Protector`User Interface`コンポーネント
- すべてのMicrosoft Exchange Serverシステム上のData Protector`MS Exchange Server 2010+ Integration`コンポーネント

Data Protectorバックアップソリューションが『*HPE Data Protectorインストールガイド*』および『*HPE Data Protectorインテグレーションガイド*』の説明に従ってインストール済みで、構成されていることを確認してください。

他のData Protector以外のソフトウェアとサービス

- Windows PowerShell 1.0以降(Windows Management Framework Coreパッケージ)をインストールします。
- PowerShellの英語以外の言語はサポートされていません(Windows OSは英語版を使用する必要があります)。
- Granular Recovery Webサービス用にTCP/IPポート60000 (デフォルト)を空きポートにしておきます。
- 新しいポートを許可するようにファイアウォールを構成します。

サポートされる環境

次のような異なるMicrosoft Exchange Server環境でこの拡張機能をMicrosoft Exchange Serverと統合できます。

- スタンドアロンMicrosoft Exchange Serverシステム(スタンドアロン環境)
- 複数のMicrosoft Exchangeメールボックスサーバーシステム(複数サーバーシステム)
- Microsoft Exchange Server Database Availability Group環境(DAG環境)

Microsoft Exchange Server環境の構成に応じて、以下のように拡張機能をインストールします。

スタンドアロン環境

すべてのMicrosoft Exchange Serverサービスとデータが1台のMicrosoft Exchangeメールボックスサーバーにインストールされるので、小規模な環境に適しています。`MS Exchange Granular Recovery Extension`コンポーネントをExchangeメールボックスサーバーシステムにインストールします。

複数Exchange Serverシステム環境

環境に複数のMicrosoft Exchange Serverデータベースが含まれている場合です。`MS Exchange Granular Recovery Extension`コンポーネントを単一アイテムを復元するExchangeメールボックスサーバーシステムにインストールします。

DAG環境

環境には最大16のMicrosoft Exchangeメールボックスサーバーシステムを含めることができます。`MS Exchange Granular Recovery Extension`コンポーネントを任意のMicrosoft Exchangeメールボックスロールシステムノードにインストールします。コンポーネントがインストールされたら、Granular Recovery Extensionのグラフィカルユーザーインターフェイス(GUI)にDAG環境内のすべてのメールボックスサーバーノードのすべてのメールボックスデータベースオブジェクトが表示されます。拡張機能は、DAG環境の動的な動作を自動的に想定します。

CCR環境

`MS Exchange 2010 Granular Recovery Extension`コンポーネントをメールボックスサーバーノードにインストールします。

LCR環境

`MS Exchange 2010 Granular Recovery Extension`コンポーネントを、アクティブおよびパッシブのメールボックスデータベースが置かれているサーバーにインストールします。

Microsoft Exchange Serverの概念の詳細については、Microsoft Exchange Serverのドキュメントを参照してください。

拡張機能のインストール

Microsoft Exchange Server用HPEData ProtectorGranular Recovery Extensionは、Data Protectorコンポーネントとして提供されます。`MS Exchange Granular Recovery Extension`コンポーネントには、Granular Recovery Extensionグラフィカルユーザーインターフェイス、コマンドラインオプション、Webサービスコンポーネント、および状況依存型(F1)ヘルプが含まれています。すべてのコンテンツがいっしょにインストールされます。

> **注:**
> 拡張機能は、Microsoft Exchange組織のMicrosoft Exchange Serverメールボックスロールシステムにのみインストールする必要があります。これらのシステムには、Microsoft Exchange Serverメールボックスデータベースと、完全なMicrosoft Exchange Serverデータベースとメールボックスアイテムを復元するために必要なリカバリデータベース(RDB)などの復元テクノロジが含まれています。

手順

Data Protectorグラフィカルユーザーインターフェイス(GUI)を使用して拡張機能をインストールします。

> **重要:**
> Microsoft Exchange Serverメールボックスロールシステム上でWindowsローカルユーザーアカウントSYSTEMまたはWindowsドメインユーザーアカウントの管理権限を持っていることを確認してください。レジストリエントリの作成および`Program Files`ディレクトリへのファイルやフォルダーのインストールを許可されている必要があります。

1. 以下の手順を実行して、リモートインストールを実行します。
   - クライアントの追加
   - クライアントのインポート
2. `MS Exchange Granular Recovery Extension`コンポーネントをData Protectorクライアントシステムに追加します。

Data Protectorのインストールの詳細については、『Data Protector』の「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のインポート」、「HPE Data Protectorインストールガイドコンポーネントの追加」を参照してください。

拡張機能の削除

以下のいずれかの操作を行います。

- Data Protector GUIを使用して、拡張コンポーネントがインストールされたクライアントをリモートから削除します。

  Data Protectorクライアントの削除の詳細については、『*HPE Data Protectorヘルプ*』のキーワード「アンインストール、クライアント」で表示される内容を参照してください。
- `MS Exchange Granular Recovery Extension`コンポーネントを手動で削除します。

Data Protectorソフトウェアコンポーネントの削除の詳細については、『*HPE Data Protectorヘルプ*』のキーワード「アンインストール、Data Protectorソフトウェア」で表示される内容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 Integration`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。次のソリューションから選択することができます。

- Data Protector Microsoft SharePoint Server 2007/2010/2013 integration、下
- Data Protector Microsoft SharePoint Server VSSベースソリューション、下
- 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、次のページ
- Data Protector Microsoft SharePoint Server用Granular Recovery Extension、次のページ

Data Protector Microsoft SharePoint Server 2007/2010/2013 integration

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 2007/2010/2013 Integration` – Microsoft SharePoint Serverシステム上(Microsoft SQL Serverシステムは除外されます)
- `MS SQL Integration` – Microsoft SQL Serverシステム

> **注:**
> システムにMicrosoft SQL ServerとMicrosoft SharePoint Serverの両方がインストールされている場合、システムに両方のData Protectorコンポーネントをインストールします。

Data Protector Microsoft SharePoint Server VSSベースソリューション

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 Volume Shadow Copy Integration – 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 Services Help Search
  - Office SharePoint Server Search

  Microsoft SharePoint Server 2010:

  - SharePoint Foundation Database
  - SharePoint Foundation Help Search
  - SharePoint Server Search

  Microsoft SharePoint Server 2013:

  - SharePoint Foundation Database
  - SharePoint Server Search

- Data ProtectorUser Interfaceコンポーネント - Data ProtectorMS Volume Shadow Copy Integrationコンポーネントがインストールされたシステムの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、ページ 126を参照)。

Data Protector Microsoft SharePoint Server用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:**
> - Granular Recovery Extensionをインストールできるのは、Microsoft SharePoint Serverがインストールされているシステムのみです。
> - 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。

前提条件

- **Microsoftパッケージ:**

  以下のWindows Management Framework Coreパッケージをインストールします。
  - Microsoft PowerShell 2.0以降

- **Microsoft SQL Serverパッケージ:**

  Microsoft SQL Server 2005またはMicrosoft SQL Server 2008用の以下のパッケージをインストールします。
  - Microsoft SQL Server Native Client
  - Microsoft Core XML Services (MSXML) 6.0
  - Microsoft SQL Server 2008管理オブジェクトコレクション

  Microsoft SQL Server 2012用の以下のパッケージをインストールします。
  - Microsoft SQL Server Native Client
  - Microsoft Core XML Services (MSXML) 6.0以降
  - Microsoft SQL Server 2012管理オブジェクトコレクション

  上記のパッケージは、以下のサービスの少なくとも1つが有効になっているMicrosoft SharePoint Serverシステムすべてにインストールされている必要があります。
  - Central Administration
  - Windows SharePoint Services Web Application (Microsoft Office SharePoint Server 2007)
  - Microsoft SharePoint Foundation Web application (Microsoft SharePoint Server 2010/2013)

  これらのパッケージは以下のWebサイト(http://www.microsoft.com/downloads/en/default.aspx)からダウンロードできます。

  Microsoft SQL Server 2008用Feature Packまたは**Microsoft SQL Server 2012用Feature Pack**を検索してください。

- **Data Protector コンポーネント:**

  Data Protectorバックアップソリューションは、以下の説明に従ってインストールおよび構成する必要があります。

- *HPE Data Protectorインストールガイド*
- 該当する章 *HPE Data Protectorインテグレーションガイド*
- *HPE Data Protector Zero Downtime Backup Integration Guide*
- *HPE Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*

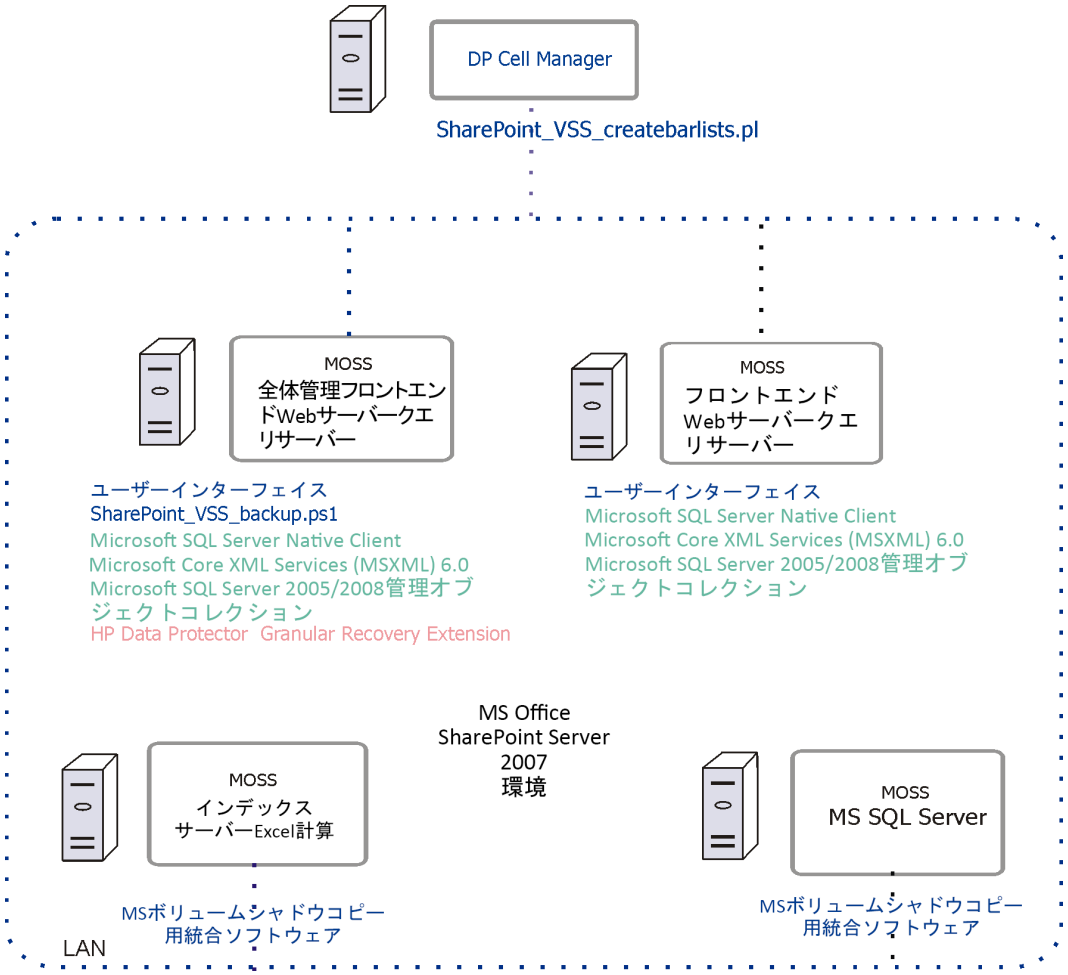
このほか、以下のサービスの少なくとも1つが有効になっているMicrosoft SharePoint Serverシステムすべてに、Data Protector`User Interface`コンポーネントがインストールされていることを確認してください。

- Central Administration
- Windows SharePoint Services Web Application (Microsoft Office SharePoint Server 2007)
- Microsoft SharePoint Foundation Web application (Microsoft SharePoint Server 2010/2013)

GRE環境

HPE Data Protector Microsoft SharePoint Server VSSベースソリューションを使用する中規模ファームのインストール(例)、次のページでは、HPE Data Protectorコンポーネントが青色、Microsoft SQL Serverのインストールパッケージが緑色、HPE Data Protector Granular Recovery Extensionが赤色で示されています。

HPE Data Protector Microsoft SharePoint Server VSSベースソリューションを使用する中規模ファームのインストール(例)



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 Volume Shadow Copy Integration.
- ディスクアレイを(ハードウェアプロバイダーとともに)使用する場合は、適切なディスクアレイエージェント: HPE P4000 VSS Agent、HPE P6000 / HPE 3PAR SMI-S Agent、HPEP9000 XP Agent、またはHPE 3PAR VSS 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オプションが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。

詳細については、『*HPE Data Protector Zero Downtime Backup Integration Guide*』を参照してください。

Sybase Server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 Integration - 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。Data Protector
  - 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 Integration — 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。Data Protector
  - 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クラスター

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 Integration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:**
> 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 Integration`
- `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 MaxDB Integration` - 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データベースのファイルシステムバックアップを実行する場合

SAP HANAアプライアンスクライアント

Data ProtectorをSAP HANAアプライアンス(SAP HANA)と統合するには、次のData Protectorソフトウェアコンポーネントを SAP HANAシステムにインストールします。

- SAP HANA Integration

  このコンポーネントをインストールすると、完全なSAP HANAデータベースおよびSAP HANA REDOログの統合バックアップが可能になります。

- Disk Agent

  このコンポーネントをインストールすると、Data Protectorファイルシステムのバックアップ機能を使用したSAP HANA構成ファイルの非統合バックアップが可能になります。障害が発生した場合、SAP HANA構成ファイルのバックアップイメージがあれば、変更内容をより簡単に特定および復元できるようになります。

SAP HANAの分散環境では、このような環境を構成している各SAP HANAシステムに上記のコンポーネントをインストールします。

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 Integration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、『*HPE Data Protectorインテグレーションガイド*』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 9.08
```

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。

MySQLクライアント

Data ProtectorとMySQLデータベース管理システムを統合し、MySQLのインスタンスとデータをバックアップできるようにするには、以下のData Protectorコンポーネントを MySQLホストにインストールします。

- MySQL Integration

  このコンポーネントは、MySQLデータベースのバックアップと復元の統合化を可能にします。

- Disk Agent

  このコンポーネントは、MySQLバイナリログをバックアップし、MySQLデータベースの復旧の前提条件としてバイナリログを復元できるようにします。また、MySQLがインストールされたData Protectorクライアントに関する問題を解決する目的で、MySQLデータの非統合化バックアップ用に使用することもできます。

PostgreSQLクライアント

Data ProtectorをPostgreSQLデータベースサーバーシステムと統合し、PostgreSQLインスタンスおよびデータをバックアップするには、以下のData Protectorコンポーネントをインストールします。

- PostgreSQL Integration
  このコンポーネントにより、PostgreSQLデータベースの統合バックアップおよび復元が可能となります。

IBM DB2 UDB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 Integration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 Integration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:**
> rootとしてログオンした後、インストールを実行します。

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 Integration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 files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

Lotus Integration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。

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、使用する復元とバックアップソリューションによって異なります。

このセクションでは、次の項目について説明します。

- GRE環境
- Data Protector GREのインストール
- Data Protector GREのアンインストール

Data Protector GRE for VMware vSphere

HPE Data Protector Granular Recovery Extensionは、Data Protector仮想環境統合ソフトウェアを使用してデータを復元します。この拡張は、復旧ソリューション専用です。マウントプロキシおよびvCenter Serverを含むGRE環境は、GREプラグインをインストールするために、特定の要件を満たす必要があります。

GREプラグインには、拡張GRE Webプラグインのユーザーインターフェイスを使用してアクセスすることができます。

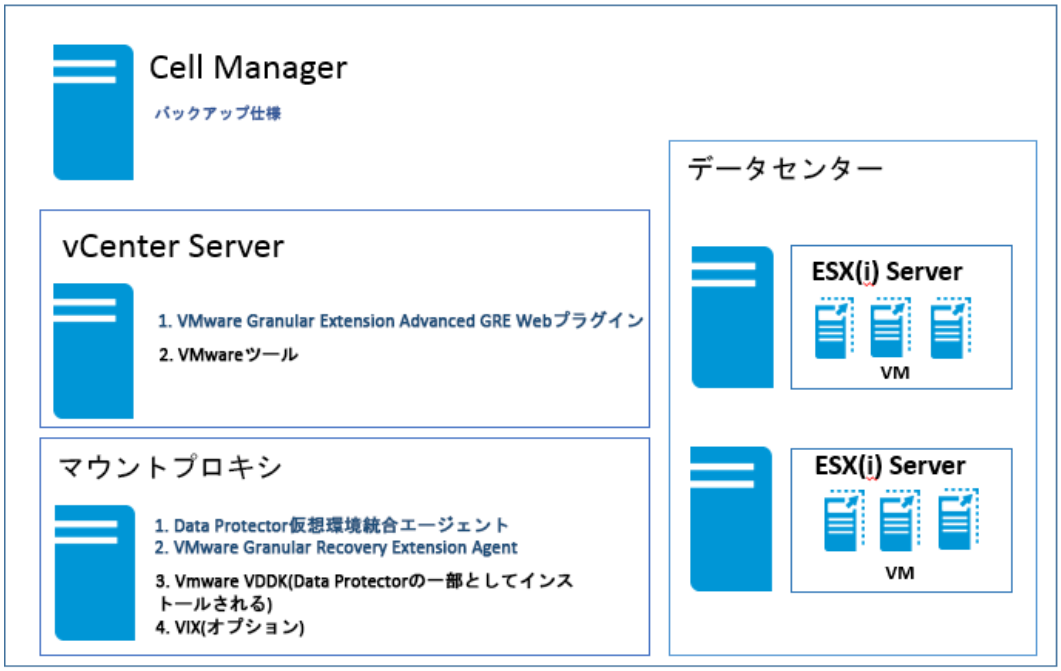
このセクションでは、この環境を作成するために必要な情報について説明します。

GRE環境

次の図では

- HPE Data Protectorコンポーネントは青色で示されています。
- VMwareコンポーネントは黒色で示されています。

HPE Data ProtectorGranular Recovery Extensionのインストール



マウントプロキシシステム

VMware vSphere用Data Protector Granular Recovery Extensionは、VMware vCenter Serverシステム上に、元の場所と復元先の場所の間で一時的に復元または復旧する場所としてマウントプロキシシステムを必要とします。サポート対象のシステムであれば、仮想マシンも含め、どのシステムもマウントプロキシシステムとして使用できます。

仮想マシンディスクはすぐにはマウントされません。マウントセッションは、VMware vCenterユーザーがvCenter環境で統合された拡張を使用してファイルの参照を始めたときに開始されます。

マウントプロキシシステムには、データを復元するための十分なディスクスペースが必要です。追加のディスクまたは別のマウントプロキシシステムを接続することで必要に応じてディスクスペースを調整することもできます。

> **注：**
> マウントプロキシシステムとして専用のシステムを構成することをお勧めします。

システム要件

マウントプロキシシステムは次のシステム要件を満たす必要があります。

- **Windowsシステムの場合：**
  (オプション)ファイルの復元にVIX APIを使用する場合は、次のユーティリティがインストールされていることを確認してください。VIXは、ネットワーク共有を利用できない場合のフォールバックオプションとして使用されます。
  - VMware VIX API 1.14
- **Linuxシステムの場合：**

次のオペレーティングシステムコンポーネントとユーティリティがインストールされていること確認してください。

- FUSE 2.7.3以降*
- cifs-utilsパッケージ(LinuxマウントプロキシシステムにWindows仮想マシンディスクをマウントするために使用します)
- ntfs-3gパッケージ(LinuxマウントプロキシシステムにWindows仮想マシンディスクをマウントするために使用します)
- NFSサービス
- VMware VIX API 1.14(オプション: ファイルを復元するため、ネットワーク共有を利用できない場合のフォールバックオプションとして使用されます)
- kpartxは、LVMパーティションが作成されたディスクに必要です。
- Sambaサーバー。Data Protectorは復旧中に共有を作成するためにSambaサーバーを使用します。Samba共有に読み取り書き込みのパーミッションがあることを確認してください。Security-Enhanced Linux (SELinux)カーネルセキュリティモードがLinuxシステムに展開されている場合、`# setsebool -P samba_export_all_rw on`コマンドを実行して、Samba共有の読み取り書き込みパーミッションを有効にします。
- `smbpasswd –a <user>`コマンドを使用してMedia AgentホストのユーザーをSambaのパスワードデータベースに追加します。次のコマンドを使用して、ユーザーがパスワードデータベースに追加されているかどうかを確認できます。`pdbedit -w -L`
- Windows Firewallを構成する必要があります。構成に関する詳細については、*HPE Data Protector Granular Recovery Extensionユーザーガイド*の「Configuring Windows Firewall exceptions」を参照してください。

> **注:**
> 1. Smart Cacheデバイスの構成に関する詳細については、*HPE Data Protector管理者ガイド*の「Smart Cacheを構成する」セクションを参照してください。
> 2. StoreOnceデバイスの構成に関する詳細については、*HPE Data Protector管理者ガイド*の「ディスクへのバックアップデバイスを構成する - StoreOnce」セクションを参照してください。

*SUSE Linux Enterprise Server (SLES)の場合はFUSE 2.7.2を使用します。

*SUSE Linux Enterprise Server 12 (SLES 12)の場合はFUSE 2.9.3を使用します。

マウントプロキシシステムに必要なData Protectorコンポーネント

Data Protectorクライアントをインストールします。次に、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ます。

- **`Virtual Environment Integration`**
- **`VMware Granular Recovery Extension Agent`**

コンポーネントの選択画面を参照してください。インストール手順の実行中にこのコンポーネントを選択する必要があります。Data Protectorクライアントのインストール、ページ 54を参照してください。

リモートインストールに失敗した場合は、ローカルシステムに拡張をインストールします。『*HPE Data Protector Granular Recovery Extensionユーザーガイド*』の「ローカルインストール回避策」セクションを参照してください。ただし、パッチ更新の場合は、GREエージェントをリモートにインストールする必要があります。

インポート手順の詳細については、『*HPE Data Protectorインテグレーションガイド*』の「統合ソフトウェアの構成」を参照してください。

デフォルトでは、RHEL 7.0およびSLES 12に対してLinuxループデバイスが作成されません。マウントプロキシシステムに十分なLinuxループデバイスがあることを確認してください。完全な論理ボリュームグループを使用できるようにするために、マウントされたディスクの数に応じて十分なループデバイスが必要です。

> **注:**
> HPE Data Protectorコンポーネントまたは VMware VDDKを追加または削除した場合は、`VMware Granular Recovery Extension Agent`をインストールする前に、システムを再起動します。

> **注:**
> `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しているときに、場合によっては、インストールセッションの出力にユーザーへの通知が表示され、インストールを完了するためにターゲットホストの再起動が必要になることがあります。

> **注:**
> VMware Consolidated Backup (VCB)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、バックアップホストとして使用 *できません*。

VMware vCenter Server (VirtualCenter Server)

VMware vSphere用Data Protector Granular Recovery Extension (GRE)は、VMware vCenter Serverに統合されます。仮想マシンにアクセスするには、VMware vSphere Web Clientを使用します。VMware vSphere Web Clientのインターフェイスに[HPE Data Protector]タブが追加されます。

> **注:**
> 拡張GRE Webプラグインは、VMware vSphere Webクライアントバージョン5.5.0 U2以降でサポートされます。

VMware vCenter Server Appliance (VCSA) 6.0環境

前提条件

VCSAサーバーで以下のコマンドを実行する必要があります。

```
iptables -P INPUT ACCEPT

iptables -P OUTPUT ACCEPT

iptables -P FORWARD ACCEPT

iptables -F
```

VMware vSphere Web Client用Data Protector GREのインストール

考慮事項

1. 復元操作を行う仮想マシンにVMwareツール4.x以降がインストールされている必要があります。VMwareツールのインストールパッケージは、http://www.vmware.com/download Webページからダウンロードできます。
2. VMware vSphere用Data Protector Granular Recovery Extension Webクライアントでは、リモートインストールのみがサポートされています。
3. 拡張が適切に機能するようにするには、VMware vCenter Serverシステムとマウントプロキシシステムの両方を同じクライアントシステムにインストールして構成しないでください。
4. `VMware Granular Recovery Extension Agent`、`Virtual Environment Integration Agent`、Data Protector Cell Managerが同じバージョンであることを確認してください。バージョンが異なるエージェントはサポートされていません。

要件

拡張を使用するには、次のシステムをインストールして構成する必要があります。

- **Data Protector**セルおよびクライアント
- VMware vCenter Serverシステム
- マウントプロキシシステム

GREプラグインには、拡張GRE Webプラグインのユーザーインターフェイスを使用してアクセスすることができます。

新規インストール

以下の手順を実行して、VMware vSphere Web Client用GREをインストールします。

環境: Data Protectorバージョン(9.02以降)、vCenter (サポートされるバージョンについては、『Virtualization Support Matrix』を参照)、拡張GRE Webプラグイン。

手順1: Cell Managerをセットアップします。

Cell ManagerはWindowsシステムおよびLinuxシステムにインストールできます。

手順2: インストールサーバーをセットアップします。

デフォルトでインストールサーバーがCell Managerのインストールの一部として追加されます。

- WindowsインストールサーバーをCell Managerと共にWindowsにインストールする場合 (デフォルトのオプション)、この手順をスキップして、マウントプロキシの設定に進むことができます。
- Cell ManagerがLinux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をセットアップし、Linux上のCell Managerにインポートする必要があります。

手順3: マウントプロキシをセットアップします。

- WindowsシステムまたはLinuxシステムで実行できます。
- Cell Managerとは異なる専用のマシンにマウントプロキシをインストールすることをお勧めします。
- Data Protectorクライアントは、次のコンポーネントがインストールされたマウントプロキシマシンにインストールする必要があります。
  1. `Virtual Environment Integration`
  2. `VMware Granular Recovery Extension Agent.`

手順4: vCenter Serverをセットアップします。

- vCenterはWindows環境またはLinux環境にインストールできます。
- Data Protectorクライアントは必要ありません。

手順5: vCenter Serverに拡張GRE Webプラグインをインストールします。

1. vCenterマシンをvCenterクライアントとしてData Protector Cell Managerにインポートするには、以下の手順を実行します。
   a. **[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]**を選択します。
   b. vCenterのホスト名を入力し、タイプとして**VMware vCenter**を選択します。**[次へ]**をクリックします。
   c. vCenterの資格情報(vCenter Webクライアントへのログインに使用する資格情報と同じ)を入力します。**[拡張GRE Webプラグイン]**チェックボックスを選択し、**[完了]**をクリックします。

> **注：**
> `omnicc -import_vcenter` コマンドと`omnicc -export_host` コマンドをそれぞれ使用して、拡張GRE Webプラグインを登録および登録解除できます。詳細については、『*HPE Data Protector Command Line Interface Reference*』ガイドを参照してください。

> **注：**
> 複数のvCenterをData Protector Cell Managerにインポートできます。

アップグレード

適用できる環境または最適な環境を識別し、アップグレード手順を続行します。以下を参照してください。

Data Protector		**プラグイン**		
開始	**この行を、以下のように変更します。**	**アップグレード元**	**この行を、以下のように変更します。**	**参照先**
任意の旧バージョン	DP 9.02以降	Webプラグイン	拡張GRE Webプラグイン	オプション1
DP 9.02以降	最新バージョン	拡張GRE Webプラグイン	拡張GRE Webプラグイン	オプション2

オプション1

環境: vCenter 5.5 U2以降でWebプラグインが付属している以前のData Protectorバージョンから拡張GRE Webプラグインが付属しているData Protectorの新しいバージョン(9.02以降)にアップグレードする場合(サポートされるバージョンについては、『Virtualization Support Matrix』を参照)。

Data Protectorのアップグレード手順が完了したら、手順2に進みます。

以下の手順を実行します。

1. ネイティブ(必須バージョン)のData Protectorインストーラーを使用して、Data Protector Cell Managerをアップグレードします
2. Cell Managerで**vCenter**クライアントを右クリックし、**[アップグレード]**をクリックします(ユーザーがWeb Plug-inを設定したときに、vCenterマシンがすでにData Protectorクライアントとしてインストールされている必要があります)。この手順により、vCenter上の既存のWeb Plug-inが削除され、vCenter上のData Protectorクライアントが必須バージョンにアップグレードされます。

   > **注:**
   > 既存の要求ファイルは削除されるので、新しい要求を作成する必要があります。

3. Cell Managerでクライアントを右クリックし、**[アップグレード]**をクリックします。すべてのマウントプロキシと他のクライアントについてこの手順を繰り返します。

   vCenterマシンをvCenterクライアントとしてData Protector Cell Managerにインポートするには、以下の手順を実行します。

   a. **[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]**を選択します。
   b. vCenterのホスト名を入力し、タイプとして**VMware vCenter**を選択します。**[次へ]**をクリックします。
   c. vCenterの資格情報(vCenter Webクライアントへのログインに使用する資格情報と同じ)を入力します。**[拡張GRE Webプラグイン]**チェックボックスを選択し、**[完了]**をクリックします。

> **注:**
> 必要な場合は、Data Protectorクライアントをvcenter上で保持することができます。

オプション2

環境: Data Protectorの拡張GRE Webプラグインが付属しているData Protector 9.02以降をインストールしている場合、最新のアップグレードで拡張GRE Webプラグインの更新された機能を入手するには、以下の手順を実行します。

1. Data Protectorから拡張GRE Webプラグインの登録を解除するには、**[拡張GRE Webプラグインの登録解除]**チェックボックスの選択を解除して、**[適用]**をクリックします。拡張GRE Webプラグインのホストリストで、すべてのCell Managerが削除されていることを確認します。
2. 拡張GRE Webプラグインの登録するには、**[拡張GRE Webプラグインの登録解除]**チェックボックスを選択して、**[適用]**をクリックします。

> **注:**
> Cell Managerとすべてのプロキシサーバーがアップグレードされていることを確認します。

拡張GRE Webプラグインのアンインストール

プラグインの起動時に問題が発生する場合、以下の手順を実行して、環境に応じてそれまでに指示されたアップグレード手順を再開します。

拡張GRE Webプラグインをアンインストールするには

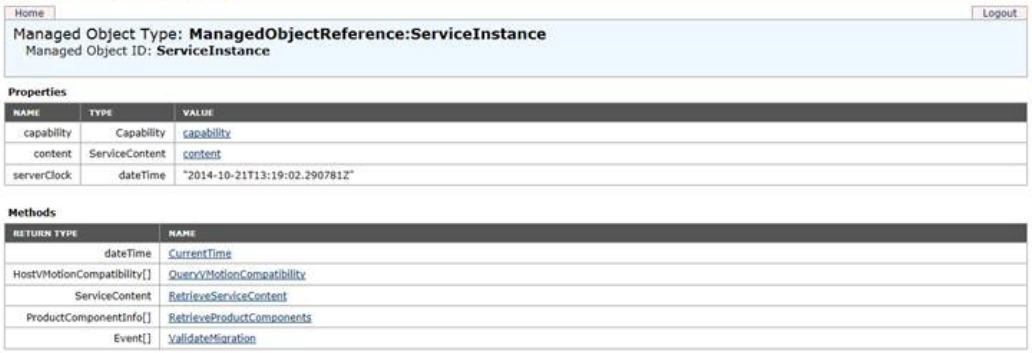
拡張GRE Webプラグインをアンインストールするには、VMware vCenterクライアントの[ログイン]タブで**[拡張GRE Webプラグイン]**チェックボックスの選択を解除し、**[適用]**をクリックします。

> **注：**
> Cell Managerまたは複数のCell Managerを、拡張GRE Webプラグインの登録解除をしないでアンインストールした場合、VMware vSphere Web Clientに[HPE Data Protector]タブが表示されますが、接続することはできません。手動で拡張GRE Webプラグインの登録を解除する必要があります。詳細については、VMware vSphere管理対象オブジェクト参照の手動による登録解除

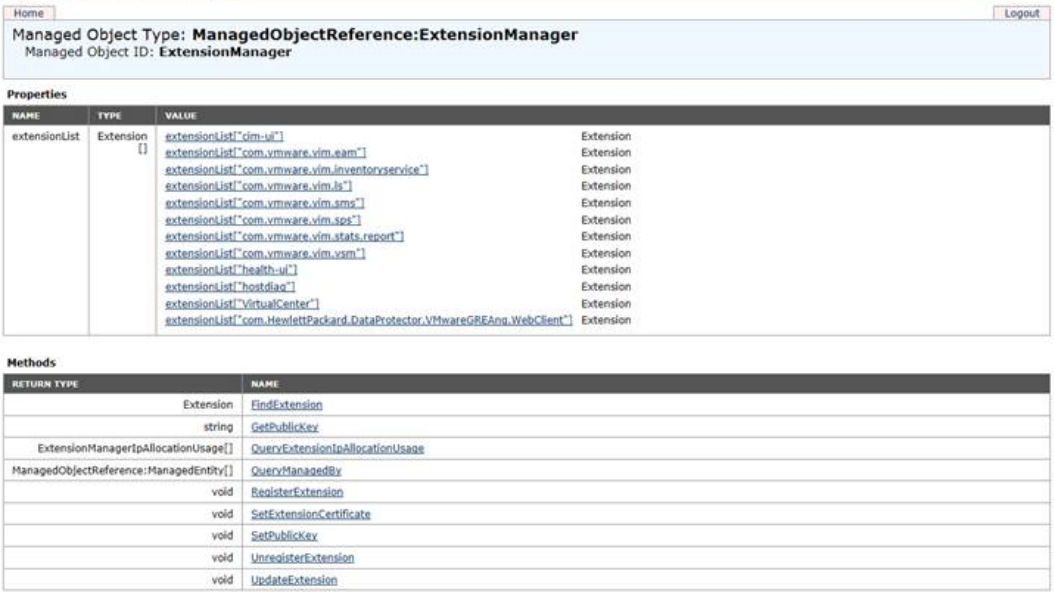
VMware vSphere管理対象オブジェクト参照の手動による登録解除

vCenterに登録されている1つ以上のCell Managerを削除するには、以下の手順を実行します。

1. VMware vSphere管理対象オブジェクト参照URLであるhttps://<vcenter>/mobに移動します。



2. **[Content]**をクリックし、**[ExtensionManager]**をクリックします。
3. HPEキー"com.HewlettPackardEnterprise.DataProtector.VMwareGREAng.WebClient"を選択します。



4. ページの下部にある**UnregisterExtension**をクリックします。

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。次のソリューションから選択することができます。

- Microsoft Hyper-Vクライアント、上
- Data Protector Microsoft Volume Shadow Copy Service integration、次のページ

Data Protector仮想環境用統合ソフトウェア

コンポーネントのインストール先となるシステムがすべて稼働状態であることが前提となります。

バックアップおよび復元セッションを制御するシステム(**バックアップホスト**)に次のData Protectorコンポーネントをインストールします。

- Virtual Environment Integration
- MS Volume Shadow Copy Integration
- Disk Agent

> **注：**
> Disk Agentコンポーネントをインストールすると、バックアップホスト上にあるディレクトリへの復元時に**[参照]**ボタンが表示されます。このコンポーネントをインストールしない場合は、ターゲットディレクトリを入力する必要があります。

Microsoft Hyper-Vシステムに次のData Protectorコンポーネントをインストールします。

- MS Volume Shadow Copy Integration

> **注:**
> Microsoft Hyper-Vシステムをクラスター内で構成する場合、クラスター対応クライアントとしてインストールする必要があります。詳細は、Microsoft Hyper-VクラスターでのData Protectorのインストール、ページ 189を参照してください。

バックアップシステム(VSSトランスポータブルバックアップ)に次のData Protectorコンポーネントをインストールします。

- MS Volume Shadow Copy Integration

> **注:**
> *バックアップホストとバックアップシステムは、同じシステムではありません。*

Data Protector Microsoft Volume Shadow Copy Service integration

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 Hyper-Vクライアント、前のページを参照してください。

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。

インストール手順中で、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:**
> 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。

HPE P4000 SANソリューション clients

HPE 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 Volume Shadow Copy Integration
- HPE P4000 VSS Agent

ディスクとテープへのZDBセッションまたはテープへのZDBセッションを実行するには、次のData Protectorソフトウェアコンポーネントをバックアップシステムに追加でインストールする必要があります。

- General Media Agent

HPE P6000 EVAディスクアレイファミリクライアント

HPE 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。

- `HPE P6000 / HPE 3PAR 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、ファイルシステムまたはディスクイメージのゼロダウンタイムバックアップを実行する場合に、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、`Application system`ドロップダウンリストおよび`Backup system`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 HPE 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/971254からダウンロードしてください。
>
> この追加要件は、Windows Server 2008 R2システムには適用されません。

クラスターへのインストール

HPE 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については、『*HPE 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

HPE 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。
HPE 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。

HPE 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ーを使用して、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オプションを設定します。詳細については、『*HPE 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

インストール作業は、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のドキュメントを参照し

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。
   - HPE P6000 / HPE 3PAR 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 Integration – 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:**
> - バックアップシステムのData ProtectorOracle Integration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方式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 ProtectorOracle IntegrationソフトウェアおよびHPE P6000 / HPE 3PAR 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。

HPE 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。詳細については、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*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。制御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、制御ファイルとオンライン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`ZDB_ORA_NO_CHECKCONF_IR`、`ZDB_ORA_INCLUDE_CF_OLF`、`ZDB_ORA_INCLUDE_SPFomnirc`オプションを設定します。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、『*HPE Data Protector Zero Downtime Backup Integration Guide*』を参照してください。

> **注:**
> 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システムの場合:*** 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システムの場合、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。
  - ora*ORACLE_SID* プライマリグループ `dba`
  - *ORACLE_SID* `adm` UNIXグループ `sapsys`
- 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:**
  > 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。詳細については、SAP R/3のドキュメント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) *SAPDATA_HOME*`\sapreorg` (Windowsシステムの場合)
  - *SAPDATA_HOME* `/sapcheck` (UNIXシステムの場合) *SAPDATA_HOME*`\sapcheck` (Windowsシステムの場合)
  - *SAPDATA_HOME* `/saptrace` (UNIXシステムの場合) *SAPDATA_HOME*`\saptrace` (Windowsシステム

の場合)

- /usr/sap/*ORACLE_SID*/SYS/exe/run (UNIXシステムの場合)
  c:\Oracle*ORACLE_SID*\sys\exe\run (Windowsシステムの場合)

> **注:**
> 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システムでは、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 2011 brarchive -rwsr-xr-x 1 orapro dba
4750020 Apr 17 2011 brbackup -rwsr-xr-x 1 orapro dba 4286707 Apr 17 2011
brconnect -rwsr-xr-x 1 proadm sapsys 430467 Apr 17 2011

brrestore -rwsr-xr-x 1 orapro dba 188629 Apr 17 2011 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。
   - HPE P6000 / HPE 3PAR SMI-S Agent
   - SAP R/3 Integration
   - Disk Agent

> **注:**
> 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。

HPE 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。

- `HPE P6000 / HPE 3PAR 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 Integration` – アプリケーションシステムのみ

HPE P6000 EVA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。

- `HPE P6000 / HPE 3PAR 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 Integration` – アプリケーションシステムのみ

HPE P9000 XPディスクアレイファミリクライアント

HPE 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。

- `HPEP9000 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、ファイルシステムまたはディスクイメージのゼロダウンタイムバックアップを実行する場合に、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、`Application system`ドロップダウンリストおよび`Backup system`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 HPE 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/971254からダウンロードしてください。
>
> この追加要件は、Windows Server 2008 R2システムには適用されません。

クラスターへのインストール

HPE 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については、『*HPE 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

HPE 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。HPE 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。

HPE 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ーを使用して、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HPE 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オプションを設定します。詳細については、『*HPE 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

インストール作業は、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のドキュメントを参照し

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。
   - `HPE 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 Integration` – 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:**
> - バックアップシステムのData Protector `Oracle Integration`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方式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`Oracle Integration`べてのシステムに`HPE P9000 XP Agent`およびData Protector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。

HPE 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。詳細については、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*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。制御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、制御ファイルとオンライン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`ZDB_ORA_NO_CHECKCONF_IR`、`ZDB_ORA_INCLUDE_CF_OLF`、`ZDB_ORA_INCLUDE_SPFomnirc`オプションを設定します。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、『*HPE Data Protector Zero Downtime Backup Integration Guide*』を参照してください。

> **注:**
> 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システムの場合:*** 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システムの場合、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。
  - ora*ORACLE_SID* プライマリグループ `dba`
  - *ORACLE_SID* `adm` UNIXグループ `sapsys`
- 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:**
  > 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。詳細については、SAP R/3のドキュメント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) - OracleおよびSAP R/3プロファイル
  - *ORACLE_HOME* `/bin or` (UNIXシステムの場合)
    ORACLE_HOME `\bin` (Windowsシステム) - Oracleバイナリ
  - *SAPDATA_HOME* `/sapbackup` (UNIXシステムの場合)
    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システムの場合)
    SAPDATA_HOME`\sapreorg` (Windowsシステム)
  - *SAPDATA_HOME* `/sapcheck` (UNIXシステムの場合)
    SAPDATA_HOME`\sapcheck` (Windowsシステム)
  - *SAPDATA_HOME* `/saptrace` (UNIXシステムの場合)

SAPDATA_HOME\saptrace (Windowsシステム)

- /usr/sap/*ORACLE_SID*/SYS/exe/run (UNIXシステムの場合)

  c:\Oracle*ORACLE_SID*\sys\exe\run (Windowsシステムの場合)

  > **注:**
  > 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システムでは、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 2011 brarchive -rwsr-xr-x 1 orapro dba
4750020 Apr 17 2011 brbackup -rwsr-xr-x 1 orapro dba 4286707 Apr 17 2011
brconnect -rwsr-xr-x 1 proadm sapsys 430467 Apr 17 2011

brrestore -rwsr-xr-x 1 orapro dba 188629 Apr 17 2011 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。
   - HPEP9000 XP Agent
   - SAP R/3 Integration
   - Disk Agent

> **注:**
> 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。

HPE 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HPE 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、HPE BC P9000 XPまたはHPE 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。

- `HPE 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 Integration` – アプリケーションシステムのみ

HPE 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。

- `HPE P9000 XP Agent`
- `MS SQL Integration`

HPE 3PAR StoreServ Storage clients

HPE 3PAR StoreServ Storage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。

- HPE P6000 / HPE 3PAR SMI-S Agent

ボリュームシャドウコピーサービスを使用してオブジェクトをバックアップおよび復元するには、以下のコンポーネントも必要になります。

- MS Volume Shadow Copy Integration
- HPE 3PAR VSS Agent

オペレーティングシステムに関係なく、ディスクとテープへのZDBセッションまたはテープへのZDBセッションを実行するには、次のData Protectorソフトウェアコンポーネントをバックアップシステムに追加でインストールする必要があります。

- General Media Agent

EMC Symmetrixクライアント

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、Application systemドロップダウンリストおよびBackup system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については、『*HPE 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

インストール作業は、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のドキュメント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 Integration` – 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:
- バックアップシステムのData Protector`Oracle Integration`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方式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`ソフトウェアおよび`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。詳細については、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*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。制御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、制御ファイルとオンライン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:
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システムの場合:*** 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システムの場合、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。
  - ora*ORACLE_SID* プライマリグループ dba
  - *ORACLE_SID* adm UNIXグループ sapsys
- 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:**
  > ディレクトリの場所は、環境変数によって変わります。詳細については、SAP R/3のドキュメント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
  - *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:**
    > 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 2011 brarchive -rwsr-xr-x 1 orapro dba
  4750020 Apr 17 2011 brbackup -rwsr-xr-x 1 orapro dba 4286707 Apr 17 2011
  ```

```
brconnect -rwsr-xr-x 1 proadm sapsys 430467 Apr 17 2011 brrestore -rwsr-xr-x 1
orapro dba 188629 Apr 17 2011 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 Integration
   - Disk Agent

> **注:**
> 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 Integration

non-HPE Storage Arrays

Data Protectorは、non–HPE Storage Arrays用のストレージプロバイダーを使用して、ZDBストレージアレイ(NetAppストレージ、EMC VNX、およびEMC VMAXストレージファミリー)と統合されます。このストレージプロバイダーコンポーネントは、Data Protector SMI-S Agentのプラグインです。これにより、SMI-S Agentを介してそれぞれのストレージのZDB機能が有効になります。

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。

- non–HPE Storage Arrays用のいずれかのストレージプロバイダーコンポーネント(どのコンポーネントかは、使用するストレージ(NetApp Storage Provider、EMC VNX Storage Provider、またはEMC VMAX Storage Provider)によって異なります)

テープへのZDBセッションを実行するには、次のData Protectorソフトウェア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する必要があります。

- General Media Agent

他のアプリケーションの統合

Data Protector non–HPE Storage Array用統合ソフトウェアをデータベースアプリケーションまたは仮想環境統合ソフトウェアと組み合わせてインストールする場合は、特定の統合ソフトウェアに必要なData Protectorコンポーネントを該当するシステムにインストールし、この統合ソフトウェア特有のインストール作業を実行してください。non–HPE Storage Array用統合ソフトウェアをVMware、Oracle Server、SAP R/3、およびMicrosoft SQL Serverと共にインストールできます。non–HPE Storage Arrayとの組み合わせがサポートされているデータベースアプリケーションまたは仮想環境統合は、https://softwaresupport.hpe.com/にある最新のサポート一覧で確認してください。

non-HPE Storage ArrayとVMwareの仮想環境の統合

制限事項

- VMware vCenter環境のみがサポートされます。
- インスタントリカバリはサポートされていません。
- テープへのZDBのみがサポートされます。

前提条件

コンポーネントのインストール先となるシステムがすべて稼働状態であることが前提となります。

インストール手順

バックアップおよび復元セッションを制御するシステム(バックアップシステム)に次のData Protectorコンポーネントをインストールします。

- Virtual Environment Integration
- 非HPEストレージアレイ(NetApp Storage Provider)用ストレージプロバイダー
- General Media Agent
- Disk Agent

> **注:**
> - Disk Agentコンポーネントをインストールすると、バックアップホスト上にあるディレクトリへの復元時に**[参照]**ボタンが表示されます。このコンポーネントをインストールしない場合は、ターゲット

ディレクトリを入力する必要があります。
- VMware Consolidated Backup (VCB)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、バックアップホストとして使用 *できません*。

non-HPE Storage ArrayとOracle Serverの統合

制限事項

- RACクラスター環境はサポートされません。
- インスタントリカバリはサポートされていません。
- テープへのZDBのみがサポートされます。

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ーを使用して、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、インストールしたストレージプロバイダー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。
  - 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。

  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

インストール作業は、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のドキュメント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。
   - non–HPE Storage Array用のストレージプロバイダー(`NetApp Storage Provider`、`EMC VNX Storage Provider`、または`EMC VMAX Storage Provider`)
   - `Oracle Integration` – 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:
   - バックアップシステムのData Protector`Oracle Integration`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方式の場合は必要ありません。
   - 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。

HPE以外のストレージアレイとSAP R/3の統合

制限事項

- インスタントリカバリはサポートされていません。
- テープへのZDBのみがサポートされます。

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。詳細については、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、ストレージシステムに配置する*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REDOログをストレージシステム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。制御ファイルはストレージシステム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、制御ファイルとオンラインREDOログはストレージシステムに配置する*必要があります*。
- アーカイブREDOログファイルは、ストレージシステムに配置する必要はありません。

> **注:**
> 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システムの場合:***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システムの場合、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ora*ORACLE_SID*
  - UNIXグループsapsysに属する *ORACLE_SID* adm
- 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:**
  > 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。詳細については、SAP R/3のドキュメント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)

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システムでは、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  2011 brarchive
-rwsr-xr-x   1 orapro dba 4750020 Apr 17  2011 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  2011 brconnect
-rwsr-xr-x   1 proadm sapsys 430467 Apr 17  2011

brrestore
-rwsr-xr-x   1 orapro dba 188629 Apr 17  2011 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。
   - 非HPEストレージアレイ(NetApp Storage Provider)用ストレージプロバイダー
   - SAP R/3 Integration
   - Disk Agent

> **注:**
> 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。

HPEストレージアレイとMicrosoft SQL Serverの統合

制限事項

- インスタントリカバリはサポートされていません。
- テープへのZDBのみがサポートされます。

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。

- non–HPE Storage Array用 のストレージプロバイダー(NetApp Storage Provider、EMC VNX Storage Provider、またはEMC VMAX Storage Provider) – 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 Integration – アプリケーションシステムのみ

第5章: クラスターへのData Protectorのインストール

HPE ServiceguardへのData Protectorのインストール

Data Protectorは、HP-UXおよびLinux用のHPE Serviceguard (HPE SG)をサポートしています。サポートされているオペレーティングシステムバージョンは、『HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照してください。

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。

構成の段階

1. プライマリCell Managerの構成
2. セカンダリCell Managerの構成
3. Cell Managerパッケージの構成

クラスター対応Cell Managerのインストール

前提条件

HPE Serviceguard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。

- 一次Cell Managerとなるシステムと二次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、HPE 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必要があります。
- 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。
- ユーザーグループhpdpと、専用のユーザーアカウントhpdpには、両方のノードで同じIDを割り当てる必要があります。
- このクラスター環境では、Data Protector Cell Managerに専用のパッケージを持つ必要があります。HPE Serviceguard環境内にData Protector Cell Managerをインストールする前に、ネットワーク管理者から以下の情報を取得する必要があります。
  - 仮想サーバー名(クラスターパッケージで指定されたホスト名)
  - パッケージIPまたは仮想IPアドレス

さらに、共 有 ディスクにボリュームグループを作 成 する必 要 があります。詳 細 は、「ボリュームグループ作 成 の例 、ページ 169」を参 照 してください。

- クラスターノードとパッケージIP(仮 想 IP)が同 じサブネット上 に存 在 する必 要 があります。
- 環 境 内 にDNSがある場 合 は、クラスターのすべてのノードとパッケージIPをDNSサーバーに登 録 しておく必 要 があります。

プライマリCell Managerの構 成

手 順

1. クラスターを起 動 します。

   ```
   cmruncl
   ```

2. ボリュームグループをアクティブ化 します。

   HP-UX:

   ```
   vgchange -a e vg_name
   ```

   Linux:

   ```
   vgchange -a y vg_name
   ```

3. 論 理 ボリュームをポイントディレクトリ(例 : /omni_shared)にマウントします。

   ```
   mount lv_path /omni_shared
   ```

4. /etc/opt/omni/server/sg/sg.confテンプレートファイルを変 更 します。

   > **注 :**
   > 使 用 するマウントポイントディレクトリの名 前 をSHARED_DISK_ROOTオプションで定 義 しておく必 要 があります(例 : SHARED DISK ROOT=/omni_shared)。
   >
   > 仮 想 Cell Managerをネットワークで認 識 するための名 前 をCS_SERVICE_HOSTNAMEオプションで定 義 しておく必 要 があります。クラスター内 の各 パッケージに対 して、専 用 の仮 想 IPアドレスとネットワーク名 を割 り当 てる必 要 があります(例 : CS_SERVICE HOSTNAME=ob2cl.company.com)。

5. プライマリCell Managerを構 成 します。このスクリプトを実 行 するときは、カレントディレクトリが /etc/opt/omni/または/var/opt/omni/でないことを確 認 してください。/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 を実 行 します。

   ```
   /opt/omni/sbin/install/omniforsg.ksh -primary
   ```

   なお、このスクリプトを実 行 すると、Data Protectorのサービスが停 止 されます。これらのサービスは、後 で再 開 されます。

6. マウントポイントディレクトリのマウントを解 除 します。

   ```
   umount dirname
   ```

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
   ```

セカンダリCell Managerの構成

手順

1. ボリュームグループをアクティブ化します。

   HP-UX:

   ```
   vgchange -a e vg_name
   ```

   Linux:

   ```
   vgchange -a y vg_name
   ```

2. 論理ボリュームをポイントディレクトリにマウントします。

   ```
   mount lv_path /omni_shared
   ```

3. セカンダリCell Managerを構成します。

   ```
   /opt/omni/sbin/install/omniforsg.ksh -secondary dirname
   ```

   ここで、*dirname*は、マウントポイントまたは共有ディレクトリを表します(例：`/omni_shared`)。

4. マウントポイントディレクトリのマウントを解除します。

   ```
   umount /omni_shared
   ```

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
   ```

Cell Managerパッケージの構成

前提条件

- 両方のクラスターノードにData Protector Cell Managerがインストールされており、正しく構成されていること。
- Data Protectorクラスターパッケージを構成する前に、クラスター構成ファイルを作成して編集しておくこと。

レガシーパケージ構成には常に、パッケージ構成ファイルとパッケージコントロールスクリプトの2つのファイルが含まれます。レガシーパケージ構成ファイルは、ASCIIファイルとして作成され、`cmapplyconf`コマンドを使用して、バイナリのServiceguard構成に格納されます。モジュールパッケージ構成ファイルには、1つのファイルにすべてのパッケージファイルシステム、マウントポイント、サービス定義が含まれます。このファイルは、`cmapplyconf`コマンドを使用して、バイナリのServiceguard構成に格納されます。

> **注：**
> どちらのクラスターノードでもData Protectorデーモンは稼動しなくなります。

手順

プライマリCell Manager上で、以下の手順を実施します。

1. クラスター構 成 ファイル(cluster.confなど)にエラーがないかどうかをチェックします。

   ```
   cmcheckconf -C /etc/cmcluster/cluster.conf
   ```

   エラーがある場 合 は、エラーを修 正 します。

   エラーがなければ、構 成 を有 効 化 します。

   ```
   cmapplyconf -C /etc/cmcluster/cluster.conf
   ```

2. まだ起 動 していない場 合 は、クラスターを起 動 します。

   ```
   cmruncl
   ```

3. Data Protectorクラスターパッケージファイル(構 成 と制 御)を作 成 および修 正 します。モジュールパッケージの場 合 は、1つのクラスターパッケージファイル(構 成)を作 成 し、修 正 します。

   a. /etc/cmclusterの下 層 にData Protectorパッケージ用 のサブディレクトリを作 成 します。

      ```
      mkdir /etc/cmcluster/ob2cl
      ```

   b. /etc/cmcluster/ob2clディレクトリに移 動 します。

      ```
      cd /etc/cmcluster/ob2cl
      ```

   c. レガシーパッケージの場 合 は、Data Protectorのパッケージディレクトリ内 にパッケージ構 成 ファイルを作 成 します。

      ```
      cmmakepkg -p /etc/cmcluster/ob2cl/ob2cl.conf
      ```

      モジュールパッケージの場 合 は、次 のコマンドを使 用 します。

      ```
      cmmakepkg -m sg/all ob2cl.conf
      ```

   d. この手 順 は、レガシーパッケージに対 してのみ実 行 する必 要 があります。Data Protectorのパッケージディレクトリ内 にパッケージコントロールファイルを作 成 します。cmmakepkg -s /etc/cmcluster/ob2cl/ob2cl.cntl

   e. Data Protectorパッケージ構 成 ファイルを修 正 します(例 : /etc/cmcluster/ob2cl/ob2cl.conf)。詳 細 は、「Data Protectorパッケージ制 御 ファイルの修 正 、ページ 172」を参 照 してください。

   f. この手 順 は、レガシーパッケージに対 してのみ実 行 する必 要 があります。Data Protectorパッケージ制 御 ファイルを修 正 します(例 : /etc/cmcluster/ob2cl/ob2cl.cntl)。詳 細 は、「Data Protectorパッケージ制 御 ファイルの修 正 、ページ 174」を参 照 してください。

4. Data Protectorクラスターパッケージファイルをチェックおよび伝 播 します。

   a. レガシーパッケージの場 合 、パッケージ制 御 ファイルをクラスター内 の他 のノード(system2)にコピーします。

      ```
      remsh system2 "mkdir /etc/cmcluster/ob2cl" rcp
      /etc/cmcluster/ob2cl/ob2cl.cntl system2: /etc/cmcluster/ob2cl/ob2cl.cntl
      ```

   b. Data Protectorの共 有 ディスクを、以 前 作 成 したクラスターボリュームグループとしてすべてのクラスターノード上 で有 効 にします。

      HP-UX:

      ```
      vgchange -c y vg_name
      ```

      Linux:

      ```
      vgchange -a y vg_name
      ```

   c. Data Protectorパッケージをチェックします。

      ```
      cmcheckconf -P /etc/cmcluster/ob2cl/ob2cl.conf
      ```

チェックが正 常 に終 了 したら、Data Protectorパッケージを追 加 します。

```
cmapplyconf -P /etc/cmcluster/ob2cl/ob2cl.conf
```

d. パッケージを起 動 します。

```
cmrunpkg ob2cl
```

異 常 がなければ、クラスターが形 成 され、Data Protector Cell Managerパッケージが稼 動 を開 始 します。

5. プライマリノード で、IDBおよびアプリケーションサーバーのData Protector領 域 クライアント のクラスターホスト名 を更 新 します。以 下 のコマンドを最 初 のアクティブノード で1回 だけ実 行 します。

```
#omnidbutil -config_unixCluster -clusterHost  <clusterHostName>
```

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セカンダリHPE 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システム用 のインストールサーバーのインストール、ページ 42

> **注 :**
> プライマリノードをクラスター対 応 Cell Managerとして構 成 する前 に、インストールサーバーをインストールする場 合 、インストールサーバーが、各 2次 クラスターノードにインストールされていることを確 認 します。プライマリノード の構 成 中 、インストールサーバーが、仮 想 サーバー名 を使 ってインポートされます。インストールサーバーが各 クラスターノードにインストールされていない場 合 、その仮 想 サーバー名 をインストールサーバーのリストからエクスポートする必 要 があります。さらに、クラスター対 応 Cell Managerの構 成 が完 了 した後 、対 応 する各 物 理 クラスターノード 名 もインポートする必 要 があります。

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。

インストール手 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 については、HP-UXクライアント のインストール 、ページ 71とLinuxクライアント のインストール、ページ 81を参 照 してください。

次 に行 う手 順

インストールが完 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 、ページ 192」を参 照 してください。

バックアップデバイスとメディアプールの構 成 方 法 、または追 加 のData Protector構 成 タスクについては、*HPE Data Protector*ヘルプのキーワード「構 成 」で表 示 される内 容 を参 照 してください。

ボリュームグループ作 成 の例

両 方 のCell Managerからアクセスできる共 有 ディスク上 にボリュームグループを作 成 します。

> **注 :**
> ob2ディスクをクラスターロックディスクとして使 用 する場 合 は、そのディスク用 のボリュームグループを事 前 に作 成 しておく必 要 があります。

プライマリノード の手 順

プライマリノード 上 で、以 下 の手 順 を実 行 します。

1. a. 新 しいボリュームグループ用 のディレクトリを作 成 します。

   ```
   mkdir vg_name
   ```

   > **注 :**
   > vg_nameは、/devディレクトリのサブディレクトリにあるボリュームグループのパス名 です。

   b. システム上 のすべての既 存 ボリュームグループのリストを表 示 し、どのマイナー番 号 が使 用 中 かをチェックします。

   ```
   ll /dev/*/group
   ```

   c. ボリュームグループに対 してグループファイルを作 成 します。

   ```
   mknod vg_name/group c 64 0xNN0000
   ```

   > **注 :**
   > NNは、使 用 可 能 なマイナー番 号 です。

   d. Data Protector Cell Manager用 のディスク上 に物 理 ボリュームを作 成 します。

   ```
   pvcreate -f pv_path ...
   ```

   > **注 :**
   > pv_pathは、pvcreateコマンドとともに使 用 され、/dev/rdskディレクトリのサブディレクトリ内 にある物 理 ボリュームのキャラクター(raw)デバイスパス名 を示 します(たとえば、物 理 ボリュームc0t1d0のcharacter pv_pathは/dev/rdsk/c0t1d0です)。

   e. 新 しいボリュームグループを作 成 します。

   ```
   vgcreate vg_name pv_path ...
   ```

   > **注 :**
   > pv_pathは、vgcreateコマンドとともに使 用 され、新 しいボリュームグループに割 り当 てる物 理 ボリュームのブロックデバイスパス名 を示 します。これは、/dev/dskディレクトリのサブディレクトリにあります(たとえば、物 理 ボリュームc0t1d0のblock pv_pathは、/dev/dsk/c0t1d0です)。

2. このグループの論 理 ボリュームを作 成 します。
   a. ボリュームグループに対 して新 しい論 理 ボリュームを作 成 します。

   ```
   lvcreate -L lv_size -n lv_name vg_name
   ```

> **注:**
> /etc/opt/omniおよび/var/opt/omni Data Protectorディレクトリはここで利用できます。
> *lv_size*は、パーティションサイズ(MB単位)を表します。
> *lv_name*は、論理ボリュームの名前です。

b. 論理ボリューム上にジャーナルファイルシステムを作成します。

```
newfs -F FStype lv_path
```

> **注:**
> *FStype*では、動作の対象となるファイルシステムのタイプを指定します。
> *lv_path*は、論理ボリュームのキャラクター(raw)特殊デバイスパス名です。

3. クラスターのドキュメントに従ってボリュームグループのプロパティを設定します。

HP-UX:

a. 通常モードから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
```

b. ボリュームグループをクラスター用として指定します。

```
vgchange -c y vg_name
```

> **注:**
> 新しいバージョンのHPE Serviceguard(11.09など)を使用している場合、これがクラスターロックディスクであれば、クラスター用のボリュームグループが自動的に指定されます。

c. ボリュームグループを排他モードで使用します。

```
vgchange -a e vg_name
```

Linux:

a. 通常モードから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
```

b. ボリュームグループをクラスター用として指定します。

```
vgchange -a y vg_name
```

4. マウントポイントディレクトリ(例: /omni_shared)を作成し、このディレクトリに論理ボリュームをマウントします。

a. `mkdir shared_dirname`

b. `mount lv_path shared_dirname`

5. マウントポイントディレクトリのマウントを解除します。

```
umount shared_dirname
```

6. 作成した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
```

7. プライマリCell Managerに作成したボリュームグループをエクスポートします。

a. system1からLVM構成情報をエクスポートします。

```
vgexport -p -m mapfile vg_name
```

> **注 :**
> *mapfile*では、論 理 ボリューム名 および番 号 の書き込 み先 となるファイルのパス名 を指 定します。

b. マップファイルをsystem2に転 送します。

```
rcp mapfile second_system: mapfile
```

セカンダリノードの手 順

セカンダリノード上 で、以 下 の手 順を実 行します。

1. インポートするボリュームグループを作 成し、それをインポートします。
   a. 新しいボリュームグループ用 のディレクトリを作 成します。

   ```
   mkdir vg_name
   ```

   > **注 :**
   > *vg_name*は、/devディレクトリのサブディレクトリにあるボリュームグループのパス名 です。

   b. システム上 のすべての既 存 ボリュームグループのリストを表 示し、どのマイナー番 号 が使 用 中 かをチェックします。

   ```
   ll /dev/*/group
   ```

   c. ボリュームグループに対してグループファイルを作 成します。

   ```
   mknod vg_name/group c 64 0xNN0000
   ```

   > **注 :**
   > NNは、使 用 可 能 なマイナー番 号 です。

   d. ボリュームグループをインポートします。

   ```
   vgimport -m mapfile -v vg_name pv_path ...
   ```

   > **注 :**
   > *mapfile*では、論 理 ボリューム名 および番 号 の読 み取り元 のファイル名 を指 定します。
   > *pv_path*は、物 理 ボリュームのブロックデバイスパス名 です。

2. ボリュームグループのプロパティを設 定します。

   HP-UX:

   a. 通 常 モード から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
   ```

   b. ボリュームグループをクラスター用 として指 定します。

   ```
   vgchange -c y vg_name
   ```

   > **注 :**
   > 新しいバージョンのHPE Serviceguard(11.09など)を使 用している場 合 、これがクラスターロックディスクであれば、クラスター用 のボリュームグループが自 動 的 に指 定 されます。

   c. ボリュームグループを排 他 モード で使 用します。

   ```
   vgchange -a e vg_name
   ```

Linux:

a. 通 常 モード から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
```

b. ボリュームグループをクラスター用 として指 定します。

```
vgchange -a y vg_name
```

3. プライマリCell Managerに作 成したのと同じマウントポイント ディレクトリを作 成し、このディレクトリに論 理 ボリュームをマウントします。
4. マウントポイント ディレクトリのマウントを解 除します。

```
umount shared_dirname
```

5. インポートした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
```

Data Protectorパッケージ制 御 ファイルの修 正

Data Protectorモジュールパッケージ構 成 ファイルでは、以 下 のフィールドを修 正してください。

例 :

package_name	ob2cl
run_script_timeout	600
halt_script_timeout	600
script_log_file	/usr/local/cmcluster/conf/ob2cl/ob2cl.log

サブネット設 定 は以 下 のとおりです。

例 :

monitored_subnet	10.81.0.0
ip_subnet	10.81.0.0
ip_address	10.81.8.46

> **注 :**
> monitored_subnetはクラスターノードを含 むサブネット です。
>
> ip_subnetはData Protector Cell Manager仮 想 サーバーを含 むサブネット です。
>
> ip_addressはData Protector Cell Manager仮 想 サーバーIPです。

Data Protectorサービス設 定 は以 下 のとおりです。

例 :

service_name	dp_svc
service_cmd	/opt/omni/sbin/csfailover.ksh

	start
service_restart	None
service_fail_fast_enabled	no
service_halt_timeout	300

> **注 :**
> service_cmdは/opt/omni/sbin/csfailover.ksh startに設 定 する必 要 があります。

Data Protector共 有 ファイルシステム情 報 は以 下 のとおりです。

例 :

vg	DP
fs_name	/dev/DP/vol
fs_directory	/DPCLUS
fs_type	ext3
fs_mount_opt	-o rw
fs_umount_opt	""
fs_fsck_opt	""

Data Protectorレガシーパッケージ構 成 ファイルでは、以 下 のフィールドを修 正 してください。

PACKAGE_NAME

NODE_NAME

RUN_SCRIPT(Data Protectorパッケージ制 御 ファイルと同 じ)

HALT_SCRIPT(Data Protectorパッケージ制 御 ファイルと同 じ)

MONITORED_SUBNET

SERVICE_NAME(任 意 の名 前 を入 力 できますが、制 御 ファイルを同 じ名 前 を使 用 する必 要 があります)

SERVICE_FAIL_FAST_ENABLED

SERVICE_HALT_TIMEOUT

例 :

PACKAGE_NAME	ob2cl
NODE_NAME	onca
NODE_NAME	pardus
RUN_SCRIPT	/etc/cmcluster/ob2cl/ob2cl.cntl
HALT_SCRIPT	/etc/cmcluster/ob2cl/ob2cl.cntl

MONITORED_SUBNET	10.17.0.0
SERVICE_NAME	omni_sv
SERVICE_FAIL_FAST_ENABLED	NO
SERVICE_HALT_TIMEOUT	300

Data Protectorパッケージ制 御 ファイルの修 正

Data Protectorレガシーパッケージ制 御 ファイルでは、以 下 のフィールドを修 正 してください。

VG [n]

LV [n]

FS [n]

FS_MOUNT_OPT [n]

IP

SUBNET

SERVICE_NAME(構 成 ファイルで使 用 されている名 前 と同じ)

SERVICE_CMD(次 のとおりとする:/opt/omni/sbin/csfailover.ksh start)

例 :

VG[0]	vg_dp
LV[0]	/dev/vg_dp/dp_share
FS[0]	/DP_SHARE
FS_MOUNT_OPT[0]	-o rw
FS_TYPE[0]	vxfs
IP[0]	10.17.17.69
SUBNET[0]	10.17.0.0
SERVICE_NAME[0]	omni_sv
SERVICE_CMD[0]	/opt/omni/sbin/csfailover.ksh start

Symantec Veritas Cluster ServerへのData Protectorのインストール

Data Protectorは、Linux用 のSymantec Veritas Cluster Server (VCS)をサポートしています。サポートされるオペレーティングシステムバージョンの詳 細については、最 新 の『*Data Protectorのプラットフォームと統合 ソフトウェアのサポート一 覧*』を参 照してください。

> **注 :**
> Data Protectorサービスグループ IPが構 成 済 みの場 合 は、そのIPをライセンシング用 に使 用します。IPアドレスなしでData Protectorサービスグループが構 成 済 みの場 合 は、Veritas Cluster IPをライセンシング用 に使 用します。

構 成の段 階

1. プライマリCell Managerの構 成
2. セカンダリCell Managerの構 成
3. Cell Managerクラスターサービスグループの構 成

クラスター対 応 Cell Managerのインストール

前 提 条 件

VCS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。

- プライマリとセカンダリのCell Managerシステムを特 定します。このすべてのシステムは、Symantec Veritas Cluster Serverがインストールされ、クラスターのメンバーとして構 成されている必 要 があります。
- 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。
- ユーザーグループhpdpと、専 用 のユーザーアカウントhpdpには、両 方 のノードで同じIDを割り当 てる必 要 があります。
- このクラスター環 境 では、Data Protector Cell Managerにそれ独 自 のクラスターサービスが必 要 です。これは、クラスター対 応 のCell Managerの構 成 前 に作 成し準 備する必 要 があります。Data Protector Cell ManagerをVCSにインストールする前 に、仮 想 サーバー名 とそれに対 応 するIPを取 得する必 要 があります。このサーバー名 またはIPは、後 でData Protector Cell Manager仮 想 サーバー名 またはData Protectorサービスグループ IPとして使 用されます。
- クラスターノードとData Protectorサービスグループ IP(仮 想 IP)が同じサブネット上 に存 在する必 要 があります。

  > **注 :**
  > Data Protectorサービスグループ IPとVeritas Cluster IPは異 なっていることを確 認してください。

- 環境内にDNSがある場合は、クラスター内のすべてのノードとData Protectorサービスグループ IPをDNSサーバーに登録しておく必要があります。
- インストールが完了したら、インストールした一次Cell Managerと二次Cell Manager、およびCell Managerパッケージを構成する必要があります。

Data Protector Cell Manager用のクラスターサービスグループの準備

以下のリソースを持つクラスター(Data Protector)サービスグループを作成する必要があります。

- IPクラスターリソース - IPリソース構成に使用される仮想IPです。
- マウントクラスターリソース - 対応する従属リソースがあるマウントリソースで、共有ボリュームを制御するために使用します(その共有ボリュームは、共有ディスク上に作成され、Data Protectorを実行する可能性があるすべてのノードからアクセス可能です)。この共有ボリュームは、ノード間で共有されるData Protector構成とデータファイル用に使用されます。

プライマリCell Managerの構成

手順

1. プライマリノード上のData Protectorサービスグループを起動します。
2. `/etc/opt/omni/server/sg/sg.conf`テンプレートファイルを変更します。

   注:
   使用するマウントポイントディレクトリの名前を`SHARED_DISK_ROOT`オプションで定義しておく必要があります(例: `SHARED DISK ROOT=/omni_shared`)。

   仮想Cell Managerをネットワークで認識するための名前を`CS_SERVICE_HOSTNAME`オプションで定義しておく必要があります。(例: `CS_SERVICE HOSTNAME=dpvcs.company.com`)

3. プライマリCell Managerを構成します。スクリプトが、`/etc/opt/omni/`または`/var/opt/omni/`ディレクトリ、またはそれらのサブディレクトリから実行されていないことを確認します。サブディレクトリが、`/etc/opt/omni/`または`/var/opt/omni/`ディレクトリにマウントされていないことも確認します。次のコマンドを実行します。

   ```
   /opt/omni/sbin/install/omniforsg.ksh -primary
   ```

   注:
   このスクリプトを実行すると、Data Protectorのサービスが停止されます。これらのサービスは、後で再開されます。

セカンダリCell Managerの構 成

手 順

1. Data Protectorサービスグループを2次 ノード に切り替 えます。
2. セカンダリCell Managerを構 成します。

   ```
   /opt/omni/sbin/install/omniforsg.ksh -secondary dirname
   ```

   ここで、*dirname*は、マウントポイントまたは共 有 ディレクトリを表します(例： `/omni_shared`)。

Cell Managerクラスターサービスグループの構 成

手 順

1. Data Protectorサービスグループを切り替 えてプライマリノード に戻します。
2. クラスターアプリケーションリソースを追 加します。これは、Data ProtectorサービスグループへのData Protectorサービスを監 視し制 御 するために使 用され、アプリケーションの監 視 または制 御 プログラムとして`vcsfailover.ksh`スクリプトを使 用します。 例：

   ```
   Application dpapp (
   StartProgram = "/opt/omni/sbin/vcsfailover.ksh start"
   StopProgram = "/opt/omni/sbin/vcsfailover.ksh stop"
   CleanProgram = "/opt/omni/sbin/vcsfailover.ksh stop"
   MonitorProgram = "/opt/omni/sbin/vcsfailover.ksh monitor"
    )
   ```

   > **注：**
   > `vcsfailover.ksh`スクリプト のカスタマイズが必 要 なときは、そのコピーを監 視 プログラムまたは制 御 プログラムとして作 成し、使 用する必 要 があります。 アップグレード または更 新 時 には、元 のスクリプト が上 書きされます。 新しく導 入 された変 更 があれば、カスタマイズしたスクリプトをその変 更 に基 づいて手 動 で更 新 する必 要 があります。

3. Data Protectorアプリケーションリソースを作 成します。

   > **注：**
   > Data Protectorアプリケーションリソースは、マウント および仮 想 サーバーIPリソースに依 存 するようにします。

4. Data Protectorアプリケーションリソースを有 効 にし、起 動します。

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 Symantec Veritas Cluster Server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システム用 のインストールサーバーのインストール、ページ 42。

> **注 :**
> プライマリノードをクラスター対 応 Cell Managerとして構 成 する前 に、インストールサーバーをインスト ールする場 合 、インストールサーバーが、各 2次 クラスターノードにインストールされていることを確 認します。プライマリノードの構 成 中 、インストールサーバーが、仮 想 サーバー名 を使 ってインポー トされます。インストールサーバーが各 クラスターノードにインストールされていない場 合 、その仮 想 サーバー名 をインストールサーバーのリストからエクスポートする必 要 があります。さらに、クラスター 対 応 Cell Managerの構 成 が完 了 した後 、対 応 する各 物 理 クラスターノード名 もインポートする必 要 があります。

クラスター対 応 クライアントのインストール

インストール手 順 は、Data Protectorを標 準 構 成 の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 については、Data Protectorクライアントのインストール、ページ 54を参 照 してください。

次 に行 う手 順

インストールが完 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場 合 は、仮 想 サーバーをセルにインポートする必 要 があります。
- 物 理 ノードをバックアップする場 合 は、物 理 ノードも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 、ページ 192を参 照 してください。バックアップデバイスとメディアプールの構 成 方 法 、または追 加 のData Protector構 成 タスクについては、*HPE Data Protector*ヘルプのキーワード「構 成 」で表 示 される内 容 を参 照 してください。

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は、https://softwaresupport.hpe.com/manualsの最 新 のサポート一 覧 を参 照 してください。

> **注 :**
> 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にクラスター機 能 が適 切 に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_HPDP_AS、OBVS_HPDP_IDB、OBVS_HPDP_IDB_CP、OmniBack_Share。

  これらの名 前 は、Data Protector仮 想 サーバーで使 用 されます。こ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ー]**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ターリソースが定 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 したフォルダーにインストールします。

  Windows Server 2008、Windows Server 2012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 フォルダーの下 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 したフォルダーの下 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 する手 順 については、クラスターのドキュメントを参 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に対 しては、ファイルクラスターリソース 依 存 関 係 の一 部 として、IP Address、Network Name、およびPhysical Diskを設 定 しておくこと。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 フォルダーへのアクセス権 (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)が実 行 中 で、適 切 に機 能 していることを確 認 してください。
- Windows Server 2008またはWindows Server 2012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またはWindows Server 2012上 で実 行 するMicrosoftサーバークラスターの準 備 、ページ 347」で説 明 されている手 順 を実 行 します。

考 慮 事 項

- ファイルクラスターリソースの共 有 フォルダーに直 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 する必 要 があり ます。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を正 しく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 します。

- Cell Managerシステムに対する管理者権限を付与します。
- クラスター内のクラスター管理者権限
- 無期限のパスワード
- サービスとしてログオン
- ユーザーはパスワードを変更できない
- 全時間帯のログオンが可能

> **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。

- Inetサービスで使用するWindowsドメインユーザーアカウントには、すべてのクラスターノードで以下のWindowsオペレーティングシステムのセキュリティポリシー特権が付与される必要があります。
  - 認証後にクライアントを偽装
  - プロセスレベルトークンの置き換え

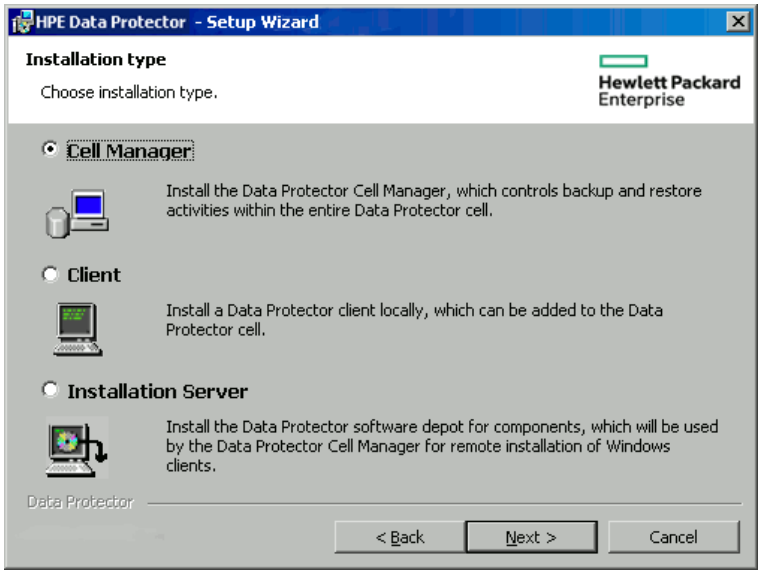
  『*HPE Data Protectorヘルプ*』のキーワード「Inetユーザーの偽装」で表示される内容を参照してください。

ローカルインストール手順

クラスター対応Data Protector Cell Managerは、インストールパッケージ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システムにダウンロードしたインストールパッケージ(zip)をコピーし、ローカルディレクトリに展開します。プラットフォームに適用可能なフォルダーから`setup.exe`ファイルを実行します。
2. セットアップウィザードに従い、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。
3. 終了情報ページで詳細を確認し、サポートされているハードウェアおよびソフトウェアバージョンのリストについて、Data Protectorが行った変更を承認する場合のみ、**[I understand the changes to the supported platforms]**をクリックします。
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。

   インストールの種類の選択

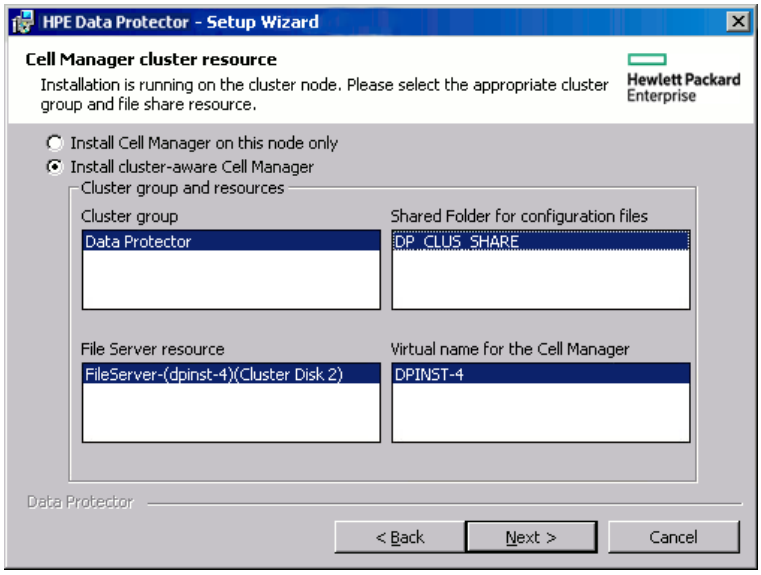


5. セットアップ時に実行環境がクラスター環境かどうかが自動的に検出されるようになっています。**[Install cluster-aware Cell Manager]**を選択して、クラスターセットアップを有効にします。

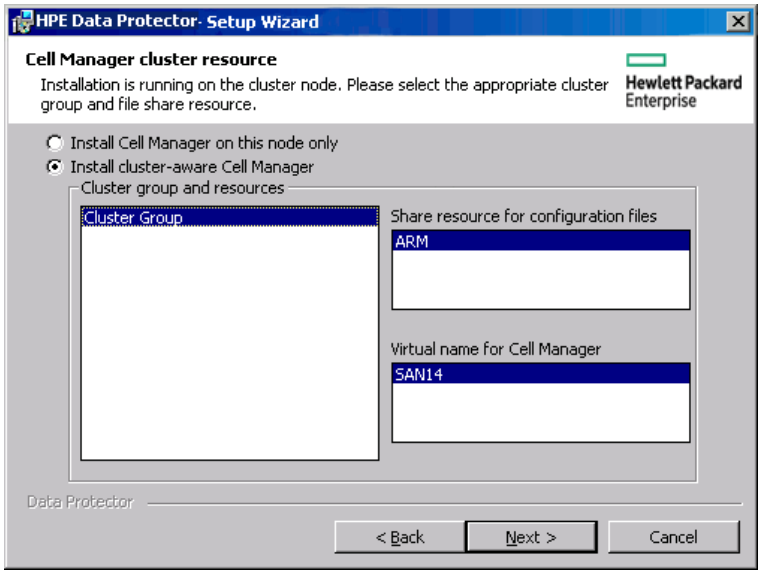
   クラスターグループ、仮想ホスト名と、Data Protectorの共有ファイルおよびデータベースのインストール先となるファイルクラスターリソースを選択します。

> **注 :**
> **[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。「Windows Cell Managerのインストール Cell Manager、ページ 34」を参照してください。

Windows Server 2008でのクラスターリソースの選択

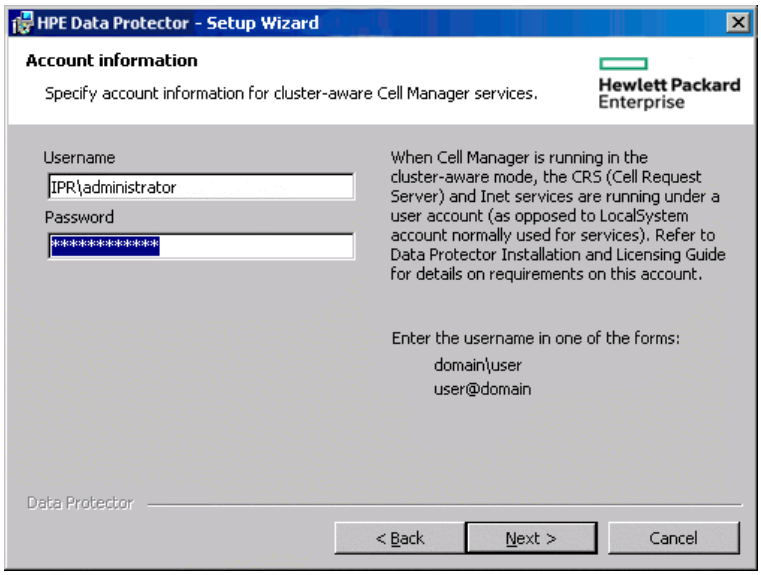


Windowsシステムでのクラスターリソースの選択



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。

   アカウント情 報 の入 力



7. Data Protectorをデフォルト のフォルダーにインストールする場 合 は、**[Next]**をクリックします。

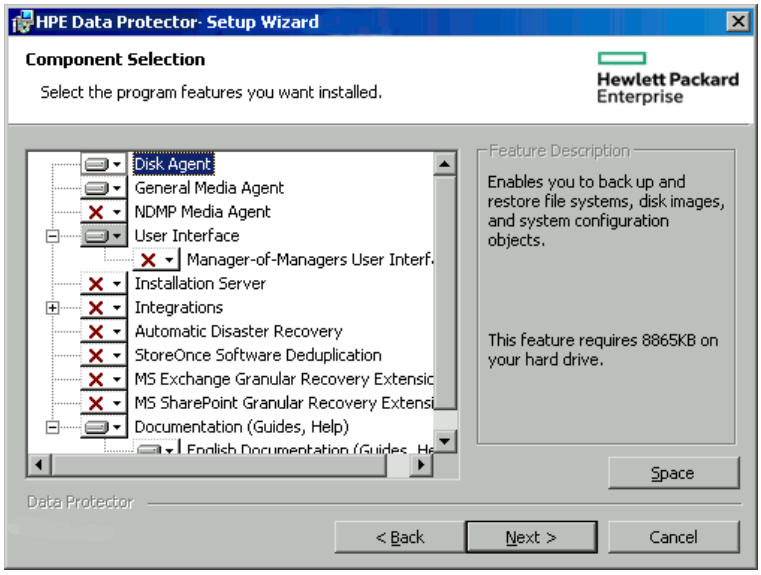
   それ以 外 の場 合 は、**[Change]**をクリックして[Change Current Destination Folder]または[Change Current Program Data Destination Folder]ダイアログボックスを開き、必 要 に応 じてインストールフォルダーを変 更 します。プログラムデータインストールフォルダーへのパスは80文 字 以 内 に制 限 されます。

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。**[次 へ]**をクリックします。

   MS Cluster Supportファイルが自 動 的 にインストールされます。

   選 択 されているコンポーネント がすべてのクラスターノード にインストールされます。

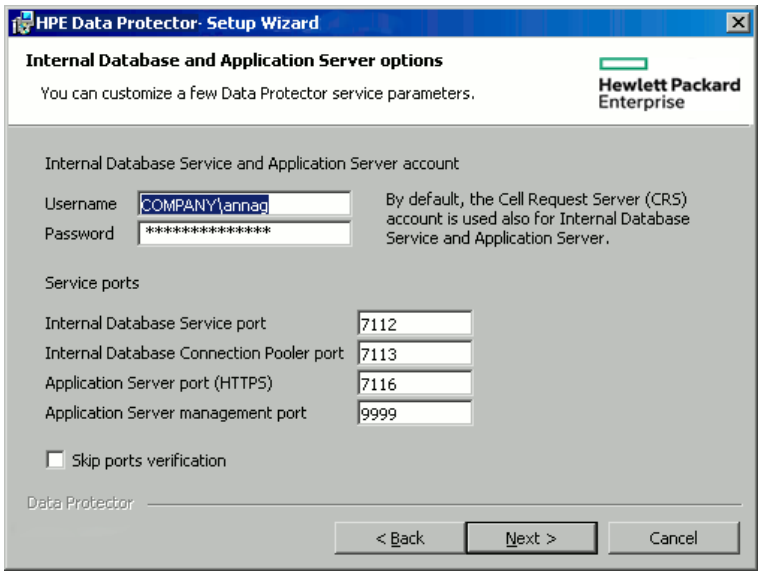
   コンポーネント選 択 ページ



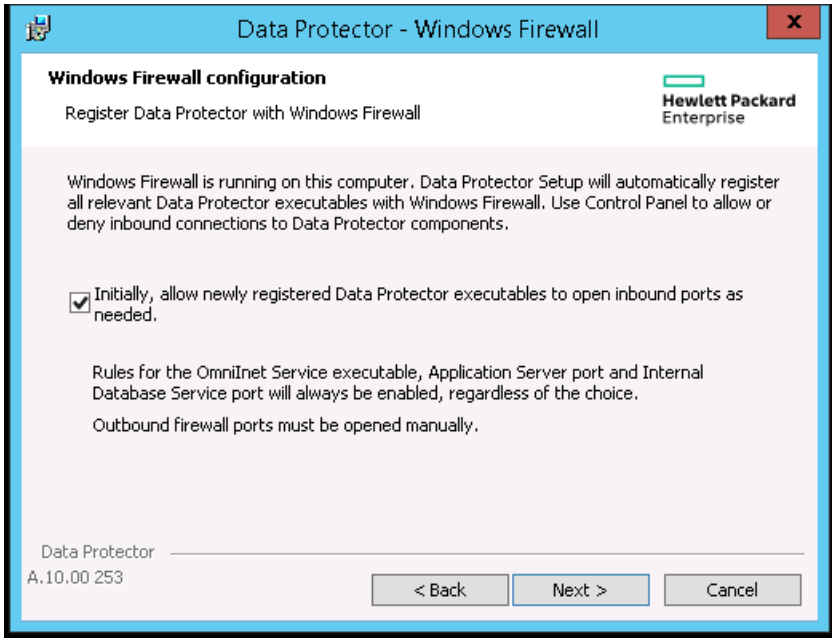
9. また、Data Protectorサービスの内 部 データベースサービスおよびアプリケーションサーバーで使 用 するユーザーカウント やポートも変 更 できます。

   [次 へ]をクリックします。

   IDBおよびアプリケーションサーバーオプションの変 更



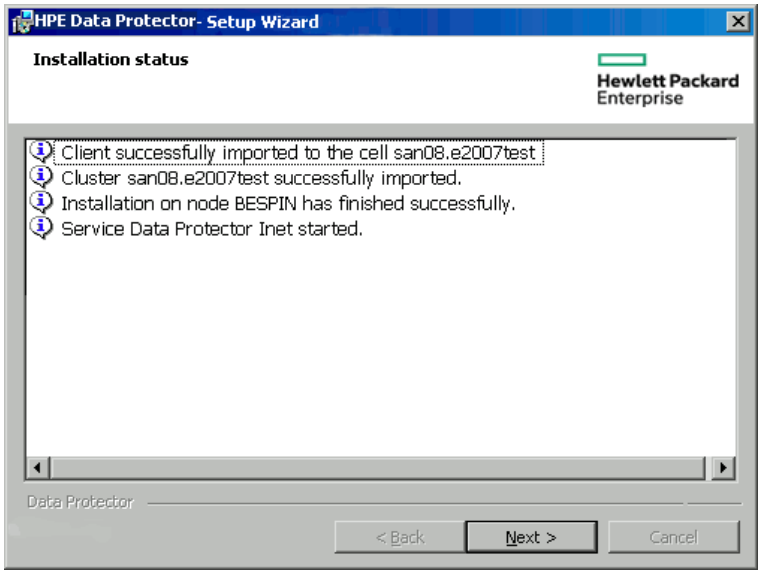
10. システムにWindows Firewallが検 出 された場 合 、Windows Firewallの構 成 ページが表 示 されます。Data Protectorセットアップでは、すべての必 要 なData Protector実 行 可 能 ファイルが記 録 されます。デフォルト では、**[Initially, allow newly registered Data Protector executables to open inbound ports as needed]**オプションが選 択 されています。この時 点 で、Data Protectorによってポート がオープンされないようにするには、オプションを選 択 解 除 します。Data Protectorが以 前 のバージョンの10.00クライアント で適 切 に機 能 するには、WindowsファイアウォールのData Protectorルールを有 効 にする必 要 があります。OmniInetサービス実 行 可 能 ファイル、アプリケーションサーバーポート、内 部 データベースポート のルールは、選 択 内 容 にかかわらず常 に有 効 になります。



[次 へ]をクリックします。

11. 選 択コンポーネントのサマリーページが表 示されます。**[Install]**をクリックします。
12. [Installation setup]ページが表 示されます。**[次 へ]**をクリックします。

    [Installation status]ページ



13. `User Interface`コンポーネントをインストールした場 合 に、セットアップ直 後 にData Protector GUIを使 用して操 作を開 始するには**[Launch Data Protector GUI]**を選 択します。

    `English Documentation (Guides, Help)`コンポーネントをインストールした場 合 に、セットアップ直 後 にHPE Data Protector製 品 案 内 、ソフトウェアノート、およびリファレンスを表 示するには、**[Open the Product Announcements, Software Notes, and References]**を選 択します。
14. **[Finish]**をクリックしてインストールを完 了します。

Windows 2012 および Windows 2012 R2 クラスター用 のクラスター対 応 Cell Manager のインストール

クラスター対 応 Cell Managerをインストールするには

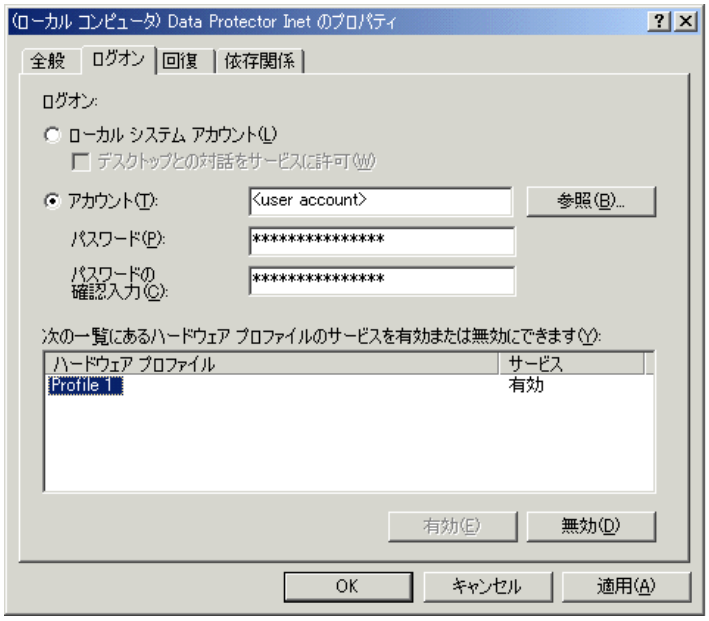
1. Data Protectorインストールサーバーをクラスターに含 まれていないマシンにインストールします。
2. 最 新 のパッチを適 用します。インストールサーバーの‘\DP_Program_data\Depot’内 のデポを使 用して、Windows 2012および2012 R2システムにクラスター対 応 Cell Managerをインストールすることができます。
3. 任 意 のクラスターノードにデポをコピーし、ローカルディスクからインストールを開 始します。
4. または、ネットワーク共 有 を使 用してデポにアクセスし、共 有 からインストールを開 始します。この手 順 では、以 下 のことを考 慮 する必 要 があります。
   - インストールサーバーは、クラスターと同じドメインに置 かれている必 要 があります。
   - 管 理 (非 表 示 の)共 有 (\\hostname or IP address of IS\c$\...)は、他 のクラスターノードからアクセスできない場 合 があるので、使 用しないでください。そのため、通 常 のパス(\\hostname or IP address of IS\depot)を使 用し、すべてのノードで共 有 する必 要 があります。
   - クラスターノードは、パスワードを指 定 せずに通 常 のネットパスにアクセスできる必 要 があります。
   - 通 常 のネットパスは、資 格 情 報 を指 定 せずにブラウザーからアクセスできる必 要 があります。資 格 情 報 が求 められた場 合 は、それらを入 力し、[Remember Credentials]を選 択します。

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 を実 行します。

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、Data Protectorユーザーアカウント、下 で示 すように、[This account]に設 定 する必 要 があります。

   Data Protectorユーザーアカウント



2. 次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`サービスおよび`CRS`サービスを実行しているアカウントを変更します。

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にクラスター機能が適切に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またはWindows Server 2012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またはWindows Server 2012上で実行するMicrosoftサーバークラスターの準備、ページ 347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

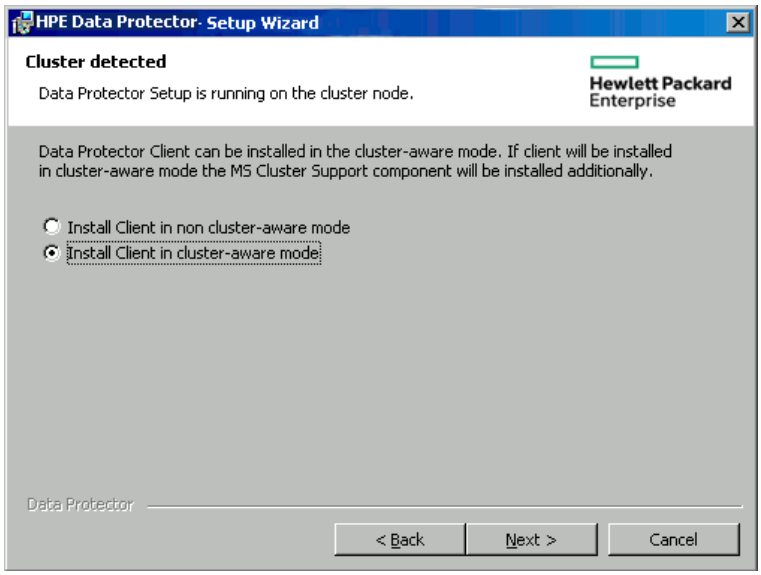
クラスター対応 Data Protectorクライアントは、各クラスターノードで、インストールパッケージからローカルにインストールする必要があります。クラスターノード(Data Protectorクラスタークライアント)は、インストールプロセス中に指定したセルにインポートされます。その後、仮想サーバー名をインポートする必要があります。

インストールを実行する際には、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ファイルが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の詳細については、「Windowsクライアントのインストール、ページ 62」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。**[Install client in cluster-aware mode]**を選択します。

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 :**
> クラスター対応クライアントは、標準のData Protectorが管理する、またはクラスター対応のCell Managerが管理するCell Managerセルのどちらにでもインポートできます。

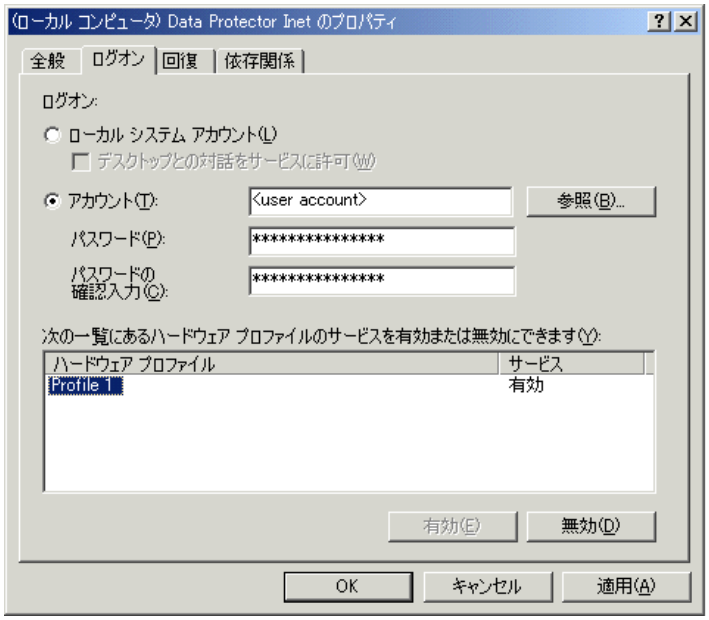
インストールのチェック

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。以下の手順を実行します。

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、Data Protectorユーザーアカウント 、下 で示 すように、**[アカウント]**に設 定する必 要 があります。

Data Protectorユーザーアカウント



2. 以 下を実 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、ページ 349」を参 照してください。

次 に行う手 順

インストールが完 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 、ページ 192」を参 照してください。

バックアップデバイスとメディアプールの構 成 方 法 、または追 加 のData Protector構 成 タスクについては、*HPE Data Protector*ヘルプのキーワード「構 成 」で表 示される内 容を参 照してください。

Inetアカウントとクラスターアカウントの変 更

必 要 に応じて、Data Protector `Inet`サービスおよび`CRS`サービスを実 行しているアカウントを変 更します。

Data ProtectorのIBM HACMPクラスターへのインストール

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、リモートインストール、ページ 94またはUNIXおよびMac OS Xシステムでのローカルインストール、ページ 102を参照してください。

次に行う手順

インストールが終了したら、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、ページ 192を参照してください。

バックアップデバイスとメディアプールの構成方法、または追加のData Protector構成タスクについては、『*HPE Data Protectorヘルプ*』のキーワード「構成」で表示される内容を参照してください。

Microsoft Hyper-VクラスターでのData Protectorのインストール

Microsoftフェールオーバークラスタリング機能を使用するクタスター内で構成したMicrosoft Hyper-VシステムにData Protectorをインストールする手順は、Data ProtectorをMicrosoft Cluster Serverにインストールする手順に類似しており、Microsoft Hyper-VシステムはData Protectorクラスター対応クライアントとして構成する必要があります。詳細は、Microsoft Cluster ServerへのData Protectorのインストール、ページ 178を参照してください。

> **注:**
> Microsoft Hyper-Vシステムをクラスター対応クライアントとして構成すると、追加のData Protectorコンポーネントをインストールサーバーでリモートインストールできるようになります。

第6章: インストールの保守

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。

- 保守モードを使用する方法と使用のタイミング
- グラフィカルユーザーインターフェイ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
- グラフィカルユーザーインターフェイ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
- グラフィカルユーザーインターフェイ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
- グラフィカルユーザーインターフェイスを使用してクライアントをエクスポートする方法
- グラフィカルユーザーインターフェイスを使用して保護を設定する方法
- Data Protectorでユーザー認証用にLDAPを構成する方法
- 証明書生成ユーティリティを使用する方法と使用のタイミング
- Data Protectorパッチバンドルを管理し、インストールしたData Protectorパッチを識別する方法
- Data Protectorソフトウェアをアンインストールする方法
- 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

Data Protector保守モード

Cell Managerで保守タスクを実行する場合、Data Protectorは保守モードに入る必要があります(この間、内部データベースへの書き込み操作は避けてください)。このようなタスクには、Data Protectorインストールのアップグレードや、パッチと重要な修正プログラムのインストール、ハードウェアまたはオペレーティングシステムのアップグレードがあります。保守モードは、この章で説明する特定の手順に対してのみ必要ですが、他の章で説明するタスクに対しても適用されます。

保守モードに入るプロセスを実行すると、スケジューラーの停止やバックアップ仕様ディレクトリの名前変更、実行中のプロセスの中止、ロックされたリソースの解放などの一連のタスクが自動的に開始されます。保守モードは、個々のセル、およびMoMとクラスター環境でサポートされています。

保守モードの開始

保守モードは、管理者権限を持つユーザーがコマンドラインインターフェイスを使用して開始できます。保守モードを開始するには、以下を実行します。

個々のセルの場合:

```
omnisv -maintenance [GracefulTime]
```

MoM環境の場合:

```
omnisv -maintenance -mom
```

実行中のセッションはCell Managerによって同時にすべてを停止するように指示されますが、MoM環境内のセルは個別に保守モードに入ります。

Cell Managerが保守モードに入る方法をカスタマイズするには、適切なグローバルオプションを変更します。MaintenanceModeGracefulTimeオプションは、実行しているセッションを中止するためにData Protectorサービスに指定された秒数を示しますが、MaintenanceModeShutdownTimeオプションは、セッションが中止するまでに待機する秒数を示します。両方のオプションのデフォルト値は300です。*GracefulTime*オプションを使用すると、MaintenanceModeGracefulTimeグローバルオプションより優先されます。このオプションの値を超えてもまだ復元セッションが実行されていると、保守モードの開始が失敗します。

MoM環境内のセルが保守モードに入ることができないと、保守モードは元の状態に戻ります。

Data Protectorが保守モードで実行されているかをチェックするには、omnisv -statusを実行してCRSサービスのステータスを確認するか、GUIステータスバーをチェックしてください。GUIが保守モードであることを正確に示すことができるのはCell Managerに接続しているときのみです。Cell Managerは通常のモードに切り替わった後もステータスバーに保守モードを示す場合があるので注意してください。

保守モード中、Cell Managerは、新しいデバイスの作成、バックアップと復元セッションまたはそれらのプレビュー、削除、コピー、集約セッションなどのIDBへのデータ書き込みを行うすべての操作を拒否します。

クラスター環境では、保守モードがアクティブな場合、クラスターパッケージのシャットダウンやData Protectorサービスの停止、手動によるボリュームのマウントなど、手動クラスター関連アクティビティしか実行できません。

保守モードがアクティブな場合、読み取り専用IDB操作すべてを実行できます。Data Protectorサービスはすべて正しく動作します。Cell Managerが保守モードである間、セルまたはMoMに接続できるのはData Protectorの管理者権限を持つユーザーだけです。

保守モードの終了

Cell ManagerでCLIを使用して保守モードを終了するには、以下を実行します。

- 個々のセルの場合:

  ```
  omnisv -maintenance -stop
  ```

- MoM環境の場合:

  ```
  omnisv -maintenance –mom_stop
  ```

MoM環境では、個々のセルは保守モードを終了できません。MoMの保守はMoMサーバーからしか起動できません。

GUIを使用して保守モードを終了するには、以下を実行します。

1. コンテキストリストで、**[クライアント]**を選択します。
2. **[アクション]**メニューの**[保守モードの停止]**をクリックします。

通常モードが再開したら、中止されたセッションと拒否されたセッションを再起動できます。これらは、デフォルトのData Protectorログファイルディレクトリにあるmaintenance.logファイルに記録されています。

次の2つの例では、中止されたセッションと拒否されたセッションのmaintenance.logエントリを示しています。

```
10.5.2013 10:52:45  OMNISV.2492.9936
["/cli/omnisv/omnisv.c $Rev: 22709 $ $Date:: 2013-03-22 18:00:03":247] X.99.01 b2
Session was aborted - graceful period expired!
session id:        2013/05/10-8
session type:      0
```

```
datalist:          large_backup
start date:        2013-05-10 10:52:45
owned by:          JOHN.JOHNSON@company.com

10.5.2013 10:48:45  CRS.7620.3308 ["/cs/mcrs/sessions.c $Rev: 22709 $ $Date:: 2013-
03-22 18:00:03":142] X.99.01 b2
CRS is in maintenance mode - session rejected
session id:        R-2013/05/10-200
session type:      dbsm
session desc:      Database
start date:        2013-05-10 10:48:45
owned by:          .@ pid=0
```

保守モードがアクティブであった場合にセッションの開始を試みると、セッションは「中止されたセッション」として記録されます。中止されたセッションを後で実行するには、以下を実行します。

1. コンテキストリストで**[内部データベース]**をクリックします。
2. Scopingペインで**[セッション]**を展開します。
3. セッションを右クリックして、コンテキストメニューから**[失敗したオブジェクトの再開]**を選択します。

Cell Managerが保守モードに入っている場合にセッションの開始を試みると、セッションは「拒否されたセッション」として記録されます。拒否されたセッションを後から実行する場合は、手動で各セッションを再起動します。

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

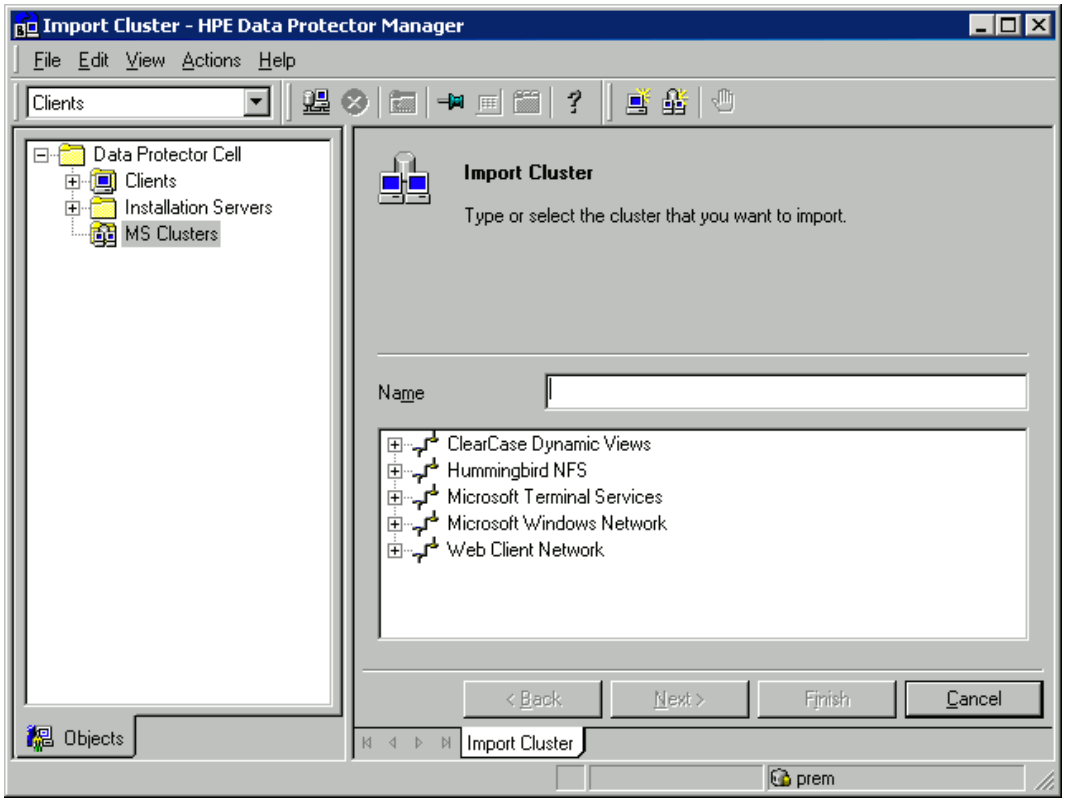
- すべてのクラスターノード上にData Protectorがインストールされていること。
- クラスター内ですべてのクラスターパッケージが実行されていること。

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

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。

   セルへのMicrosoft Cluster Serverクライアントのインポート



4. **[次へ]**をクリックします。
5. **[完了]**をクリックしてクラスター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。

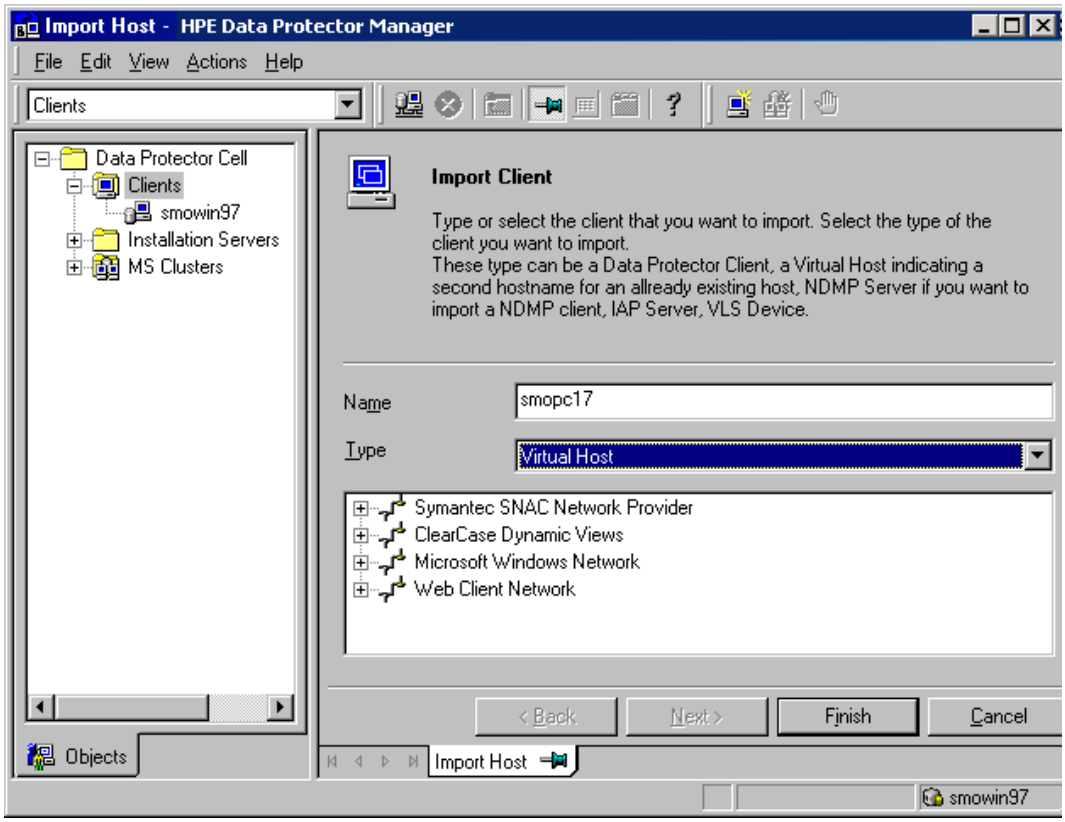
その他のクラスター

HPE Serviceguard、Veritas、またはIBM HACMPクラスター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

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. 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仮想サーバーのホスト名を入力するか、ネットワークをブラウズして、インポートする仮想サーバーを選択します(Windows GUIの場合のみ)。

   [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。

HPE ServiceguardまたはVeritasクライアントのセルへのインポート



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。

> **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。

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とは、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、クライアントへの参照をCell ManagerのIDBから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。
- ライセンシングに関連する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。

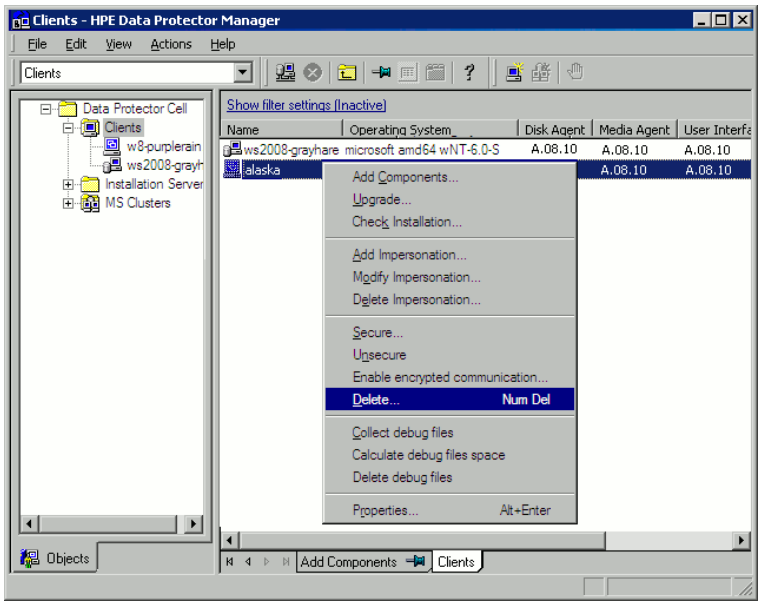
- 存在するすべてのクライアントがバックアップ仕様から削除されていること。削除されていない場合、Data Protectorは不明なクライアントのバックアップを実行しようとするため、バックアップ仕様のこのシステムに対応する部分が正常に実行されません。バックアップ仕様の変更方法については、『*HPE Data Protectorヘルプ*』のキーワード「変更、バックアップ仕様」で表示される内容を参照してください。
- クライアントに接続済みおよび構成済みのバックアップデバイスやディスクアレイが存在しないこと。システムのエクスポートが完了すると、Data Protectorは元のセル内のバックアップデバイスやディスクアレイを使用できなくなります。

クライアントをエクスポートする

Data Protector GUIを使ってクライアントをエクスポートするには

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。

   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：**
> 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クライアントのエクスポートまたは削除はできません。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

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。

セキュリティの留意事項

ここでは、Data Protectorのセキュリティ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。

環境全体のセキュリティを強化するには追加作業が必要なため、多くの機能は、デフォルトで有効にすることができません。

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、クライアントを追加する場合、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。

クライアントのセキュリティ

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ーや複数の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、ほかにも考慮すべき事項が存在することがあります。

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、他のクライアントから信頼される以下のようなコンピューターについては、セキュリティの強化が重要です。

- Cell Manager / Manager-of-Managers
- インストールサーバーs
- Media Agentクライアント

> **注:**
> ユーザーインターフェイスクライアントは、信頼でき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。
- あまり強力ではないユーザー権限でも、その権限に関連するリスクを内包しています。Data Protectorでは、特定のユーザー権限を制限して、このようなリスクを軽減するように構成できます。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、ページ 200」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環境のユーザーの種類ごとに特定のグループを定義して、最小限の権限だけをユーザーに割り当てるようにすることをお勧めします。
- ユーザー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。詳細については、『*HPE Data Protector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(厳密なホスト名チェック、次のページを参照)。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ありません。反対に、細心の注意を払ってユーザーを構成してもユーザーのチェックを強化しないとうまくいきません。
- Data Protectorのユーザーリストに「脆弱な」ユーザーが存在しないようにすることが重要です。

> **注:**
> 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の管理に使用する特定のクライアントに対して構成する必要があります。複数のクライアントを使用する場合は、そのユーザーをユーザー、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、『*HPE Data Protectorヘルプ*』のキーワード「構成、ユーザー」で表示される内容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Cell Manager護は重要です。

Cell Managerの保護は、厳密なホスト名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、他のクライアントから信頼されるコンピューターについては、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。

詳細については、『厳密なホスト名チェック、下』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

ほかにも、以下のように、考慮する必要のあるセキュリティ関連の要素がいくつかあります。

- ユーザーが信頼できるクライアント(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。anonymous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、またはカスタム暗号化ライブラリを使用します。暗号化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。

その他セキュリティ関連の内容については、『*HPE Data Protectorヘルプ*』と『*HPE Data Protectorコンセプトガイド*』を参照してください。

厳密なホスト名チェック

デフォルトでは、Cell Managerによって、比較的簡単な方法を使ってユーザーのチェックが行われます。この方法では、ユーザーインターフェイスまたはApplication Agentを起動しているクライアントが認識できるホ

スト名が使用されます。この方法は、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、厳密なホスト名チェックの設定を使用すると、ユーザーのチェックが強化されます。このチェックでは、Cell Managerで接続から取得したIPを基にDNS逆引きを行ってホスト名を解決し、そのホスト名を使用します。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。
- ユーザー仕様内で使用されているホストは、固定IPが割り当てられていてDNSで構成されている場合を除き、DHCPを使用するように構成できません。

厳密なホスト名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

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

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

この設定で有効になるチェックの特性により、Data Protectorユーザーを再構成する必要があることがあります。既存のData Protectorユーザーの仕様をチェックして、上記のいずれかの理由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、厳密なホスト名チェックを有効にするときにユーザー仕様を変更する必要があった場合は、デフォルトのユーザーチェックに戻すときにユーザーを再構成する必要があります。そのため、継続的に使用するユーザーチェックを事前に決定することをお勧めします。

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

ホスト名の代わりにIPを使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、SYSTEM、NT AUTHORITY、*クライアント*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。詳細については、『*HPE Data Protectorヘルプ*』のキーワード「厳密なホスト名チェック」で表示される内容を参照してください。

ユーザーを構成する方法の詳細については、*HPE Data Protectorヘルプ*のキーワード「構成、ユーザー」で表示される内容を参照してください。

機能を使用可能にする

厳密なホスト名チェックを有効に設定するには、StrictSecurityFlagsグローバルオプションを0x0001に設定します。

グローバルオプションの詳細については、『*HPE Data Protectorトラブルシューティングガイド*』を参照してください。

[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については、*HPE Data Protectorヘルプ*のキーワード「ユーザー」で表示される内容を参照してください。

[Start backup specification]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:**
> [Start Backup Specification]を[Start Backup]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。バックアップ仕様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、StrictSecurityFlagsグローバルオプションを0x0200に設定します。

グローバルオプションの詳細については、『*HPE Data Protectorトラブルシューティングガイド*』を参照してください。

バックアップ仕様の内容にアクセスできないようにする

セキュリティの高い環境では、保存されているバックアップ仕様の内容が重要な情報または機密情報として扱われることがあります。Data Protectorは、[Save backup specification]ユーザー権限を持つユーザーを除き、すべてのユーザーがバックアップ仕様の内容にアクセスできないように構成できます。これを行うには、StrictSecurityFlagsグローバルオプションを0x0400に設定します。

グローバルオプションの詳細については、『*HPE Data Protectorトラブルシューティングガイド*』を参照してください。

ホストの信頼

ホスト信頼機能を使用すると、少数のクライアント間で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。そのデータを使用する信頼関係のあるホストのグループを定義できます。

ホストの信頼は、通常、以下のような場合に使用します。

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

ホストの信頼を構成するには、Cell Managerでファイル*Data_Protector_program_data*\Config\Server\cell\host_trusts(Windowsシステム)または/etc/opt/omni/server/cell/host_trusts(UNIXシステム)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。例:

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、Data Protectorのデフォルトのログファイルディレクトリにある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。

Cell Manager保護イベント

Cell Managerの保護イベントは、Data Protectorサーバーのデフォルトのログファイルディレクトリにある`security.log`ファイルに記録されます。

ユーザー認証とLDAP

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

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

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

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

1. LDAPログインモジュール: 既存のLDAPサーバーに対して、ユーザー名とパスワードなどのユーザーの資格情報を認証します。「LDAPログインモジュールを初期化して構成する」を参照してください。
2. Data Protector ログインモジュール: Data Protectorユーザーリストと Webアクセスパスワードに対してユーザー資格情報を認証します。「Data Protectorの権限をLDAPユーザーまたはグループに付与する」を参照してください。
3. LDAPの初期化と構成に必要なすべての手順を実行すると、構成もチェックできます。「LDAP構成をチェックする」を参照してください。

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

LDAPログインモジュールを初期化して構成する

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

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

LDAPログインモジュールを初期化する

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

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

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

```
<security-domain name="hpdp-domain">
<authentication>
<login-module code="LdapExtended" flag="optional">
<module-option name="java.naming.factory.initial"
value="com.sun.jndi.ldap.LdapCtxFactory"/>
<module-option name="java.naming.security.authentication" value="simple"/>
<module-option name="roleFilter" value="(member={1})"/>
<module-option name="roleAttributeID" value="memberOf"/>
<module-option name="roleNameAttributeID" value="distinguishedName"/>
<module-option name="roleAttributeIsDN" value="true"/>
<module-option name="searchScope" value="SUBTREE_SCOPE"/>
<module-option name="allowEmptyPasswords" value="true"/>
<module-option name="password-stacking" value="useFirstPass"/>
</login-module>
<login-module code="com.hp.im.dp.cell.auth.DpLoginModule" flag="required">
<module-option name="password-stacking" value="useFirstPass"/>
</login-module>
</authentication>
</security-domain>
```

> **注:**
> このコマンドラインによってstandalone.xml構成ファイル内に生成されるデフォルト値は、Cell

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

2. Cell Manager上に置かれているWildFly管理コンソールにリモートクライアントからアクセスするには、WildFly管理コンソールへのリモートアクセスを有効にする必要があります。これを行うには、テキストエディターを使用して、以下のように`standalone.xml`ファイルのインターフェイスセクション内の管理インターフェイスのバインドアドレスを127.0.0.1から0.0.0.0に変更します。

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

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

3. 以下を使用してData Protectorサービスを再起動します。

```
omnisv stop
omnisv start
```

LDAPログインモジュールの構成

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

1. WildFly管理コンソールにアクセスするには、WildFlyユーザーを作成します。WildFlyユーザーを作成するには、add-userユーティリティを実行します。
   - **Windowsの場合**: `add-user.bat` 場所: `%Data_Protector_home%/AppServer/bin`
   - **UNIXの場合**: `add-user.sh` 場所: `/opt/omni/AppServer/bin`
2. 次のパラメーターを入力します。
   - **Type of user to add**: [Management User]を選択します。
   - **Realm**: ユーティリティによってデフォルト値のManagementRealmが選択されているため、このフィールドは空白のままにします。
   - **Username**: ユーザー名を追加します。
   - **Password**: パスワードを追加します。
   - **Group**: なし。
3. WildFly管理コンソールにアクセスするには、ブラウザーで次のURLを開きます。<http://cell-manager-name:9990/console>
4. [認証]画面で、add-userユーティリティを使用して作成した**ユーザー名**と**パスワード**を指定します。
5. **[ログイン]**をクリックします。WildFlyアプリケーションサーバーの管理コンソールが表示されます。
6. WildFly管理コンソールで、**[プロファイル]**タブを選択します。
7. **[プロファイル]**タブで、**[セキュリティ]**ノードを展開し、**[セキュリティドメイン]**をクリックします。
8. 登録済みのセキュリティドメインのリストで、hpdp-domainの**[表示]**をクリックします。セキュリティドメインhpdp-domainに対して、次のログインモジュールが定義されています。
   - LdapExtended
   - Com.hp.im.dp.cell.auth.DpLoginModule

9. **LdapExtended**モジュールを選択します。
10. [詳細]セクションで、**[モジュールオプション]**タブをクリックします。構成済みのすべてのモジュールオプションが**[モジュールオプション]**タブに表示されます。
11. LDAPログインモジュールをカスタマイズして使用するには、他のモジュールオプションを追加する必要があります。**[追加]**をクリックして、各モジュールオプションの**[名前]**と**[値]**を指定します。詳細については、次の表を参照してください。

モジュールオプション	名前	値	説明
プロバイダーURL	java.naming.provider.url	LDAPサーバーのURLを次の形式で指定します。ldap://<server>:<port>	標準プロパティ名
基本コンテキスト識別名(DN)	baseCtxDN	ユーザーが格納されているLDAPの場所のDNを指定します。	ユーザー検索の開始場所となるコンテキストの固定DN
基本フィルター	baseFilter	ユーザーのログイン名に一致するLDAPセットアップの属性を次の形式で指定します。((<user-login-name-attribute>={0}))。<user-login-name-attribute>は、対応するLDAP属性名に置き換える必要があります。	認証対象のユーザーのコンテキストを検索するために使用する検索フィルター
役割コンテキストDN	rolesCtxDN	ユーザーグループが格納されているLDAPの場所のDNを指定します。	ユーザーグループを検索するためのコンテキストの固定DN
バインドDN	bindDN	ログインモジュールが最初のLDAPバインドを実行するために使用するLDAPユーザーのDNを指定します。ユーザーとグループのLDAP場所を検索してユーザーとユーザーグループを取得するために、必要な権限を持っている必要があります。これらの場所は、baseCtxDN と rolesCtxDN モジュールオプションで定義されます。	ユーザーと役割を問い合わせるためにLDAPサーバーに対してバインドするために使用されるDN。これは、baseCtxDN と rolesCtxDN 値に対する読み取り/検索権限を持つDNです。
バインド資格情報	bindCredential	BindDNモジュールオプションで入力したLDAPユーザーのパスワードを指定します。	bindDNのパスワード。

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

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

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

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

Data Protectorパーミッションの LDAPユーザーまたはグループへの付与

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

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

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

LDAPユーザーのユーザーグループへの追加

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

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

- **エンティティ**: LDAPユーザーを入力します。
- **説明**: これは省略可能です。

5. **[完了]**をクリックしてウィザードを終了します。

LDAPグループのユーザーグループへの追加

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

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

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

LDAP資格情報を使用したログイン

LDAP資格情報を使用してログインするには、以下の手順に従ってください。

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

LDAP構成のチェック

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

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

1. ブラウザーを使用してData Protectorログインプロバイダーの`Web`サービスに接続します。
2. ブラウザー上にサーバー証明書の承認を求めるメッセージが表示される場合があります。**[承認]**をクリックして要求を確認します。

3. ログイン資格情報の入力を求めるダイアログボックスが表示されます。Data Protectorを使用して設定した有効なLDAPユーザー名とパスワードを入力します。LDAPログインモジュールの構成を参照してください。
4. ブラウザーから次のACL (アクセス制御リスト)が返されます。`https://<server>:7116/dp-loginprovider/restws/dp-acl`
5. このACLを使用して、割り当てられている権限が、対応するData Protectorユーザーグループに指定されているData Protectorユーザー権限に一致しているかどうかを確認します。

証明書生成ユーティリティ

X.509証明書生成ユーティリティ(`omnigencert.pl`)によって、証明機関(CA)、サーバー、クライアントの各証明書が生成されます。このユーティリティは、以下の作業を実行します。

- 第1層のルートCAを設定する
- CA、サーバー、クライアントの各証明書を生成する
- キー、証明書、構成、キーストアファイルを格納するために必要なディレクトリ構造を作成する
- CM上の定義済みの場所に生成された証明書を格納する
- Webサービスの役割のプロパティファイルを生成する

> **注:** `omnigencert.pl`ユーティリティは、管理者ユーザー(Windows)またはルートユーザー(UNIX)しか実行できません。

`omnigencert.pl` ユーティリティはスクリプトとして開発され、Cell Manager(CM)インストールキットとともにインストールされます。CMのインストールの一環としてスクリプトが初めて実行され、証明書が生成され、定義済みの場所に保存されます。

`omnigencert.pl` スクリプトは以下の場所に格納されます。

Windowsの場合: `%Data_Protector_home%\bin`

Unix:`/opt/omni/sbin`

Data Protector管理者は、必要に応じてインストール後いつでもこのユーティリティを実行して、新しいキーペア、または新しいCAセットアップを使用して証明書を再生成できます。ただし、証明書ベースの認証では、このユーティリティによって生成された証明書を必ずしも使用する必要はありません。代わりに、必要な証明書を生成するための既存のCAセットアップを使用できます。

構文

このユーティリティはCell Managerのインストールの一環としてインストーラーによって最初に実行され、必要な証明書が生成され、事前に定義された場所に格納されます。

このユーティリティを使用できるのは管理者に限られており、新規のCAセットアップも含め、新しいキーペアを使用して証明書を再生成するのにもこのユーティリティを使用します。Windowsプラットフォーム上の'Administrator'ユーザーおよびUNIXプラットフォーム上の'root'ユーザーはこのスクリプトを実行できます。

`omnigencert.pl` スクリプトは以下の場所に格納されます。

Windowsの場合: `%Data_Protector_home%\bin`

UNIX: /opt/omni/sbin

omnigencert.plユーティリティは、次の構文およびオプションを使用して実行できます。

使用法

[-no_ca_setup]

[-server_id ServerIdentityName]

[-user_ID UserIdentityName]

[-store_password KeystorePassword]

[-cert_expire CertificateExpireInDays]

[-ca_dn CertificateAuthorityDistinguishedName]

[-server_dn ServerDistinguishedName]

[-client_dn ClientDistinguishedName]

[-server_san]

omnigencert.plユーティリティでは複数のオプションがサポートされていて、これらのオプションを使用することで、柔軟に証明書を生成できます。オプションを指定しないと、ユーティリティはデフォルト値を使用して証明書を生成します。

omnigencert.pl ユーティリティでは以下のオプションがサポートされています。

オプション	説明
-no_ca_setup	既存のCAセットアップ用のクライアントとサーバーの証明書を生成します。CAセットアップがない場合はこのオプションは無効になります。
-server_id	サーバー証明書の識別名(DN)セクションに共通名(CN)エンティティの値を指定します。このオプションのデフォルト値は、CM完全修飾ドメイン名(FQDN)です。
-user_id	クライアント証明書のDNセクションにCNエンティティの値を指定します。このオプションのデフォルト値はWebService Userです。
-store_password	キーストアまたは信頼ストアのパスワードを定義します。キーストアまたは信頼ストアにはサーバーとクライアントの各証明書、およびそれらのキーが格納されます。このオプションを指定しないと、ストアを作成する際にデフォルトのパスワードが使用されます。
-cert_expire	生成された証明書の有効期限(日数)を定義します。このオプションのデフォルト値は8760日(24年間)です。
-ca_dn	CAのDN文字列を定義します。DN形式は次のと

オプション	説明
	おりです。"CN=<値>, O=<値>, ST=<値>, C=<値>" CN = 共通名, O=組織の名前, ST=州名, C=国名。O、ST、Cパラメーターのデフォルト値は、次のとおりです。CN = CA <CMサーバーのFDQN名> O = HEWLETT-PACKARD ST = CA C= US
-server_dn	サーバー証明書のDN文字列を定義します。DN形式は次のとおりです。"CN=<値>, O=<値>, ST=<値>, C=<値>" CN = 共通名, O=組織の名前, ST=州名, C=国名。O、ST、Cパラメーターのデフォルト値は、次のとおりです。CN = <CMサーバーのFDQN名> O = HEWLETT-PACKARD ST = CA C= US
-client_dn	クライアントまたはユーザーの証明書のDN文字列を定義します。DN形式は次のとおりです。"CN=<値>, O=<値>, ST=<値>, C=<値>" CN = 共通名, O=組織の名前, ST=州名, C=国名。O、ST、Cパラメーターのデフォルト値は、次のとおりです。CN = WebServiceのユーザーO = HEWLETT-PACKARD ST = CA C= US

-server_san	サーバー証明書のサブジェクト代替名(SAN)を指定します。ただし、Cell Managerのインストール中に生成されたサーバー証明書には、SANセクションのDNSタイプのエントリがあります。これらのSANエントリは、Cell Managerの使用可能なIP番号に基づいて自動的に生成されます。サーバー証明書のSANエントリのデフォルトの自動生成を上書きするには、証明書生成ユーティリティを使用して証明書を生成する際にこのオプションを指定します。
	
	SANエントリのDNSとIPタイプがサポートされています。
	
	このオプションの値の形式は次のとおりです。
	`santype:value,santype:value`
	
	各SANエントリはカンマで区切られ、次の2つのパートで構成されています。1) SANタイプ、2) SANタイプの値。
	
	例:
	
	`dns:iwf1112056.dprdn.hpe.com、dns:iwf1113456.dprnd.hpe.com`
	
	`ip:15.218.1.100, ip:15.218.1.200, ip:15.218.1.155`
	
	`dns:iwf1112056.dprnd.hpe.com, ip:15.218.1.100`

> **注:**
> このユーティリティでは、次のオプションを組み合わせて使用することはできません。
>
> - -server_idおよび -server_dn
> - -user_id および -client_dn
> - -no_ca_setupおよび -ca_dn.

例

次の項では、WindowsおよびUNIX上でomnigencert.plユーティリティを実行するためのコマンドのサンプルを記載します。

omnigencert.pl スクリプトは以下の場所に格納されます。

Windowsの場合: %Data_Protector_home%\bin

UNIX: /opt/omni/sbin

WindowsおよびUNIXコマンド

タスク	Windowsコマンド	Unixコマンド
CAをセットアップし、デフォルト値を使用してCA、クライアント、サーバーの各証明書を生成するには	%Data_Protector_home%\bin\perl.exe omnigencert.pl	/opt/omni/bin/perl omnigencert.pl
CAをセットアップし、指定した共通名値を使用してCA、クライアント、サーバーの各証明書を生成するには	%Data_Protector_home%\bin\perl.exe omnigencert.pl -server_id <value> -user_id <value>	/opt/omni/bin/perl omnigencert.pl -server_id <value> -user_id <value>
CAをセットアップし、指定したストアパスワードを使	%Data_Protector_home%\bin\perl.exe omnigencert.pl -store_password <value>	/opt/omni/bin/perl omnigencert.pl -store_password <value>

タスク	Windowsコマンド	Unixコマンド
用して CA、クライアント、サーバーの各証明書を生成するには		
CAをセットアップし、指定した証明書の有効期限(日数)を使用して CA、クライアント、サーバーの各証明書を生成するには	%Data_Protector_home%\bin \perl.exe omnigencert.pl -cert_expire <value>	/opt/omni/bin/perl omnigencert.pl -cert_expire <value>
既存のCAセットアップ(インストールの一環で作成されたもの)を使用して、デフォルト値でクライアントとサーバーの各証明書を生成するには	%Data_Protector_home%\bin \perl.exe omnigencert.pl –no_ca_setup	/opt/omni/bin/perl omnigencert.pl –no_ca_setup
CAをセットアップし、指定したDNを使用してCA、クライアント、サーバーの各証明書を生成するには	%Data_Protector_home%\bin \perl.exe omnigencert.pl -ca_dn <value> -server_dn <value> -client_dn <value>	/opt/omni/bin/perl omnigencert.pl -ca_dn <value> -server_dn <value> -client_dn <value>

タスク	Windowsコマンド	Unixコマンド
既存のCAセットアップを使用して、指定したDNでクライアントとサーバーの各証明書を生成するには	%Data_Protector_home%\bin \perl.exe omnigencert.pl -no_ca_setup -server_dn <value> -client_dn <value>	/opt/omni/bin/perl omnigencert.pl -no_ca_setup -server_dn <value> -client_dn <value>
SG-CLUSTER環境で既存のCA証明書を使用してクライアントとサーバーの各証明書を生成するには	1.<DP_DATA_DIR>\Config\client\ components\webservice.propertiesから既存のキーストアパスワードを取得します。 2.<DP_SDATA_ DIR>\server\idb\idb.configから**PGOSUSER**値を取得します。 3.次のようにクラスター 仮想システム名を使用して omnigencert.p lユーティリティを実行します。 %Data_Protector_home%\bin\ perl.exe omnigencert.pl –no_ca_setup -server_id cm_virtual_ name.domain.com -user_id hpdp_so_user -store_password existing_keystor_ passwd	1./etc/opt/omni/client/ components/webservice .propertiesから既存 のキーストアパスワードを取得します。 2. /etc/opt/omni/server/ idb/idb.config.から **PGOSUSER**値を取得します。 3.次のようにクラスター 仮想システム名を使用して omnigencert.pl ユーティリティを実行します。 /opt/omni/bin/perl omnigencert.pl –no_ca_setup -server_id cm_virtual_name.domain.com -user_id hpdp_so_user -store_password existing_keystor_ passwd
SG-CLUSTER環境でCA、クライアント、サーバーの各証明書を生成するには	1. <DP_DATA_ DIR>\Config\client\components\webservice.propertiesから既存のキーストアパスワードを取得します。 2. <DP_SDATA_ DIR>\server\idb\idb.configから**PGOSUSER** 値を取得します。 3.次のようにクラスター	1. /etc/opt/omni/client/components/webservice.propertiesから既存のキーストアパスワードを取得します。 2. /etc/opt/omni/server/idb/idb.configから**PGOSUSER**値を取得します。 3.次のようにクラスター仮想システム名を使用してomnigencert.pl ユーティリティを実行します。 /opt/omni/bin/perl

タスク	Windowsコマンド	Unixコマンド
	仮想システム名を使用して omnigencert.pl ユーティリティを実行します。 %Data_Protector_home%\bin\perl.exe omnigencert.pl -server_id cm_virtual_name.domain.com -user_id hpdp_so_user -store_password existing_keystor_passwd	omnigencert.pl -server_id cm_virtual_name.domain.com -user_id hpdp_so_user -store_password existing_keystor_passwd
特定のCell Managerサーバーに対して、DNSタイプのSANエントリを使用してサーバー証明書を生成するには	%Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_dn iwf11160123.dprnd.hpe.com -server_san "dns:iwf11160123.dprnd.hpe.com,dns:iwf11160123.dp.hpe.com"	/opt/omni/bin/perl omnigencert.pl -no_ca_setup -server_dn iwf11160123.dprnd.hpe.com -server_san "dns:iwf11160123.dprnd.hpe.com,dns:iwf11160123.dp.hpe.com"
特定のCell Managerサーバーに対して、IPタイプのSANエントリを使用してサーバー証明書を生成するには	%Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_dn 15.218.1.100 -server_san “ip:15.218.1.100, ip:15.218.1.101, ip:15.218.1.125, ip:15.218.1.116”	/opt/omni/bin/perl omnigencert.pl -no_ca_setup -server_dn 15.218.1.100 -server_san "ip:15.218.1.100, ip:15.218.1.101, ip:15.218.1.125, ip:15.218.1.116"
特定のCell Managerサーバーに対して、	%Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_dn	/opt/omni/bin/perl omnigencert.pl -no_ca_setup -server_dn iwf111206.dprnd.hpe.com

タスク	Windowsコマンド	Unixコマンド
DNSタイプとIPタイプのSANエントリを使用してサーバー証明書を生成するには	iwf111206.dprnd.hpe.com -server_san "dns: iwf111206. dprnd.hpe.com, iwf111206.hpe.com, ip:15.218.1.100, ip:15.218.1.101, ip:15.218.1.125, ip:15.218.1.116"	-server_san "dns: iwf111206.dprnd .hpe.com, iwf111206.hpe.com, ip:15.218.1.100, ip:15.218.1.101 ,ip:15.218.1.125, ip:15.218.1.116"

ディレクトリ構造

次の項では、証明書の格納先となるディレクトリの一覧を示します。

Windowsディレクトリ	Unixディレクトリ	説明
ProgramData\Omniback\Config\Server\certificates	/etc/opt/omni/server/certificates	CA証明書ファイルcacert.pemが格納されます。このファイルにはCA公開キーが含まれています。
ProgramData\Omniback\Config\Server\certificates\ca	/etc/opt/omni/server/certificates /ca	CAが機能するために必要となる構成、入力、およびその他のファイルが格納されます。
ProgramData\Omniback\Config\Server\certificates\ca\keys	/etc/opt/omni/server/certificates /ca/keys	CA秘密キーファイルのcakey.pemが格納されます。
ProgramData\Omniback\Config\Server\certificates\server	/etc/opt/omni/server/certificates /server	キーストアと信頼ストアの2種類のストアが格納されます。これらのストアは、サーバー証明書とそのキーを保護するためにJavaユーティリティのkeytoolで作成されます。これらのストアは、ストアパスワード

Windowsディレクトリ	Unixディレクトリ	説明
		で保護されています。このディレクトリには次のストアが格納されます。 ca.truststore server.keystore server.truststore
ProgramData\Omniback\Config\Server\certificates\client	/etc/opt/omni/server/certificates /client	キーストアと信頼ストアの2種類のストアが格納されます。これらのストアは、クライアント証明書とそのキーを保護するためにJavaユーティリティのkeytoolで作成されます。これらのストアは、ストアパスワードで保護されています。このディレクトリには次のストアが格納されます。 • client.keystore • client.truststore
ProgramData\Omniback\Config\Server\AppServer	/etc/opt/omni/server/AppServer	このユーティリティによって作成されたプロパティファイルが格納されます。このディレクトリには、次のプロパティファイルとは別に他のファイルも格納されます。 • jce-webservice-roles.properties • dp-webservice-roles.properties

既存の証明書の上書き

CMのインストールの一環としてユーティリティによって生成された既存の証明書を、既存のCAセットアップによって生成された証明書で上書きするには、次のいずれかのオプションを使用してください。

- 既存のキーストアと信頼ストアファイル内の証明書を上書きする
- 新しいキーストアと信頼ストアファイルを作成して証明書を上書きする

> **注: 注記**: 証明書を再生成した場合や、新しい証明書を使用した場合は、CM上でData Protectorサービスを再起動する必要があります。サービスを再起動すると新しい証明書が確実に有効になるので、証明書を使用する操作を実行する前に必ずサービスを再起動してください。

既存のキーストアおよび信頼ストアファイル内の証明書の上書き

既存のキーストアと信頼ストアファイル内の証明書を上書きするには、以下の作業を実施します。

- 既存のサーバーとクライアントのストアファイルを置き換える
- CA証明書を置き換える
- 識別名(DN)文字列を更新する

既存のサーバーとクライアントのストアファイルの置換

既存のサーバーとクライアントのストアファイルを置き換えるには、以下の手順に従ってください。

1. 以下の場所にあるwebservice.propertiesおよびstandalone.xml 構成ファイルから、キーストアと信頼ストアファイルのストアパスワードを取得します。

   Windows

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

   UNIXの場合

   - /etc/opt/omni/client/components/webservice.properties
   - /etc/opt/omni/server/AppServer/standalone.xml

2. 以下の場所にある既存のサーバーとクライアントのストアファイルserver.keystore、server.truststore、client.keystore、およびclient.truststoreから、すべてのエントリを削除します。

   サーバー

   - Windowsの場合: ProgramData\Omniback\Config\Server\certificates\server
   - UNIX:の場合: /etc/opt/omni/server/certificates/server

クライアント

- Windowsの場合: `ProgramData\Omniback\Config\Server\certificates\client`
- UNIXの場合: `/etc/opt/omni/server/certificates/client`

これらの変更を行うには、Java keytoolユーティリティを使用してください。Java keytoolユーティリティは以下の場所にあります。

Windowsの場合: `Program Files\Omniback\jre\bin`

UNIXの場合: `/opt/omni/jre/bin`

3. 生成された証明書をJava keytoolユーティリティを使用して次のストアにインポートします。
   - サーバーとCA証明書を`server.keystore`にインポートする
   - CAとクライアント証明書を`server.truststore`にインポートする
   - CA証明書を`ca.truststore`にインポートする
   - クライアントとCA証明書を`client.keystore`にインポートする
   - CAとサーバー証明書を`client.truststore`にインポートする

CA証明書の置換

既存のCA証明書を置き換えるには、以下の手順に従ってください。

1. 以下の場所にある既存のCA証明書ファイル`cacert.pem`の権限に注意してください。
   - **Windowsの場合**: `ProgramData\Omniback\Config\Server\certificates`
   - **UNIXの場合:** `/etc/opt/omni/server/certificates`
2. 既存のCA証明書ファイル`cacert.pem`を生成されたCA証明書に置き換えます。

識別名(DN)文字列の更新

`jce-webservice-roles.properties`および`dp-webservice-roles.properties`ファイル内の既存の識別名(DN)を、クライアント証明書に使用するDN文字列に置き換えます。これらのファイルは以下の場所に置かれています。

Windowsの場合: `ProgramData\Omniback\Config\Server\AppServer`

UNIXの場合: `/etc/opt/omni/server/AppServer`

> **注:** DN文字列では、スペースと"="文字の前にはバックスラッシュ(\)記号を挿入します。

新しいキーストアと信頼ストアファイルを作成して証明書を上書きする

新しいキーストアと信頼ストアファイル内の証明書を上書きするには、以下の作業を実施します。

- 既存のサーバーとクライアントのストアファイルを置き換える
- CA証明書を置き換える
- 識別名(DN)文字列を更新する
- ストアパスワードを使用して構成ファイルを更新する

> **注:** サーバーとクライアントのストアパスワードは保持する必要があります。

既存のサーバーとクライアントのストアファイルの置換

既存のサーバーとクライアントのストアファイルを置き換えるには、以下の手順に従ってください。

1. 既存のサーバーとクライアントのストアファイル、 `server.keystore`、`server.truststore`、`client.keystore`、`client.truststore`の権限を書き留めてください。これらのファイルは以下の場所に置かれています。

   サーバー

   - Windowsの場合: `ProgramData\Omniback\Config\Server\certificates\server`
   - UNIXの場合: `/etc/opt/omni/server/certificates/server`

   クライアント

   - Windowsの場合: `ProgramData\Omniback\Config\Server\certificates\client`
   - UNIXの場合: `/etc/opt/omni/server/certificates/client`

2. サーバーとクライアントのストアファイルを削除します。
3. 同じファイル名と権限を使用してストアを作成します。
4. 生成された証明書をJava keytoolユーティリティを使用して次のストアにインポートします。
   - サーバーとCA証明書を`server.keystore`にインポートする
   - CAとクライアント証明書を`server.truststore`にインポートする
   - CA証明書を`ca.truststore`にインポートする
   - クライアントとCA証明書を `client.keystore`にインポートする
   - CAとサーバー証明書を`client.truststore`にインポートする

> **注:** Java keytoolユーティリティは以下の場所にあります。Windowsの場合、`Program Files\Omniback\jre\bin` 。UNIXの場合、`/opt/omni/jre/bin`。

CA証明書の置換

既存のCA証明書を置き換えるには、以下の手順に従ってください。

1. 以下の場所にある既存のCA証明書ファイル`cacert.pem`の権限に注意してください。

   Windows

ProgramData\Omniback\Config\Server\certificates

UNIXの場合

/etc/opt/omni/server/certificates

2. 既存のCA証明書ファイルcacert.pemを生成されたCA証明書に置き換えます。

識別名(DN)文字列の更新

jce-webservice-roles.propertiesおよびdp-webservice-roles.propertiesファイル内の既存の識別名(DN)を、クライアント証明書に使用するDN文字列に置き換えます。これらのファイルは以下の場所に置かれています。

Windows

ProgramData\Omniback\Config\Server\AppServer

UNIXの場合

/etc/opt/omni/server/AppServer

> **注:** DN文字列では、スペースと"="文字の前にはバックスラッシュ(\)記号を挿入します。

ストアパスワードによる構成ファイルの更新

ストアパスワードを使用して構成ファイルを更新するには、以下の手順に従ってください。

> **注:** この作業は、新しいパスワードを使用して新しいストアを作成する場合にのみ必要になります。

1. server.keystore、server.truststore、 ca.truststore、client.keystore、client.truststoreなどのストアファイルを作成するときに使用したストアパスアワードを使用して、webservice.propertiesとstandalone.xml構成ファイルを更新します。

   これらの構成ファイルは以下の場所に置かれています。

   Windows

   •ProgramData\OmniBack\Config\client\components\webservice.properties

   •ProgramData\OmniBack\Config\server\AppServer\standalone.xml

   UNIX

   •/etc/opt/omni/client/components/webservice.properties

   • /etc/opt/omni/server/AppServer/standalone.xml

2. standalone.xmlファイルでは、以下のストアパスワード(太字)を更新します。

   ```
   <ssl name="ssl" password="M6.pOino06L3w" certificate-key-
   file="/etc/opt/omni/server/certificates/server/server.keystore" protocol="TLS"
   verify-client="want" ca-certificate-
   file="/etc/opt/omni/server/certificates/server/ca.truststore" ca-certificate-
   password="M6.pOino06L3w"/>
   ```

3. webservice.propertiesファイルでは、パスワード(太字)を更新します。

```
 <jsse keystore-password="M6.pOino06L3w" keystore-
url="/etc/opt/omni/server/certificates/server/server.keystore" truststore-
password="M6.pOino06L3w" truststore-
url="/etc/opt/omni/server/certificates/server/server.truststore"/>

<jsse keystore-password="M6.pOino06L3w" keystore-
url="/etc/opt/omni/server/certificates/server/server.keystore" truststore-
password="M6.pOino06L3w" truststore-
url="/etc/opt/omni/server/certificates/server/server.truststore"/>

 <ssl name="ssl" password="M6.pOino06L3w" certificate-key-
file="/etc/opt/omni/server/certificates/server/server.keystore" protocol="TLS"
verify-client="want" ca-certificate-
file="/etc/opt/omni/server/certificates/server/ca.truststore" ca-certificate-
password="M6.pOino06L3w"/>
```

Data Protectorパッチの管理

Data ProtectorパッチはHPEサポートによって提供され、HPEサポートWebサイトからダウンロードできます。Data Protectorパッチは、個別またはバンドルで提供されます。

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

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。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。

> **注：**
> サイト専用パッチまたはパッチバンドルをインストールすると、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。

前提条件

- この機能を使用するには、User Interfaceコンポーネントをインストールしておく必要があります。

制限事項

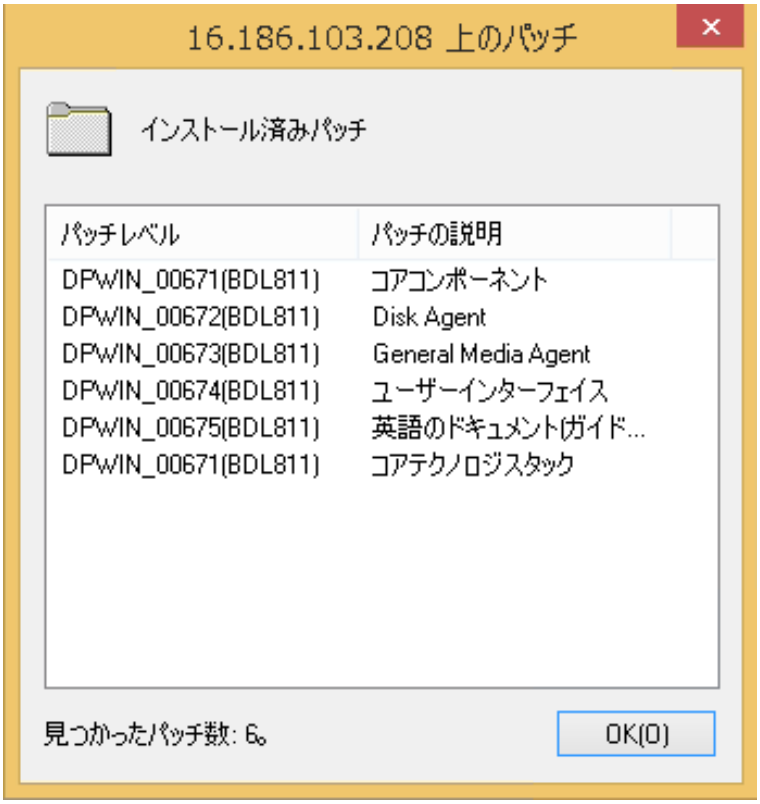
- パッチの確認は、同じセル内にあるシステムにインストールされているパッチのみが対象です。

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

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。

   インストール済みパッチの確認

   システム上にパッチが検出されると、各パッチのレベルおよび説明とインストールされているパッチの数が返されます。

   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。

   確認しようとしたシステムがセルのメンバーでないか、現在アクセス不能になっているか、エラーが発生した場合はエラーメッセージが返されます。
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、`omnicheck -patches -host` *`hostname`*コマンドを実行します。ここで、*hostname*は、確認対象システ

ムの名前を表します。

omnicheckコマンドの詳細については、omnicheck manページを参照してください。

Data Protectorで必要なパッチ

Data Protectorのパッチに関する最新情報は、https://softwaresupport.hpe.com/を参照してください。

Windowsシステムのパッチ

Windowsを実行しているシステムに関しては、最新のMicrosoft Windows Service PackについてMicrosoft社までお問い合わせください。

HP-UXシステムのパッチ

HP-UXオペレーティングシステムを実行しているシステムのパッチについては、http://h20565.www2.hpe.com/portal/site/hpscで最新情報を確認するか、レスポンスセンターで最新のパッチ番号を確認してください。サポートへのお問い合わせの前に、最新のパッチをインストールしてください。記載されているパッチは、新しいパッチに更新されている場合があります。

HPEHP-UX用として配布されるExtension Software Packageを定期的にインストールすることをお勧めします。これは推奨されるパッチを集めたものであり、その一部を以下に列挙します。HP-UX Extension Software Packageの現行バージョンについてはHPEのサポート担当にお問い合わせください。

HP-UX 11.11

Data Protectorでは以下のHP-UX 11.11パッチバンドルが必要です。

サービスパック	バンドル名	説明
最新を使用	GOLDQPK11i	HP-UX 11.11の最新パッチバンドル
最新を使用	HWEnable11i	必要とされるハードウェア有効化のためのパッチ

以下に挙げるHP-UX 11.11の個別パッチは、Data Protectorセル内のすべてのシステムに推奨されます。

パッチ名	ハードウェアプラットフォーム	説明
PHCO_40310	s700、s800	libc累積パッチ
PHSS_41214	s700、s800	ld(1)およびリンカーツールの累積パッチ
KRNG11i	s700、s800	Strong Random Number Generator

以下のHP-UX 11.11の個別パッチは、Data Protectorセル内のすべてのHP-UX 11.11クライアントに推奨されます。

パッチ名	ハードウェアプラットフォーム	説明
最新を使用	s700、s800	使用バージョンに対するHPE Serviceguardのパッチ

以下に挙げる製品およびHP-UX 11.11パッチは、AES 256ビット暗号化形式でのデータバックアップを実行する各Data Protector Disk Agentシステムにインストールする必要があります。

製品番号またはパッチ名	ハードウェアプラットフォーム	説明
KRNG11I	s700、s800	HP-UX Strong Random Number Generator
PHKL_27750	s700、s800	vparの有効化、krngの有効化

また、HP-UX 11.11でIPv6を使用する場合は、以下のバンドルとパッチがData Protectorに必要です。

バンドルまたはパッチ名	ハードウェアプラットフォーム	説明
IPv6NCF11iバンドルまたはTOUR移行用パッチ	s700、s800	Transport Transitionパッチ

HP-UX 11.23

Data Protectorでは以下のHP-UX 11.23パッチバンドルが必要です。

サービスパック	バンドル名	説明
最新を使用	QPK1123	HP-UX 11.23の最新パッチバンドル

以下のHP-UX 11.23の個別パッチは、Data Protectorセル内のすべてのHP-UX 11.23クライアントに推奨されます。

パッチ名	ハードウェアプラットフォーム	説明
PHKL_32272 [1]	s700、s800	getacl/setacl内の間欠的な故障を修正するための変更
PHSS_41178	s700、s800	linkerおよびfdp累積パッチ

HP-UX 11.31

Data Protectorでは以下のHP-UX 11.31パッチバンドルが必要です。

サービスパック	バンドル名	説明
最新を使用	QPK1131	HP-UX 11.31の最新パッチバンドル

[1] このパッチは、アクセス制御リスト(ACL)機能をサポートするために必要です。

Data Protectorでは以下のHP-UX 11.31の個別パッチが必要です。

パッチ名	ハードウェアプラットフォーム	説明
PHCO_38050	Itanium、PA-RISC	pthreadライブラリ累積パッチ
PHKL_38055	Itanium、PA-RISC	スケジューラー累積パッチ
PHSS_41179	Itanium、PA-RISC	linkerおよびfdp累積パッチ

SUSE Linux Enterprise Serverシステムのパッチ

SUSEで提供されている最新の推奨システムパッチをご使用ください。

Red Hat Enterprise Linuxシステムのパッチ

Red Hatで提供されている最新の推奨システムパッチをご使用ください。

パッチのインストール

Cell Managerパッチはローカルにインストールできます。ただし、クライアントにパッチを適用するには、インストールサーバーが必要です。インストールサーバーにパッチを適用した後、リモートでクライアントにパッチを適用できます。

> **重要:**
> HP-UXシステムでは、Cell Manager (CS)のパッチをCell Managerに適用する前に、Data Protector omnisvコマンドを使用してのData Protectorサービスを停止し、パッチの適用が完了した後に再度を開始してください。

1つのパッチバンドルに個々のパッチを含める場合、インストールできるのはバンドル全体のみです。詳細については、パッチで指定される手順を参照してください。

システム上にインストールされているパッチは、Data Protector GUIまたはCLIで確認できます。「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、ページ 222」を参照してください。

Symantec Veritas Cluster Server上で構成されているCell Managerへのパッチのインストール

Cell Managerコンポーネントのパッチ(CSパッチおよびパッチバンドル)をインストールする場合は、まずそのパッチを各ノードにローカルに適用する必要があります。Symantec Veritas Cluster Server上で実行されるクラスター対応のCell Managerに対するパッチ処理手順は、アップグレード(「Symantec Veritas Cluster Server上で構成されているCell Managerのアップグレード」を参照)と類似していますが、以下の点は異なります。

1. 構成手順はスキップする必要があります(つまり、omniforsg.kshは実行しません)。
2. Data Protectorのサービスをパッチインストールの前に開始してはなりません。

パッチをローカルにインストール(それが必要な場合)した後で、非Cell Managerコンポーネントおよびコアコンポーネントを、パッチ処理されたインストールサーバーからプッシュアップグレードする必要があります。これは、クラスター非対応のCell Managerに対する通常のパッチインストール手順でもあります。

Data Protectorパッチバンドルのインストールと削除

既にData Protectorがシステムにインストールされている場合、Data Protectorパッチバンドル(Data Protectorパッチのセット)もこのシステムにインストールできます。

Data Protectorパッチバンドルを UNIXシステムにインストールする操作には、`omnisetup.sh`スクリプトを使用できます。Windowsシステムでは、パッチバンドルは実行可能ファイルで提供されます。

また、パッチバンドルは削除することもできます。パッチバンドルを削除すると、Data Protectorは直前のリリースバージョンに戻ります。詳細については、パッチバンドルで指定される手順を参照してください。

UNIXシステムでData Protectorパッチバンドルをインストールおよび削除する

Data Protectorパッチバンドルをインストールするには、tarアーカイブに含まれている`omnisetup.sh`コマンドを、パッチバンドルファイルと共に使用します。`-bundleadd`オプションを使用します。

テレメトリーサブスクリプション

テレメトリーデータのコレクションをオプトインするには、テレメトリーライセンス契約を承認し、`omnisetup.sh`コマンドの`-telemetry`オプションで必要な詳細を入力します。

テレメトリーに使用するコマンドオプションは、`-compname`、`-proxyhost`、`-proxyport`、`-proxyuser`、`-proxypasswd`、`-no_telemetry`、`-accept_obsolescence`です。

`omnisetup.sh`コマンドの詳細については、『*HPE Data Protector CLI Reference Guide*』を参照してください。

> **注:**
> インストールプロセスでテレメトリーサブスクリプションを構成しない場合、Data Protector GUIを使用して後で構成することができます。

Data Protectorパッチバンドルをインストール可能なのは、インストールサーバーとCell Managerのみです。インストールが失敗した場合や途中で停止した場合、インストールを続行して残りのパッチのインストールをインストールする操作(Linuxシステムのみでサポートされている機能)、インストールしたパッチをロールバックして直前のパッチレベルに戻す操作、すべてのパッチのインストールをキャンセルして終了する操作が可能です。

Data Protectorパッチバンドルを削除するには、`omnisetup.sh -bundlerem`コマンドを実行します。

詳細については、パッチまたはパッチバンドルに用意されているインストール手順を参照してください。

WindowsシステムでのData Protectorパッチバンドルのインストールと削除

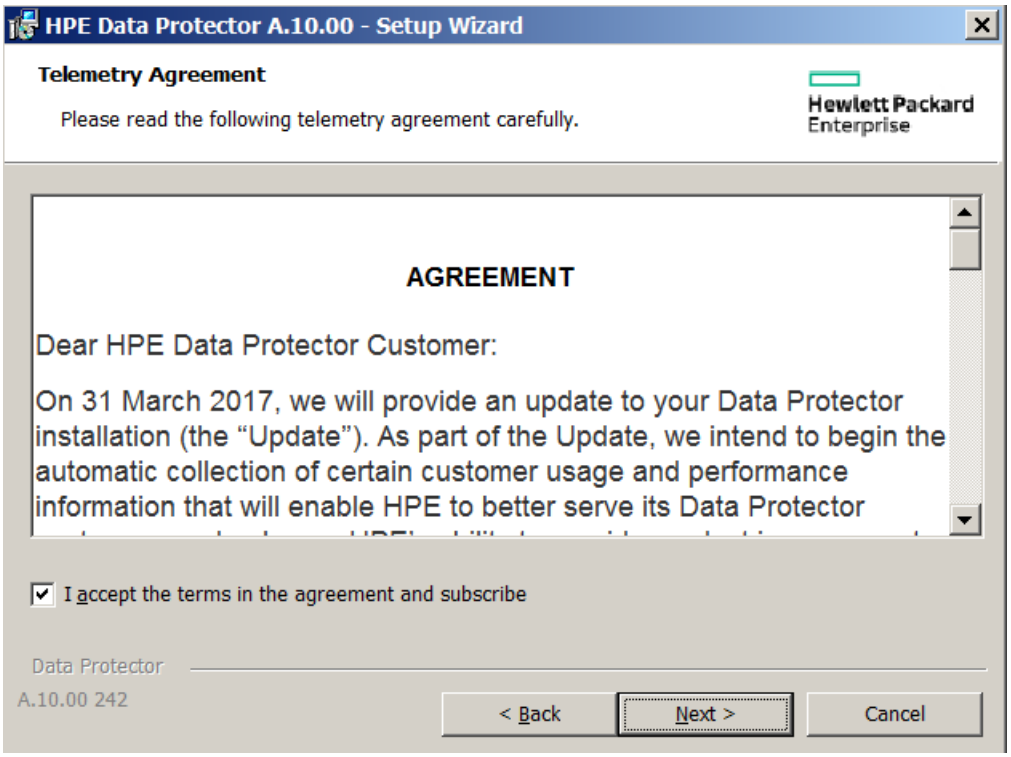
Windows用のData Protectorパッチバンドルは、実行可能ファイル(たとえば、`DPWINBDL_00701.exe`)として用意されています。Data Protectorパッチバンドルは、インストールサーバー、Cell Manager、またはクラ

イアントシステムにインストールできます。

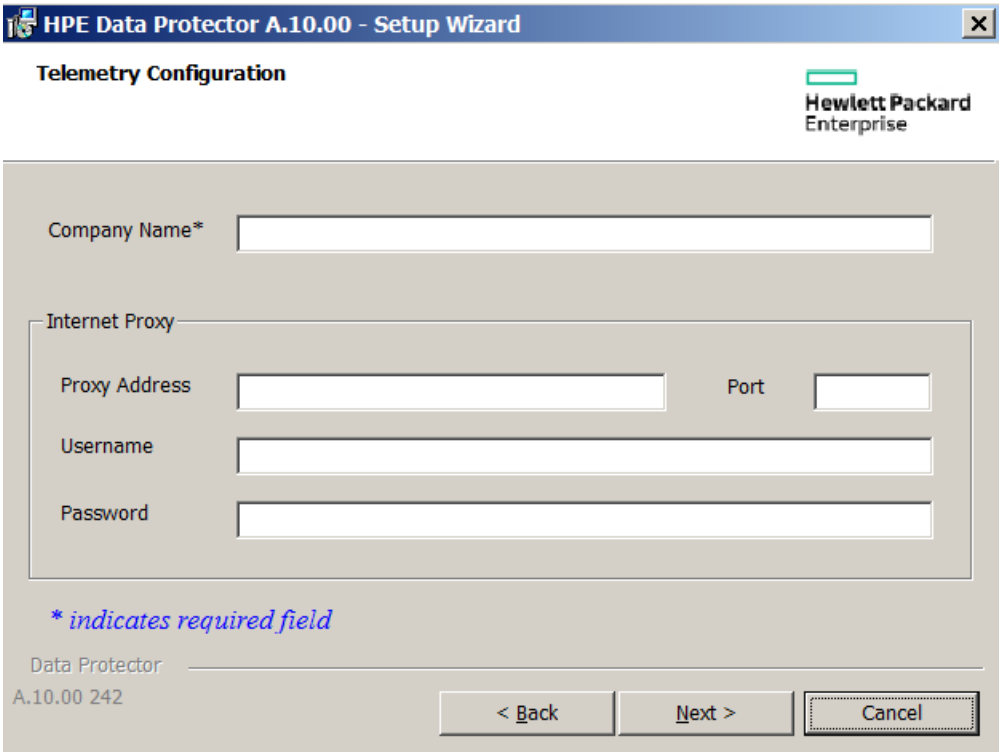
Windowsシステムにパッチバンドルをインストールするには、*BundleName*.exeコマンドを実行します。

テレメトリーサブスクリプション

- **テレメトリーに関する契約**: テレメトリーデータのコレクションをオプトインするには、テレメトリーライセンス契約を承認し、必要な詳細を入力します。テレメトリーの詳細については、『*HPE Data Protector Administration Guide*』を参照してください。



- **テレメトリーの構成**: 契約を承認した後で、以下のパラメーターを更新する必要があります。



- 会社名: 会社の名前
- プロキシアドレス: プロキシサーバーのアドレス
- ポート: プロキシサーバーのポート
- ユーザー名: プロキシサーバーに接続するユーザーの名前
- パスワード: 指定したユーザー名のパスワード

> **注:**
> セルコンソール(CC)クライアントからHPEインフラストラクチャーにテレメトリーデータをロードするには、プロキシの構成が必要です。

> **注:**
> インストールプロセスでテレメトリーサブスクリプションのオプトアウトを選択しない場合、Data Protector GUIを使用して後で構成することができます。

このコマンドは、システム上にインストールされているコンポーネントを認識し、それらを最終パッチにアップグレードします。

Data Protectorパッチバンドルを削除するには、`utilns`ディレクトリのData Protectorのデフォルトのコマンドの場所にある`remove_patch.bat`コマンドを実行します。

`remove_patch`*BundleNameDPInstallationDepot*(*DPInstallationDepot*は、Data Protectorのインストール元となった場所を示します。パッチバンドルのインストール元ではありません)。たとえば、パッチサービスバンドル`b701`を削除する場合は次のようになります。Data Protectorは、`D:\WINDOWS_OTHER`からインストールされたとします。

```
remove_patch.bat b701 D:\WINDOWS_OTHER
```

Data Protectorパッチバンドルは、インストールサーバー、Cell Manager、またはクライアントシステムから削除できます。

> **注：**
> Windowsシステムでは、`remove_patch.bat`コマンドを使用して個別のパッチを削除することもできます。ただし、システム上にパッチが残っている状態でcoreパッチを削除しないでください。先に削除すると、その後他の個別のパッチを削除できなくなります。
>
> メジャーリリースの後で導入されたData Protectorコンポーネントがシステムにインストールされている場合は、そのシステム上の製品を更新して、そのコンポーネントが既知であるパッチレベルまで戻すか、またはそのコンポーネントを削除してから、coreパッチやパッチバンドルをアンインストールしてください。Data Protectorコンポーネントの削除の詳細については、『Data Protectorソフトウェアコンポーネントの変更、ページ 234』の項を参照してください。

詳細については、パッチまたはパッチバンドルに用意されているインストール手順を参照してください。

内部データベースパッチのダウングレード

Data Protector 9.07以上のバージョンでは、パッチを削除する前にIDBをダウングレードする必要があります。

IDBパッチをダウングレードするには、以下の手順を実行します。

1. 次のコマンドを実行して、IDBを除くすべてのサービスを停止します。

   ```
   omnisv stop
   omnisv start -idb_only
   ```

2. Data Protector 9.04レベルにIDBをダウングレードします。

   Windowsシステムの場合：

   ```
   cd %DP_HOME_DIR%bin\dbscripts
   omnidbutil -run_script CPE\downgrade_to_904.sql
   ```

   GNU/LinuxまたはUNIXシステムの場合：

   ```
   cd /opt/omni/sbin/dbscripts
   omnidbutil -run_script CPE/downgrade_to_904.sql
   ```

3. パッチ削除を行って、Data ProtectorバージョンがDP 9.04より古くなり、DP 9.04にアップグレード可能になるまですべてのパッチを削除します。
4. パッチを削除したら、ただちに少なくとも9.04以上のバージョンに再アップグレードします(バックアップや復元を実行する前に行います)。

サイト固有のパッチとホットフィクスの管理

サイト固有のパッチ(SSP)とホットフィクス(HF)は影響を受けるクライアントまたはCell Managerに対して手動で適用されます。

インストールサーバーあるいはSSPまたはHFのリモートインストールの準備

Data Protector SSPまたはHFパッケージはHPEのサポートによって提供されます。SSPまたはHFパッケージを次の場所にあるインストールサーバーのデポにコピーする必要があります:

UNIXの場合: `/opt/omni/databases/vendor/ssphf`

Windowsの場合: `Data_Protector_program_data\depot\ssphf` (例: `C:\ProgramData\Omniback\depot\ssphf`)

> **注:**
> 修正プログラムはZIPファルで提供されます。インストールサーバーでファイルの使用を開始する前に、SSPまたはHFをアンパックする必要があります。Windowsの場合、展開したzipファイルを`Data_Protector_program_data\depot\ssphf`にコピーできます。Linux/UNIXの場合、SSPまたはHFをインストールサーバーにコピーした後、Linux/UNIX上で展開したtar.gzファイル(gzipを使用)をアンパックする必要があります。インストールサーバーのSSPまたはHF形式は、通常、Windowsの場合はZIP、Linux/UNIXの場合はTARです。

インストールサーバーへのリモートインストールに利用できるSSP/HFパッケージを確認するには、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**[インストールサーバー]**を展開し、SSP/HFのインストールをプッシュするセル内のシステムを選択します。
3. [結果エリア]で**[SSPs and HFs...]**をクリックして[SSPs/HFs]ポップアップウィンドウを開きます。

   システム上にSSP/HFが見つかった場合、インストールサーバーにSSP/HFのIDとSSP/HFの数が表示されるはずです。
4. **[OK]**をクリックしてウィンドウを閉じます。

クライアントへのサイト固有のパッチまたはホットフィクスのインストール

SSP/HFパッケージがインストールサーバーにコピーされると、Data Protector GUIで使用できるSSP/HFの選択リストを使用してインストールするSSP/HFを選択できます。SSP/HFが選択されている場合、一度にインストールできるSSP/HFパッケージは1つだけなので、その他のすべてのData Protectorコンポーネントが選択できなくなります。SSP/HFはさまざまなData Protectorコンポーネントのバイナリを提供できるため、インストールされているData Protectorコンポーネントのバイナリだけがシステムに適用されます。ただし、適用可能なすべてのバイナリがシステムに適用されるため、SSP/HFパッケージのステータスは[インストール済み]と表示されたままです。

> **注:**
> SSP/HFパッケージのリモートインストールもMoM-GUIで使用可能です。

SSP/HFパッケージのリモートインストールは、リモートシステムへのSSP/HFパッケージの導入、抽出、適用可能なバイナリのターゲットの場所へのコピーを意味します。そのため、使用中のファイルを置換するために必要とされる特別な手順は処理されません。

SSP/HFをクライアントに手動でインストールするには、以下の手順に従ってください。

- SSP/HFのアーカイブパッケージをあて先ホストにコピーして抽出します。
- Data Protectorサービスを停止します。影響を受けるサービスまたはプロセスのみを停止できます。
- 次のように、SSP/HFのバイナリを適用します。
  - 抽出されたSSP/HFパッケージからファイルを適用可能なあて先の場所にコピーします(Data Protectorのコンポーネントをインストールするためのファイルのみをコピーします)。
  - `CII_<SSPHFNAME>`を対応する場所にコピーします。
    例:
    Windowsの場合: `Data_Protector_program_data\config\Client\ssphf`
    その他のプラットフォームの場合: `\etc\opt\omni\client\ssphf`

また、`ob2install`コマンドを使用してクライアントにSSP/HFをインストールできます。`ob2install`コマンドの詳細については、`ob2install`のmanページを参照してください。

ほとんどの場合、リストに表示されているバイナリを提供するSSP/HFパッケージを手動でインストールする必要があります。

- Cell Serverのバイナリ - 特にサービスおよびセッションマネージャーのバイナリ。
- COREのバイナリ - **Windowsの場合:** `Inet`サービスのバイナリとカタログメッセージ。たとえば、`OmniInet.exe`、`OmniEnu.dll`など。
- GUIのバイナリ - このようなSSP/HFを適用する必要があるホスト上でData ProtectorのGUIを使用する場合。

> **注:**
> このようなSSP/HFをリモートでインストールすることはできず、適用可能なすべてのクラスターノードで手動で適用する必要があるため、MS Cluster Serverを実行しているクラスター対応Cell Managerへのコンポーネントの追加は無効です。

SSP/HFによって置換されたバイナリを元に戻す

SSP/HFのバイナリのリモートインストール中に、現在のファイルがバックアップされ、後で使用するためにシステム上に残されます。

例:

Windowsの場合: `Data_Protector_program_data\tmp\ssphf\<SSPHFNAME>\<DATE_TIME>`

その他のプラットフォームの場合: `/var/opt/omni/tmp/ssphf/<SSPHFNAME>/<DATE_TIME>`。(抽出場所はプラットフォームに応じて異なります)。

SSP/HFのプッシュインストールによって置換されたバイナリを元に戻すには、以下のいずれかのアプローチを検討してください。

- バックアップされたバイナリを手動で元に戻す。
- 影響を受けたコンポーネントをシステムに再インストールする。(推奨)
- Data ProtectorのGUIからシステムをアップグレードする。(**[クライアント]**コンテキスト)
- Data Protectorセットアップウィザードから修復オプションを実行する。(Windowsシステムのみに適用可能)

- 置換される古いSSP/HFの一部として組み込まれているすべてのバイナリが含まれるその他の任意のSSP/HFパッケージをインストールする。

各SSP/HFプッシュ操作によって、以下の場所に独自のログが作成されます。これは失敗した操作のトラブルシューティングに使用できます。

Windowsの場合: `Data_Protector_program_data\log\ssphf_install_<DATE_TIME>.log`

UNIX:の場合: `/var/opt/omni/log/ssphf_install_<PID>.log` (抽出場所はプラットフォームに応じて異なります)。

インストールされているSSPまたはHFの確認

Data ProtectorのGUIまたはCLIを使用してセル内のシステムにインストールされているData Protectorのサイト固有のパッチまたはホットフィクスを確認できます。

> **注:**
> SSP/HFを正常にインストールすると、SSPおよびHFでインストールのステータスが[Installed]と表示されます。失敗した場合、バイナリが元に戻り、そのようなSSP/HFのステータスはリストに表示されません。

SSP/HFのリモートインストールでは、ターゲットホストにインストールされるバイナリのみがインストールされます。SSP/HFパッケージでは、以下のいずれかのステータスが表示されます。

- インストール済み - システムにインストールされているData Protectorコンポーネントのすべてのバイナリがコピーされます。
- 一部 - システムにインストールされているData Protectorコンポーネントのパッケージの一部のバイナリはインストールされません。これは、以下の2つの理由によって発生する可能性があります。
  1. 完全なSSP/HFパッケージがインストールされている場合、SSP/HFが[Installed]とマークされます。ただし、どこかの時点で、別のSSP/HFまたは元のインストールのData Protectorコンポーネントがシステムにプッシュされ、SSP/HFによって提供されたバイナリの一部が上書きされる場合、このようなパッケージのステータスは[Partly]インストール済みに変更されます。
  2. SSP/HFパッケージで複数のData Protectorコンポーネントのバイナリ(たとえば、daとma)が提供され、一部のコンポーネントのみがシステムにインストールされる場合 (たとえば、da)、インストールされるコンポーネントのバイナリのみがシステムに適用されます(つまり、da)。このようなパッケージのインストールのステータスは[Installed]と表示されます。その後、maコンポーネントがシステムにインストールされる場合、このパッケージのステータスが[Partly]インストール済みに変更されます。

> **注:**
> SSP/HFパッケージによってインストールされるすべてのバイナリが他のバイナリに置換される場合、このようなSSP/HFはインストールされていないとして扱われ、SSP/HFのステータスリストに表示されません。

変更されたSSP/HFバイナリのリストを表示するには、以下の手順に従ってください。

- デバッグオプション付きでInetサービスを実行します。
- インストールされているSSP/HFパッケージのステータスを確認します。
- 変更されたバイナリのInetログを確認します。

GUIを使用してSSPまたはHFのパッケージを確認

Data ProtectorのGUIを使用して、特定のクライアントにインストールされているSSP/HF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、インストールされているSSP/HF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**[SSPs and HFs...]**をクリックして[SSPs/HFs]ポップアップウィンドウを開きます。

   システム上にSSP/HFが見つかった場合、確認によってSSP/HFのIDと各SSP/HFのステータス、インストールされているSSP/HFの数が返されます。
4. **[OK]**をクリックしてウィンドウを閉じます。

CLIを使用してSSPまたはHFを確認

Data ProtectorのCLIを使用して特定のクライアントにインストールされているSSP/HFを確認するには、`omnicheck -ssphf -host` *hostname*コマンドを実行します。ここで、*hostname*は確認するシステムの名前です。

`omnicheck`コマンドの詳細については、`omnicheck`のman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、Linuxシステムで削除および追加する方法について説明します。特定のオペレーティングシステムでサポートされているData Protectorコンポーネントのリストについては、『HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照してください。

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。詳細な手順については、リモートインストール、ページ 94を参照してください。

Data Protectorコンポーネントは、Cell Manager、インストールサーバー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

同じパッチレベルのData Protectorインストールデポが利用できる場合のみこの手順は可能です。一部のケースでは、設定するインストールデポへのパスは、**\\<DP_IS_SYSTEM>\Omniback\x8664**です。

1. Windowsのコントロールパネルで、**[プログラムの追加と削除 / プログラムと機能]**をクリックします。
2. **[HPE Data Protector 10.00]**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. [Program Maintenance]ウィンドウで**[Modify]**をクリックして**[Next]**をクリックします。
5. [Custom Setup]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. **[Install]**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. インストールが完了したら、**[Finish]**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、各クラスターノードでインストールパッケージを使用して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。

コンポーネントを削除するには、`swremove`コマンドを使用します。

手順

Data Protectorソフトウェアコンポーネントを削除するには

1. `root`としてログインし、`swremove`コマンドを実行します。
2. **[B6960MA]**、**[DATA-PROTECTOR]**、**[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. 削除する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:**
> 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 Server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。詳細については、『*HPE Data Protectorインテグレーションガイド*』を参照してください。

Linuxシステム

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、一部のData Protector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。

Data Protector Linux上の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-DOCS	OB2-CORE, OB2-TS-CORE
OB2-CS	OB2-CORE, OB2-TS-CORE, OB2-CC
OB2-TS-CS, OB2-TS-JRE, OB2-TS-AS, OB2-WS, OB2-JCE-DISPATCHER, OB2-JCE-SERVICEREGISTRY	OB2-CORE, OB2-TS-CORE, OB2-CC
インストールサーバー	
OB2-CORE-IS	OB2-CORE
OB2-CF-P, OB2-TS-CFP	OB2-CORE-IS
OB2-CCP, OB2-DAP, OB2-MAP, OB2-NDMPP, OB2-AUTODRP, OB2-DOCSP, OB2-CHSP, OB2-FRAP, OB2-JPNP, OB2-INTEGP, OB2-VMWP, OB2-VMWAREGRE-AGENTP, OB2-SODAP, OB2-TS-PEGP	OB2-CORE-IS, OB2-CF-P, OB2-TS-CFP
OB2-DB2P OB2-EMCP OB2-INFP OB2-LOTP OB2-OR8P OB2-SAPDP OB2-SAPP OB2-SSEAP OB2-SYBP	OB2-INTEGP, OB2-CORE-IS, OB2-CF-P, OB2-TS-CFP
OB2-SMISP	OB2-CORE-IS, OB2-CF-P, OB2-TS-CFP, OB2-TS-PEG-P

手順

Data ProtectorコンポーネントをLinuxシステムから削除するには

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コンポーネントを表示します。

3. インストールとは逆の順番で、ステップ2で表示したコンポーネントを削除します。`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

HP-UXまたはLinux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`の`omni_info`ファイルを更新します。

削除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ているだけで、セルからクライアントをエクスポートしていない場合は、`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。

```
omnicc -update_host HostName
```

インストールを確認する

Data Protectorソフトウェアコンポーネントが Cell Manager上またはクライアントシステム上で起動して動作しているかどうかを確認する必要がある場合は、Data Protectorグラフィカルユーザーインターフェイスを使って、インストールを確認できます。

前提条件

UNIXシステム用またはWindowsシステム用インストールサーバーなど、選択したクライアントシステムの種類に応じた、適切なインストールサーバーが必要です。

手順

1. コンテキストリストで**[クライアント]**をクリックします。
2. Scopingペインで、**[クライアント]**を展開して、Cell Managerまたはクライアントシステムを右クリックし、**[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. 同じ種類(UNIXシステムまたはWindowsシステム)のすべてのクライアントシステムが表示されます。インストールを確認するクライアントを選択して、**[完了]**をクリックすると、インストールの確認が開始されます。

[インストールチェック]ウィンドウに、インストールの確認結果が表示されます。

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、今後の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には、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。「Data Protectorクライアントのアンインストール、下」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。「Cell Managerとインストールサーバーのアンインストール、次のページ」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、ページ 234」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。「UNIXでのData Protectorソフトウェアの手動による削除、ページ 246」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ーからアンインストールする前に、以下を確認してください。

- コンピューター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。バックアップ仕様の変更方法については、『*HPE Data Protectorヘルプ*』のキーワード「変更、バックアップ仕様」で表示される内容を参照してください。
- アンインストールを行うシステムで、バックアップデバイスやディスクアレイが接続および構成されていないことを確認します。システムのエクスポートが完了すると、Data Protectorは元のセル内のバックアップデバイスやディスクアレイを使用できなくなります。
- アンインストールを行う前に、すべてのGRE電源オンのオープンリクエストがクローズしていることを確認します。また、進行中のライブ移行セッションが完了しているか、中止していることを確認します。

Data Protectorクライアントのアンインストール

> **注：**
> リモートでアンインストールを行う場合は、インストールサーバー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Data Protectorがインストールされている必要があります。

Data Protector GUIでリモートでクライアントをアンインストールするには

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には、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。

クラスタークライアントのアンインストール

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。「Cell Managerとインストールサーバーのアンインストール、下」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。ローカルでアンインストールする必要があります。

Data ProtectorクライアントをOpenVMSシステムからアンインストールするには

1. まず、セルからのクライアントのエクスポート、ページ 194の手順に従って、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、次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、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

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

1. すべてのData Protectorセッションが終了し、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. 構成データをシステム上に残しておくかどうかによって、実行する作業が異なります。

   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。

   - 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、**[HPE Data Protector 10.00]**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の構成データを削除するには、**[HPE Data Protector 10.00]**を選択して、**[変更]**、**[次へ]**の順にクリックします。[プログラムのメンテナンス]ダイアログボックスで、**[削除]**を選択します。**[Permanently remove the configuration data]**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。

HP-UXシステムからのアンインストール

HP-UX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ます。したがって、`swremove`ユーティリティを使用して、ローカルで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。

前提条件

- `omnisetup.sh -bundlerem`コマンドを使用して、インストールしたすべてのData Protectorパッチバンドルを削除します。「UNIXシステムでData Protectorパッチバンドルをインストールおよび削除する、ページ227」を参照してください。

手順

Data Protectorソフトウェアをアンインストールする前に、Data ProtectorシステムおよびCell Managerシステム上で実行されているインストールサーバー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、`omnisv -stop`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`の実行後に、Data Protectorプロセスが一切表示されないことを確認してください。

   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`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。

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、ページ 246」を参照してください。

HPE Serviceguard上で構成されているCell Managerおよびインストールサーバーのアンインストール

HPE 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 PackageName`

   *PackageName*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. 共有ディスクのマウントを解除します。

   ```
   umount shared_disk
   ```

   例:

   ```
   umount /omni_shared
   ```
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
    ```

    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_pathshared_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. 共有ディスクのマウントを解除します。

```
umountshared_disk
```

9. 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。

Symantec Veritas Cluster Server上で構成されているCell Managerおよびインストールサーバーのアンインストール

Symantec Veritas Cluster Server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アプリケーションリソースをオフラインにします。
2. Data Protectorアプリケーションリソースを無効にします。
3. Data Protectorをアンインストールしています。
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
```

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. Data Protectorサービスグループを二次ノードに切り替えます。
2. Data Protectorをアンインストールしています。
3. ソフトリンクを削除します。

```
rm /etc/opt/omni
rm /var/opt/omni
```

4. 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
```

5. 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
   ```

6. 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/var_opt_omni
   ```

以上でData Protectorがシステムから完全に削除されました。

Linuxシステムからのアンインストール

前提条件

- `omnisetup.sh -bundlerem`コマンドを使用して、インストールしたすべてのData Protectorパッチバンドルを削除します。「UNIXシステムでData Protectorパッチバンドルをインストールおよび削除する、ページ227」を参照してください。

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ます。したがって、`rpm`ユーティリティを使用して、ローカルで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ーフェイ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コンポーネントを表示します。

   Cell Managerに関連するコンポーネントは以下のとおりです。

OB2-CORE	Data Protectorのコアソフトウェア。
OB2-TS-CORE	Data Protectorコアテクノロジスタックライブラリ
OB2-CC	Cell Consoleソフトウェア。これには、コマンドラインインターフェイスが含まれます。
OB2-TS-CS	Cell Managerテクノロジスタックライブラリ

OB2-TS-JRE	Data Protectorで使用するJavaランタイム環境
OB2-TS-AS	Data Protectorアプリケーションサーバー
OB2-WS	Data Protector Webサービス
OB2-JCE-DISPATCHER	ジョブコントロールエンジンのディスパッチャー
OB2-JCE-SERVICEREGISTRY	ジョブコントロールエンジンサービスのレジストリ
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形式とのData Protectorガイドと WebHelp形式の『*HPE Data Protectorヘルプ*』を収録)

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、一覧内にその他のコンポーネントも表示されます。

> **注:**
> 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コンポーネントを削除しないでください。これは、他のコンポーネント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コンポーネントを削除します。`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

Linux上のUNIX用のインストールサーバーは、`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ます。したがって、`rpm`ユーティリティを使用して、ローカルで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セッションが終了し、GUIが閉じていることを確認します。
2. `rpm -qa | grep OB2`コマンドを入力すると、インストールサーバーシステム上のData Protectorコンポーネントとリモートインストールパッケージがすべて表示されます。

   インストールサーバーに関連するコンポーネントとリモートインストール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。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-TS-CORE	Data Protectorコアテクノロジスタックライブラリ

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-TS-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テクノロジスタックソフトウェア
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ッケージ
OB2-MAP	すべてのUNIXシステム用のMedia Agentリモートインストールパッケージ
OB2-NDMPP	NDMP Media Agentコンポーネント
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ッケージ

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、「Data Protector Linux上のソフトウェアコンポーネントの依存関係 、ページ 236」を参照してください。

> **注:**
> 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コンポーネントを削除しないでください。これは、他のコンポーネント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コンポーネントを削除します。`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。手順は、「セルからのクライアントのエクスポート 、ページ 194」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`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。

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
```

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
```

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
```

第7章: Data Protectorのアップグレード

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。

> **注:**
> インストール時には、Inet用に以下のポートを開く必要があります。
>
> - Data Protectorの新規インストール - 5565
> - Data Protectorインストールのアップグレード - 5555

アップグレードの概要

既存のプロダクトバージョンを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とバージョンについては、『https://softwaresupport.hpe.com/』および『HPE Data Protector製品案内、ソフトウェアノート、およびリファレンス』にある最新のサポート一覧を参照してください。

  Cell Managerのサポート対象外になったプラットフォームについては、まずサポート対象プラットフォームにCell Managerを移行してからData Protector 10.00にアップグレードします。詳細については、Cell Managerの異なるプラットフォームへの移行、ページ 253を参照してください。

  Data Protector 10.00では、Data Protector Javaグラフィカルユーザーインターフェイスはサポート対象外の機能領域として提供されなくなりました。Data Protector JavaグラフィカルユーザーインターフェイスがインストールされているData Protectorセル内にUNIXシステムが存在する場合、セルのアップグレード中にData Protectorグラフィカルユーザーインターフェイスクライアントの役割を果たすように、UNIXシステム以外のシステムを選択する必要があります。これらのクライアントは、元の(ネイティブ)Data Protectorグラフィカルユーザーインターフェイスによってサポートされているオペレーティングシステム上で実行する必要があります。
- Data Protector 10.00より前のリリースに対して発行されたライセンスパスワードは、このバージョンでは使用できなくなります。

  サポート契約に記載されているライセンスの種類と数量に従って新しいライセンスパスワードの資格を得るには、有効でアクティブなサポート契約を締結している必要があります。

  アップグレードを開始する前に、ご使用のData Protector環境にインストールされているライセンスキーの種類と数量をチェックし、サポート契約に記載されているライセンスの種類と数量と比較してください。

  サポート契約に記載されているライセンスの数量が、ご使用の環境に実際にインストールされているライセンスの数量より少ないか異なる場合は、アップグレードを開始しないでください。ライセンスキーの不足により、ご使用のData Protector環境が動作しなくなる可能性があります。代わりに、まずHPEの営業担当またはHPEパートナーに問い合わせて、サポート契約の対象となるライセンス機能とData Protector 9.00より古いバージョンのData Protectorで現在使用している実際のライセンスとのずれを埋めるのに必要な手順を特定してください。

  ライセンスの詳細については、Data Protector Licensing、ページ 274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、『*HPE Data Protector製品案内、ソフトウェアノートおよびリファレンス*』を参照してください。

- 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 10.00では、基本スケジューラーとアドバンストスケジューラーが廃止され、代わりに新しいWebベーススケジューラが導入されました。すべての既存のスケジュールが新しいスケジューラーに自動的に移行されます。移行にはユーザーの操作は必要ありません。

  アップグレード中に移行が失敗した場合、既存のスケジュールを新しいスケジューラーに正常に移行するために、以下のコマンドを手動で実行することができます。

  ```
  omnidbutil -migrate_schedules
  ```
- Data Protector 10.00では、JBoss 7.1がWildFly 10に代わりました。Data Protectorのアップグレードの際に、以下のJBossの構成が自動的にWildFlyに移行されます。
  - ロガーのレベルと形式
  - LDAP構成
  - PostgreSQLの資格情報

  > **重要:**
  > JBoss 7.1の`standalone.xml`ファイルに加えられた変更は、上記の構成とは別に、アップグレードの後にWildFlyの構成ファイルに手動で追加する必要があります。

  アップグレードの際に、Data Protectorによって古いJBoss構成ファイルのバックアップがフォルダーに作成されます。デフォルトでは、これらのファイルは以下の場所から利用できます。
  - Linux:`/etc/opt/omni/server/AppServer_<versionNo>`
  - Windowsの場合:`C:\ProgramData\OmniBack\Config\Server\AppServer_<versionNo>`

前提条件

- 既存のIDBに関するデータベース整合性チェックを実行し、移行の前にデータの整合性を検証します。
- 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。
- アップグレードを行う前に、すべてのGRE電源オンのオープンリクエストがクローズしていることを確認します。また、進行中のライブ移行セッションが完了しているか、中止していることを確認します。

制限事項

- アップグレード中のCell Managerプラットフォームの変更は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、LinuxからLinux、WindowsからWindowsのアップグレード)。

  お使いのプラットフォームがサポート対象外のプラットフォームである場合、まずサポートされているプラットフォームに移行してから、新しいバージョンにアップグレードします。「Cell Managerの異なるプラットフォームへの移行、ページ 253」を参照してください。

- UNIX環境の場合:アップグレードを実行する前に実行できるData Protectorプロセスは、Data Protectorサービスからのプロセスのみです。これを行うには、Data Protectorサービスを停止し、実行中のプロセスを終了して、サービスを再起動します。
- 内部データベースの復元は、内部データベースがバックアップされたのと同じマイナー-マイナーバージョンのData Protectorからのみがサポートされます。これは、新しいリリースにある内部データベースのスキーマ変更が原因です。
- 以前のバージョンのData Protectorでバックアップされた内部データベースを復元する場合は、そのバージョンを再インストールし、内部データベースバックアップメディアをインポートしてから、復元を実行してください。

アップグレード手順

旧バージョンから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 10.00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。

   Cell Managerをアップグレードする前に、まず現在のセルの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。
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. Data Protector 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. HPEでは、Data Protector 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 10.00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 10.00 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。

旧エージェントバージョンのサポート

Data Protectorセル内のすべてのクライアントのData Protectorコンポーネントは、通常のアップグレードプロセスの実行時に、可能な限り、バージョン10.00にアップグレードしてください。これによって、セル内のすべてのシステムでData Protector 10.00のフル機能セットによるメリットを得ることができるようになります。

ただし、Data Protectorの旧バージョンのDisk AgentコンポーネントとMedia Agentコンポーネントは10.00セル内でもサポートされますが、以下の制限事項があります。

- 以前の製品バージョンは、HPEによって独立した製品としてサポートされます。HPE製品の公表されたサポート終了日を確認するには、Webページhttps://softwaresupport.hpe.com/を参照してください。
- Data Protectorの旧バージョンの機能セットへのサポートは制限されています。
- 異なるシステム上のクライアントに関係する操作の場合は、同じ種類のエージェント(Media Agentsなど)のバージョンがすべて同じである必要があります。
- 以前のMedia Agentコンポーネントバージョンとの組み合わせはサポートされていません。
- ファイルシステムのバックアップは、バージョンが異なる複数のDisk Agentをそのソースとすることができます。バックアップサーバーの重複排除は、さまざまなバージョンのMedia Agentでサポートされています。Disk AgentおよびMedia Agentのバージョンは、Cell Managerのバージョン以下でもかまいません。ただし、ソースの重複排除を使用するには、Disk AgentとMedia Agentで同じバージョンが必要です。そのバージョンはCell Managerのバージョン以下でもかまいません。
- Data Protector StoreOnceソフトウェアストアの場合、Disk AgentとMedia Agentは同じバージョンであることが必要です。ただし、そのバージョンは、Cell Managerのバージョン以下でもかまいません。
- クライアント上の1つのData Protectorコンポーネントが10.00にアップグレードされたら、その他のコンポーネントもすべて10.00にアップグレードする必要があります。
- 最新のCell Managerバージョンでは、低いバージョンの統合エージェントはサポートされていません。

以前の製品バージョンのエージェントとの接続の確立に問題が発生した場合は、最初の解決方法として9.08へのアップグレードを検討してください。

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 10.00シングルサーバー版へ。詳細については、「旧バージョンのSSEからData Protector 10.00 SSEへのアップグレード」を参照してください。
- Data Protector 10.00シングルサーバー版からData Protector 10.00へ。詳細については、「Data Protector 10.00 SSEからData Protector 10.00へのアップグレード」を参照してください。

旧バージョンのSSEからData Protector 10.00 SSEへのアップグレード

旧バージョンのSSEからData Protector10.00 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 Protector10.00へのアップグレード手順と同じです。

Data Protector 10.00 SSEからData Protector 10.00へのアップグレード

Data Protector 10.00シングルサーバー版からData Protector 10.00にアップグレードするにはライセンスが必要です。ライセンスの詳細については、Data Protector Licensing、ページ 274を参照してください。

Data Protector 10.00シングルサーバー版からData Protector 10.00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、下」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、下」を参照してください。

> **注:**
> 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には、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。

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システムの場合:

   ```
   del Data_Protector_program_data\Config\server\Cell\lic.dat
   ```

   UNIXシステムの場合:

   ```
   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、ページ 23」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_program_data\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。以下を参照してください。
5. 新しいCell Managerにメディアをインポートします。

   メディアのインポートの詳細については、『*HPE Data Protectorヘルプ*』のキーワード「インポート、メディア」で表示される内容を参照してください。

Cell Managerの異なるプラットフォームへの移行

PA-RISC HP-UXシステムからIntel Itanium HP-UXシステムへの移行

Data Protectorでは、PA-RISCアーキテクチャーベースのHP-UX 11.11/11.23システムは、Cell Managerプラットフォームとしてサポートされなくなりました。したがって、アップグレードの前に、Cell ManagerをPA-RISCアーキテクチャーベースのHP-UX 11.11/11.23システムからIntel Itanium 2アーキテクチャーのHP-UX 11.23/11.31システムに移行する必要があります。

移行の手順については、適切な製品バージョンの『*HPE Data Protectorインストールガイド*』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またはWindows Server 2012への移行

Data Protectorでは、32ビットWindowsシステムをCell Managerプラットフォームとしてサポートしなくなりました。したがって、Data Protector 10.00へのアップグレード手順を開始する前に64ビットWindowsシステムにCell Managerを移行する必要があります。移行の手順については、適切な製品バージョンの『*HPE Data Protectorインストールガイド*』を参照してください。

SolarisからLinuxへの移行

この項では、SolarisシステムからLinuxシステムに既存のCell Managerを移行する手順を説明します。

> **重要：**
> Data Protector 10.00では、Cell ManagerプラットフォームとしてSolarisをサポートしなくなりました。したがって、Data Protector 10.00以降へのアップグレード手順を開始する前に、インストールされたData Protectorバージョンを使用して新しいプラットフォームにCell Managerを移行する必要があります。

手順

1. 既存のData Protectorインストールを使用して、以下の手順を実行して現在のCell Manager上のすべてのメディアカタログをエクスポートします。
   a. コンテキストリストで**[デバイス/メディア]**をクリックします。
   b. Scopingペインで**[メディア]**を展開してから、**[プール]**を展開します。
   c. カタログをコピー対象にするメディアのメディアプールを展開します。
   d. メディアを選択して右クリックして、**[カタログをファイルにコピー]**をクリックします。
   e. MCFファイルの出力ディレクトリを指定します。MCFファイルにメディア関連カタログデータが含ま

れます。

f. **[完了]**をクリックして、ウィザードを終了します。これにより、コピー処理が開始します。詳細については、『*HPE Data Protectorヘルプ*』のトピック「*MCFファイルにカタログメディアデータをコピーする*」を参照してください。

2. 新しいCell ManagerになるLinuxシステム上に、Data Protectorをインストールします。詳細については、UNIX Cell Managerのインストール Cell Manager、ページ 27を参照してください。
3. 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。「デフォルトのData Protector Inetポートの変更、ページ 345」を参照してください。
4. 新しいCell ManagerにMCFファイルをインポートするには、以下の手順に従ってください。
   a. コンテキストリストで**[デバイス/メディア]**をクリックします。
   b. Scopingペインで**[メディア]**を展開して**[プール]**を右クリックし、**[カタログをMCFファイルからインポート]**をクリックして、ウィザードを起動します。
   c. インポート対象のMCFファイルを指定します。
   d. セッションに適用するその他のオプションを指定します。デフォルトで、**[可能ならば元のプールにインポート]**オプションが選択されます。**[コピーをオリジナルとしてインポート]**オプションを選択します。
   e. **[完了]**をクリックして、ウィザードを終了します。これによって、インポート処理が開始されます。

   詳細については、『*HPE Data Protectorヘルプ*』のトピック「*MCFファイルからカタログメディアデータをインポートする*」を参照してください。
5. 新しいCell Manager上でライセンスを構成します。「Data Protectorの製品構成とライセンス、ページ 301」を参照してください。
6. 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。「MoM固有の手順、下」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。『*HPE Data Protectorヘルプ*』のキーワード「ファイアウォール環境」で表示される内容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、次のページ」を参照してください。

移行が完了したら、Data Protectorをアップグレードできます。

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、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。『*HPE Data Protectorヘルプ*』のキーワード「クライアントシステムのエクスポート」で表示される内容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。『*HPE Data Protectorヘルプ*』のキーワード「MoMの管理者、追加」で表示される内容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。『*HPE Data Protectorヘルプ*』のキーワード「インストールサーバー」で表示される内容を参照してください。

Windows Cell Manager内部データベースの異なるサーバーへの移行

次のシナリオは、内部データベース(IDB)を特定のWindows Cell Managerサーバーから別のサーバーに移行する例を示しています。

用語

このシナリオでは以下の用語を使用します。

- **OLD_SERVER**。IDBの移動元のCell Manager。
- **NEW_SERVER**。IDBの移動先のCell Manager。

前提条件

- コマンドライン引数を使用する場合は、OLD_SERVERおよびNEW_SERVERを完全修飾ドメイン名に置き換えてください。
- OLD_SERVERが、Windows 2008上で実行されている場合は、NEW_SERVERでWindows 2008またはWindows 2012を実行できます。
- OLD_SERVERが、Windows 2012上で実行されている場合は、NEW_SERVERがWindows 2012上で実行されている必要があります。
- 両方のサーバーでCell Manager上に同じバージョンのData Protectorがインストールされている必要があります。
- NEW_SERVERのIPアドレスがOLD_SERVERとは異なる場合、HPE Password Center

(http://enterpriselicense.hpe.com/)に連絡して、新しいIPアドレスにライセンスを移動する必要があります。

- NEW_SERVERで、完全なIDBバックアップが含まれるメディアをOLD_SERVERからインポートできる必要があります。
  - IDBのバックアップが物理テープに保存されている場合は、NEW_SERVERでテープドライブまたはライブラリを構成し、テープにアクセスできることを確認する必要があります。
  - IDBのバックアップが、ファイルライブラリバックアップデバイスに保存されている場合は、OLD_SERVERからファイルライブラリをエクスポートしてNEW_SERVERにインポートする必要がある場合があります。詳細は、「NEW_SERVERでの操作、下」を参照してください。
- 構成、ログ、およびデータベースファイルは*Data_Protector_program_data*ディレクトリに保存されます。通常のパス:`C:\ProgramData\Omniback.`

  異なる場所にインストールした場合は、後で使用できるようにその場所をメモしておきます。

移行の準備

移行を開始する前に、OLD_SERVERとNEW_SERVERでいくつかの作業を実行してIDBの移行のために準備する必要があります。

OLD_SERVERでの操作

- OLD_SERVERで既存のIDBに関する拡張されたデータベース整合性チェックを実行し、移行の前にデータの整合性を検証します。
- 既存のIDBのフルバックアップを実行します。

拡張されたデータベース整合性チェックの実行

1. `omnidbcheck -extended`を実行します。

   このコマンドは、以下の領域でデータの整合性を検証します。
   - データベースの接続
   - データベースおよびスキーマの整合性
   - データファイルおよびメディアの整合性

   不整合が検出された場合、最初にそれらの問題を解決してから、移行を実行してください。

OLD_SERVER上のIDBのフルバックアップの実行

IDBのフルバックアップの実行方法の詳細については、*HPE Data Protectorヘルプ*を参照してください。

NEW_SERVERでの操作

- *Data_Protector_program_data*ディレクトリ(通常は`C:\ProgramData\Omniback\Config\Server\cell\cell_info`)にある`cell_info` ファイルのコピーを保存します。このファイルは後で使用します。

omnidownloadおよびomniuploadを使用したファイルライブラリに関する情報の転送

1. OLD_SERVERで、`omnidownload -library Library`を使用して、ファイルライブラリに関する情報をData Protector IDBからASCIIファイルにダウンロードします。

   たとえば、「FL1」という名前のファイルライブラリへのIDBバックアップの場合、次のコマンドを使用します。

   ```
   omnidownload –library FL1 –file “C:\tmp\FL1.txt”
   ```

2. `omnidownload`の出力ファイルをNEW_SERVERにコピーします。

   たとえば、`C:\tmp\FL1.txt`にコピーします。

3. NEW_SERVERで、omniupload -create_library <filename>.txtを使用して、ライブラリファイルをアップロードし、NEW_SERVERに新しいバックアップデバイスを作成します。

   ```
   omniupload -create_library “C:\tmp\FL1.txt”
   ```

4. NEW_SERVERで新しいバックアップデバイスからメディアをインポートします。

   コマンドの詳細については、『HPE Data Protector Command Line Interface Reference』を参照してください。メディアのインポートの詳細については、『*HPE Data Protectorヘルプ*』を参照してください。

移行作業

Linuxの前提条件:

- IDBの復元先が新しいホストまたはCell Managerの場合は、`user`および`group ID`が元のCell Managerと同じであることが必要です。

  Data Protectorをインストールする前に、次のコマンドを使用して、新しいホスト上の`user`および`group ID`を変更します。

  - 元のホスト上の`hpdp user`および`group`のIDを確認するには、`cat /etc/passwd`を使用します。
  - 新しいホスト上の`user`および`group ID`を設定するには、以下のコマンドを使用します。

    ```
    usermod -u <NEWID> <LOGIN>
    groupmod -g <NEWID> <GROUP>
    usermod -g <GROUP> <LOGIN>
    ```

IDBのインポート

NEW_SERVER上でIDBをインポートするには

1. メディアがインポートされたら、Data Protector GUIでIDBバックアップセッションを表示できることを確認します。
2. 復元されたIDBで使用する新しいディレクトリを作成します。

   たとえば、次の場所にディレクトリを作成します。

   ```
   C:\ProgramData\Omniback\server\db80_restore\idb
   ```

> **注：注：**OLD_SERVERからNEW_SERVER上の同じ場所にIDBを復元することはできません。これはこのIDBが使用中であるためです。

3. Data Protector GUIのコンテキストリストで**[復元]**をクリックします。
4. Scopingペインで、**[復元オブジェクト]**項目、**[内部データベース]**項目を順に展開します。
5. OLD_SERVER項目を展開し、**[内部データベース]**をクリックします。
   a. 内部データベースのプロパティページで、内部データベースの基本部分を復元するには、以下の手順を実行します。
      i. **[内部データベースの復元]**オプションを選択します。
      ii. 復元中に使用する内部データベースサービス用の一時ポートと、復元先の場所として`C:\ProgramData\Omniback\server\db80_restore\idb`を指定します。
      iii. IDBのDCBF部分を復元するには、**[カタログバイナリファイルの復元]**を選択し、**[元のディレクトリに復元]**を選択します。
   b. 構成ファイルのプロパティページで、以下の手順を実行します。

      Windowsシステムの場合：

      i. **[元のディレクトリに復元]**を選択します。

      > **注：**
      > **[構成ファイルの復元]**オプションがチェックされていることを確認します。

      ii. **[ファイル重複時の処理]**リストから[最新ファイルを保持]を選択します。

      UNIXシステムの場合：

      「復元プロセスの終了時にIDBの復元に失敗する、ページ263」を参照してください。
   c. **[復元]**をクリックしてIDBの復元を開始します。

      復元中に次のエラーメッセージが他のメッセージとともに表示されることがありますが、無視できます。

      ```
      [Major] From: OB2BAR_POSTGRES_BAR@mrou77.usa.hp.com "DPIDB" Time: 10/9/2014
      10:35:29 PM The OS reported error while accessing
      C:/ProgramData/OmniBack/config/server/certificates: [80] The file exists.
      ```
   d. 復元が完了したら、Data Protectorサービスを停止してから開始します。

      ```
      omnisrv -stop

      omnisrv -start
      ```

> **注：**
> IDBの復元セッションの完了後に問題が発生した場合は、「トラブルシューティング」を参照してください。

復元後の作業

復元の後に以下の作業を実行します。

1. `omnidbutil -show_db_files`を実行して、「IDBのインポート、前のページ」の手順3で作成したディレクトリ内に復元されたファイルが存在することを確認します。

2. NEW_SERVERをCell Managerとして追加します。「Cell ManagerとしてのNEW_SERVERの追加、下」を参照してください。
3. 必要に応じて、IDB内のCell Managerの名前を変更します。「IDB内のCell Managerの名前の変更、下」を参照してください。
4. omnidbcheck -extendedを実行して、復元されたIDBの整合性を検証します。「拡張されたデータベース整合性チェックの実行、ページ 256」を参照してください。

Cell ManagerとしてのNEW_SERVERの追加

Cell ManagerとしてNEW_SERVERを追加するには

1. Data Protector GUIの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. OLD_SERVER項目を削除します。
3. NEW_SERVERをインポートし、Cell Managerとして表示されることを確認します。

上記の手順が成功しない場合

1. 「移行の準備、ページ 256」で保存したcell_infoファイルをテキストエディターで開きます。
2. NEW_SERVERのホスト名が含まれる行をクリップボードにコピーします。
3. cell_infoファイルを編集します。
   a. NEW_SERVERのエントリをクリップボードから入力します。
   b. OLD_SERVERのエントリを削除し、cell_infoファイルを保存します。
4. GUIを再起動します。

IDB内のCell Managerの名前の変更

NEW_SERVERのホスト名がOLD_SERVERと異なる場合は、IDB内でCell Managerを変更する必要があります。

たとえば、OLD_SERVERの名前がoldcm.company.comでNEW_SERVERの名前がnewcm.company.comであるとします。

NEW_SERVERで以下の手順を実行します。

1. omnidbutil -show_cell_nameを実行し、どのCell ManagerがIDBを所有しているかを表示します。

   例:

   ```
   > omnidbutil -show_cell_name
   Catalog database owner: "oldcm.company.com"
   ```

2. -change_cell_name *OldHost*を実行し、IDBの所有権をNEW_SERVERに変更します。

   例:

   ```
   > omnidbutil -change_cell_name oldcm.company.com
   This action will change ownership of libraries, devices, media pools and media.
   Are you sure [y/n]? y
   DONE!
   ```

次に行う手順

1. omnicc コマンドを実行して、クライアントをNEW_SERVERに移行します。

   omnicc -update_all -force_csコマンドを実行して、セル内のすべてのクライアントのNEW_SERVER cell_info構成ファイル内のバージョンおよびインストール済みコンポーネントの情報を更新します。

   omniccコマンドの説明については、『*HPE Data Protector Command Line Interface Reference*』を参照してください。
2. 元のIDBバックアップ仕様はOLD_SERVERを使用するように構成されているので、NEW_SERVER用の新しいIDBバックアップ仕様を作成します。

   詳細については、『*HPE Data Protectorヘルプ*』を参照してください。
3. 内部データベースに移動し、実行状態のセッションがないか確認します。ある場合は、omnidbutil -clearコマンドを実行します。
4. Data Protectorサービスを停止してから、開始します。

   omnisrv -stop

   omnisrv -start

トラブルシューティング

問題

IDB復元操作の実行後、Data Protector GUIからCell Managerへの接続が失敗する

IDB復元操作の実行後、GUIからCell Managerへの接続が失敗し、次のエラーが表示されます。

サーバーエラーが発生しました。報告されたエラーメッセージ:
ホストに接続できません。

hpdp-asサービスプロセスがポート7116でリスンしていません。

対処方法

1. コマンドウィンドウを開き、netstatコマンドを実行して、リスンポート7116を確認します。

   ```
   c:\> netstat -ban | findstr 7116 | findstr LISTEN
   ```

   このnetstatコマンドが結果を返した場合は、リスンポートが正しく構成されています。

   たとえば次のように、netstatコマンドが何も結果を返さない場合は、ポートは正しく構成されていません。

   ```
   c:\> netstat -ban | findstr 7116 | findstr LISTEN
   c:\>
   ```
2. /etc/opt/omni/server/AppServer/standalone.xmlファイルのバックアップを取ります。
3. /etc/opt/omni/server/AppServer/standalone.xml 内のキーストアとトラストストアのパスワードを/etc/opt/omni/client/components/webservice.propertiesに保存されているパスワードに置き換えます。

C:\ProgramData\Omniback\Config\client\componentsディレクトリに移動し、webservice.propertiesファイルから次のコード行を探します。

```
keystorePassword=jones7XE7EJjHzZ

truststorePassword=jones7XE7EJjHzZ
```

4. 後で使用できるようにキーストアのパスワードをメモします。
5. standalone.xmlファイルをテキストエディターで開いて、keystore-passwordが含まれる次のような行を探します。

```
<jsse keystore-password="JypjEncO.9aG1"
keystoreurl="C:/ProgramData/OmniBack/Config/server/certificates/server/server.keystore"

truststore-password="JypjEncO.9aG1"
truststoreurl="C:/ProgramData/OmniBack/Config/server/certificates/server/server.truststore"/>
```

6. standalone.xmlファイルでkeystoreおよびtruststoreパスワードのすべてのインスタンスを手順4のwebservice.propertiesファイルのキーストアパスワードに置き換えて、ファイルを保存します。
7. コマンドウィンドウで、C:\Program Files\OmniBack\binに移動します。
8. 次のコマンドを使って、証明書を再生成します。

```
perl omnigencert.pl -server_id NEW_SERVER -store_password <keystore-password>
```

*<keystore-password>*は、手順4でメモしたパスワードです。

9. Data Protectorサービスを停止してから、開始します。

```
omnisrv -stop

omnisrv -start
```

10. Cell Managerにもう一度接続してみます。

問題

IDB復元操作の実行後、Data Protector GUIからCell Managerへの接続が失敗し、SSLエラーが表示される

IDB復元操作の実行後、GUIからCell Managerへの接続が失敗し、次のエラーが表示されます。

サーバーエラーが発生しました。報告されたエラーメッセージ:
SSLピア証明書またはSSHリモートに問題があります。

対処方法

1. C:\ProgramData\Omniback\Config\client\componentsディレクトリに移動し、webservice.propertiesファイルを開きます。

```
# global property file for all components
jce-serviceregistry.URL = https://newcm.company.com:7116/jce-serviceregistry/restws
```

```
keystorePath=C:/ProgramData/OmniBack/Config/server/certificates/client/client.k
eystore

truststorePath=C:/ProgramData/OmniBack/Config/server/certificates/client/client
.truststore
keystorePassword=jones7XE7EJjHzZ
truststorePassword=jones7XE7EJjHzZ
```

2. keystorePasswordとtruststorePasswordをメモします。
3. コマンドウィンドウで、C:\Program Files\OmniBack\binに移動します。
4. 次のコマンドを使って、証明書を再生成します。

   ```
   perl omnigencert.pl -server_id NEW_SERVER -store_password <keystore-password>
   ```

   *<keystore-password>*は、手順2でメモしたパスワードです。
5. Data Protectorサービスを停止してから、開始します。

   ```
   omnisrv -stop

   omnisrv -start
   ```
6. Cell Managerにもう一度接続してみます。

問題

IDBのバックアップ中に、IDBをバックアップモードにすることができずに失敗する

IDBのバックアップ中に、セッションメッセージに次のエラーが表示されます。

```
[危険域]場所: OB2BAR_POSTGRES_BAR@oldcm.company.com "DPIDB" 時間: 10/10/2014
12:19:51 PM
```

内部データベースをバックアップモードにできませんでした

対処方法

1. C:\ProgramData\OmniBack\Config\Server\idbに移動し、idb.configファイルのコピーをバックアップとして作成します。
2. テキストエディターで、idb.configファイルを開き、PGOSUSERを検索します。
   例:

   ```
   PGOSUSER='OLD_SERVER\Administrator';
   ```
3. サーバー名が正しくない場合は、NEW_SERVERの名前になるように編集します。
   例:

   ```
   PGOSUSER='NEW_SERVER\Administrator';
   ```
4. Data Protectorサービスを停止してから、開始します。

   ```
   omnisrv -stop

   omnisrv -start
   ```
5. IDBバックアップを再度試行します。

問題

復元プロセスの終了時にIDBの復元に失敗する

復元プロセスの終了時にIDBの復元が失敗して次のメッセージが表示されます。

次のコマンドを実行できません: omnidbutil -clear

対処方法

この問題は、HP-UXのCell Managerで次の状況が発生した場合に発生する可能性があります。別のCell Managerに復元しようとしている場合、あるいは同じCell Manager上であるが、バックアップセッションの復元後または新しいCell Managerをインストールした後にpostgresパスワードを変更した場合。

> **注:**
> Linux環境では、復元は正常に完了します。これは、Linuxは、HP-UXとは対照的に、データベース上で主にオペレーティングシステム認証を使用しているためです。HP-UXはパスワード認証を使用しており、この場合パスワードファイルが正しく復元されません。ただし、Linux環境でも、正しいパスワードファイルを保持するためにこの対処方法を適用する必要があります。

1. IDB全体を復元する特定の時点まで、構成ファイルのみを別の場所<restore-conf>に復元します。
2. DCBFを除くIDB全体を復元するか、またはDCBF全体を元の場所に復元します。
3. /etc/otp/omni/server/idb/idb.configのバックアップをidb.config.bkpに保存します
4. 場所<restore-conf>から元の場所にファイルのコピーを実行します。
   a. cp <restore-conf>/etc/opt/omni/server/idb/idb.config /etc/opt/omni/server/idb/idb.config
   b. cp <restore-conf>/etc/opt/omni/server/idb/ulist /etc/opt/omni/server/idb/ulist
   c. cp <restore-conf>/etc/opt/omni/server/AppServer/standalone.xml /etc/opt/omni/server/AppServer/standalone.xml
5. 正しい場所をポイントするようにidb.config内の以下のフィールドを修正します(正しい場所はidb.config.bkpに保存されます)。
   a. PGDATA_PG='/space/restore1/pg';
   b. PGDATA_IDB='/space/restore1/idb';
   c. PGDATA_JCE='/space/restore1/jce';
   d. PGWALPATH='/space/restore1/pg/pg_xlog_archive' ;
6. Data Protectorサービスを停止してから、開始します。
   a. omnisv stopを実行します(これには時間がかかる場合があります)。
   b. omnisv startを実行します。
   c. omnidbutil -clearを実行します。

HPE 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、以前のバージョンの製品は削除されます。Data Protectorの最新バージョン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する場合は、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。

前提条件

- HPE Serviceguardの二次ノード上のData Protectorサービスは実行しないでください。

  これにより、アップグレードは一次ノードのアップグレード中にエクスポートされたIDBを使用し、他のIDBエクスポートを回避できるようになります。

以前のバージョンのData ProtectorからData Protectorの最新バージョンへ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。以下の項で示される順序で手順を実行します。

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` *`PackageName`*コマンドを実行して(*`PackageName`*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 VGName
   ```

   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 LVPathSharedDisk
   ```

   *`LVPath`*パラメーターには論理ボリュームのパス名を、*`SharedDisk`*パラメーター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. Data Protectorサービスを開始します。

   ```
   omnisv -start
   ```

5. で説明されている手順に従ってCell Managerをアップグレードします。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。
6. Data Protectorサービスを停止します。

   ```
   omnisv -stop
   ```

7. 共有ディスクのマウントを解除します。

```
umount SharedDisk
```

例:

```
umount /omni_shared
```

8. ボリュームグループを非アクティブ化します。

```
vgchange -a n VGName
```

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 VGName
```

2. 論理ボリュームを共有ディスクにマウントします。

```
mount LVPathSharedDisk
```

3. で説明されている手順に従ってCell Managerをアップグレードします。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。
4. /etc/opt/omni/server/sgディレクトリにあるcsfailover.shおよびmafailover.ksh起動スクリプトの名前を(たとえば、csfailover_DP70.shおよびmafailover_DP70.kshに)変更し、新しいcsfailover.shおよび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. Data Protectorサービスを停止します。

```
omnisv -stop
```

6. 共有ディスクのマウントを解除します。

```
umount SharedDisk
```

7. ボリュームグループを非アクティブ化します。

```
vgchange -a n VGName
```

一次ノード

一次ノードに再度ログオンし、以下の手順に従ってください。

1. Data Protectorパッケージを起動します。

```
cmrunpkg PackageName
```

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。以下を実行します。

```
/opt/omni/sbin/install/omniforsg.ksh -primary -upgrade
```

3. Data Protectorパッケージを停止します。

   ```
   cmhaltpkg PackageName
   ```

二次ノード

二次ノードに再度ログオンし、以下の手順に従ってください。

1. Data Protectorパッケージを起動します。

   ```
   cmrunpkg PackageName
   ```

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。サブディレクトリが、/etc/opt/omniまたは/var/opt/omniディレクトリにマウントされていないことも確認します。以下を実行します。

   ```
   /opt/omni/sbin/install/omniforsg.ksh -secondary /share -upgrade
   ```

   > **注：**
   > /shareは、クラスターノード間の共有のディレクトリまたはストレージです。

3. Data Protectorパッケージを停止します。

   ```
   cmhaltpkg PackageName
   ```

一次ノード

一次ノードに再度ログオンし、以下の手順に従ってください。

1. Data Protectorパッケージを起動します。

   ```
   cmrunpkg PackageName
   ```

   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 VirtualHostname -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 VirtualHostname
   ```

> **注：**
> Cell Managerからのすべての要求は、Data Protector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、セキュリティの留意事項、ページ 196を参照してください。

Symantec Veritas Cluster Server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、以前のバージョンの製品は削除されます。Data Protector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する場合は、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。

前提条件

Symantec Veritas Cluster Serverの二次ノード上のData Protectorサービスは実行しないでください。

以前のバージョンのData Protectorからアップグレードするには、一次ノードと二次ノードのアップグレードが必要です。以下の項で示される順序で手順を実行します。

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アプリケーションリソースをオフラインにします。
2. Data Protectorアプリケーションリソースを無効にします。
3. 次のコマンドを使用して、Data Protectorのサービスを開始します。

   ```
   omnisv -start
   ```
4. で説明されている手順に従ってCell Managerをアップグレードします。
5. Data Protectorアプリケーションリソースによって使用される監視スクリプトがカスタマイズ済みの場合は、新しくインストールされた`/opt/omni/sbin/vcsfailover.ksh`スクリプトから提供される変更内容をカスタマイズ済みのスクリプトに実装し直します。
6. Data Protectorサービスを停止します。

   ```
   omnisv -stop
   ```

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. Data Protectorサービスグループを二次ノードに切り替えます。
2. で説明されている手順に従ってCell Managerをアップグレードします。
3. Data Protectorアプリケーションリソースによって使用される監視スクリプトがカスタマイズ済みの場合は、新しくインストールされた`/opt/omni/sbin/vcsfailover.ksh`スクリプトから提供される変更内容をカスタマイズ済みのスクリプトに実装し直します。
4. Data Protectorサービスを停止します。

   ```
   omnisv -stop
   ```

一次ノード

一次ノードに再ログオンし、以下の手順に従ってください。

1. Data Protectorサービスグループをプライマリノードに切り替えます。
2. Data Protectorアプリケーションリソースを有効にします。
3. Data Protectorアプリケーションリソースをオンラインにします。
4. Cell Managerを構成します。スクリプトが、/etc/opt/omniまたは/var/opt/omniディレクトリ、またはそれらのサブディレクトリから実行されていないことを確認します。サブディレクトリが、/etc/opt/omni or /var/opt/omniディレクトリにマウントされていないことも確認します。次のコマンドを実行します。

   ```
   /opt/omni/sbin/install/omniforsg.ksh -primary -upgrade
   ```

二次ノード

二次ノードに再ログオンし、以下の手順に従ってください。

1. Data Protectorサービスグループを二次ノードに切り替えます。
2. Cell Managerを構成します。スクリプトが、/etc/opt/omniまたは/var/opt/omniディレクトリ、またはそれらのサブディレクトリから実行されていないことを確認します。サブディレクトリが、/etc/opt/omni or /var/opt/omniディレクトリにマウントされていないことも確認します。次のコマンドを実行します。

   ```
   /opt/omni/sbin/install/omniforsg.ksh -secondary dirname -upgrade
   ```

   ここで、*dirname*は、マウントポイントまたは共有ディレクトリを表します(例： /omni_shared)。

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サービスグループをプライマリノードに切り替えます。
2. 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、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 VirtualHostname
   ```

> **注：**
> Cell Managerからのすべての要求は、Data Protector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、セキュリティの留意事項、ページ 196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)上でCell Managerをアップグレードするには、Windows用インストールパッケージからローカルに実行する必要があります。

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

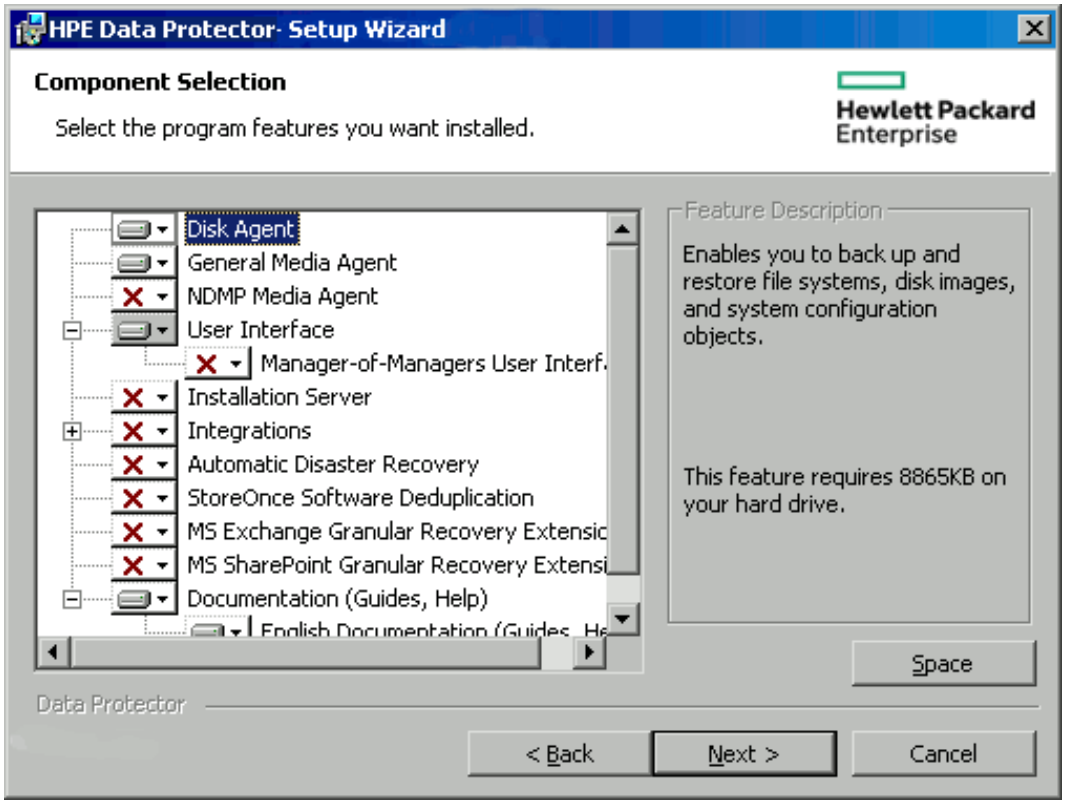
アップグレードは、以下の手順で行ってください。

1. ダウンロードしたインストールパッケージをWindowsシステムにコピーし、ファイルを一時的な場所に展開します。\Windows_Other\x8664にあるsetup.exeファイルを実行します。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、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。

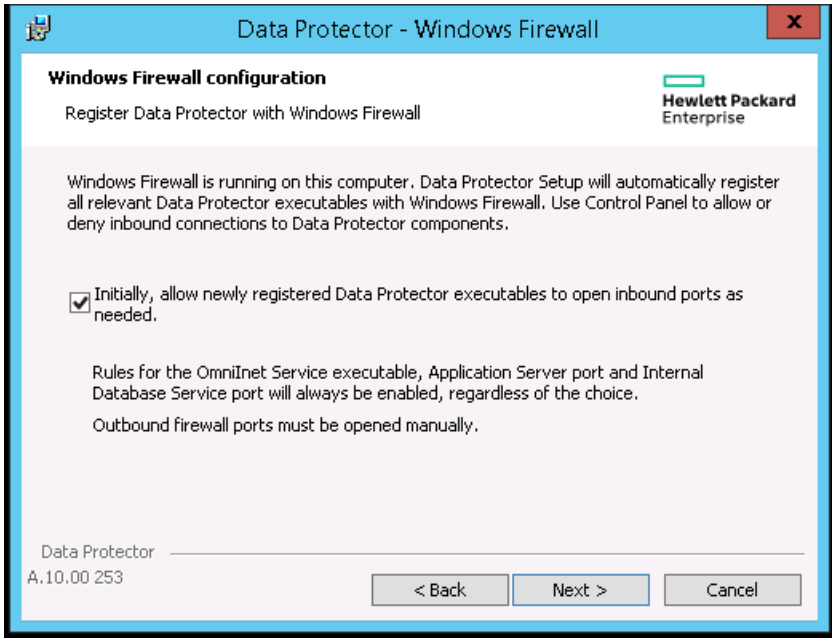
   [Next]をクリックし、次に進みます。
2. インストール済みのコンポーネントがData Protectorによって自動的に選択されます。

   コンポーネントの選択



[次へ]をクリックします。

3. システムにWindows Firewallが検出された場合、Windows Firewallの構成ページが表示されます。Data Protectorセットアップでは、すべての必要なData Protector実行可能ファイルが記録されます。デフォルトでは、**[Initially, allow newly registered Data Protector executables to open inbound 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。Data Protectorが以前のバージョンの10.00クライアントで適切に機能するには、WindowsファイアウォールのData Protectorルールを有効にする必要があります。OmniInetサービス実行可能ファイル、アプリケーションサーバーポート、内部データベースポートのルールは、選択内容にかかわらず常に有効になります。



[次へ]をクリックします。

4. 必要に応じて、Data Protector IDBおよびHTTPSアプリケーションサーバーで使用するユーザーアカウントと、これらのサービスで使用するポートを変更します。

   [次へ]をクリックします。

5. 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。

   コマンドプロンプトウィンドウが開き、古いIDBをエクスポートすることによって新しいデータフォーマットへのIDBの移行が開始されます。

   このコマンドプロンプトウィンドウは、古いIDBのエクスポート中に開いたままになり、ステータスメッセージを表示します。IDBのエクスポートが完了するまでに数分かかることがあります。

   アップグレードが進行すると、追加のコマンドプロンプトウィンドウが開き、IDB構成情報とデータのData Protectorへのインポートのステータスが表示されます。

   8.00以降からのアップグレード：

   IDBは自動的に更新され、コマンドプロンプトウィンドウは表示されません。

   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。

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

7. セットアップ直後にData Protector GUIの使用を開始するには、[Launch Data Protector GUI]を選択します。

   `English Documentation (Guides, Help)`コンポーネントをアップグレードしたか、または新しくインストールした場合に、セットアップ直後にHPE Data Protector製品案内、ソフトウェアノート、およびリファレンスを表示するには、**[Open the Product Announcements, Software Notes, and References]**を選択します。

   [完了]をクリックします。

> **注：**
> 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。

以前のバージョンからのスケジュールの移行

Data Protector 10.00にアップグレードするとき、既存のスケジュールはすべて新しいWebベースのスケジューラに自動的に移行されます。手動による操作は不要です。

Data Protector 10.00へのアップグレードの際、既存のスケジュールファイルには.migrateというサフィックスが付きます。

たとえば、10.00より前のバージョンのData ProtectorでWeeklyBackupという名前のバックアップ仕様スケジュールを使用していた場合、このファイル名はアップグレード中にWeeklyBackup.migrateに変更されます。移行に失敗した場合、ファイル名は変更されません。

スケジュールが正しく移行されない場合、トラブルシューティングのために、HPEサポートからこれらの.migrateファイルの提供を求められる場合があります。

移行後のスケジュールファイルは以下の場所にあります。

仕様の種類	スケジュールのパス
バックアップスケジュール	Windowsの場合: *Data Protector_program_data*\OmniBack\Config\Server\amoschedules UNIXの場合: /var/opt/omni/server/amoschedules
統合スケジュール	Windowsの場合: *Data Protector_program_data*\OmniBack\Config\Server\Barschedules UNIXの場合: /var/opt/omni/server/Barschedules
コピー操作スケジュール	Windowsの場合: *Data Protector_program_data*\OmniBack\Config\Server\copylists\scheduled\schedules UNIXの場合: /var/opt/omni/server/copylists/scheduled/schedules
集約操作スケジュール	Windowsの場合: *Data Protector_program_data*\OmniBack\Config\Server\consolidationlists\scheduled\schedules UNIXの場合: /var/opt/omni/server/consolidationlists/scheduled/schedules
検証操作スケジュール	Windowsの場合: *Data Protector_program_data*\OmniBack\Config\Server\verificationlists\scheduled\schedules UNIXの場合: /var/opt/omni/server/verificationlists/scheduled/schedules
レポートグループスケジュール	Windowsの場合: *Data Protector_program_data*\OmniBack\Config\Server\rptschedules UNIXの場合: /var/opt/omni/server/rptschedules

アップグレードプロセスでスケジュールの移行に失敗した場合、既存のスケジュールを新しいスケジューラに正常に移行するために、以下のコマンドを手動で実行することができます。

```
omnidbutil -migrate_schedules
```

> **注：**
> 以前のバージョンのData Protectorでは、追加されたスケジュールに名前属性はありませんでした。そのため、移行後のスケジュールの名前は...と表示されます。この部分を編集して、スケジュールに名前を付けることができます。

第8章: Data Protector Licensing

この章は、次の項目で構成されています。

- 新たに導入されたライセンスキー
- Data Protectorライセンスのチェックとレポート
- 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

HPE Data Protector製品を使用するにはライセンスキーを取得する必要があります。

Data Protectorでは、最初のインストール時に一時(評価用)ライセンスを取得します。

評価用ライセンスは60日間有効です。Data Protectorの使用を続行するには、60日の期間が経過する前に恒久ライセンスを取得する必要があります。恒久ライセンスの取得については、ライセンスの取得、ページ 285の項を参照してください。

この章では以下の項について説明します。

- ライセンスの種類、下 - **機能ベースのライセンス**は、機能とバックアップターゲットに基づきます。**容量ベースのライセンス**は、HPE Data Protectorによって保護されるオリジナルのソースデータのボリュームに基づきます。
- ライセンスの種類の選択、ページ 284 - この項では、機能ベースのライセンスと容量ベースのライセンスの違いを説明します。機能モデルと容量モデルは同じカスタマーが使用することができますが、これらのモデルを同じCell ManagerまたはMoM環境で組み合わせて使用することはできません。
- ライセンスの取得、ページ 285 - この項では、新しいライセンスキーの取得方法とパスワードの請求方法についての詳細を説明します。
- 集中型ライセンス、ページ 293 - 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。
- ライセンスレポート、ページ 293 - 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。

ライセンスの種類

HPE Data Protectorでは、次の2つのライセンス方式がサポートされます。

- 機能とバックアップターゲットに基づく**機能ベースのライセンス**。機能ベースのライセンスは従来ベースのライセンスとも呼ばれます。
- HPE Data Protectorによって保護される元のソースデータのボリュームに基づく**容量ベースのライセンス**。容量の測定単位は、フロントエンドテラバイト/TBです。

機能ベースのライセンス

Data Protectorの製品構成と機能ベースのライセンスモデルには、主に次の3つのカテゴリがあります。

Cell Manager関連のライセンス

- **スターターパック:**

  Data Protectorスターターパックには以下が含まれています。

  - 指定したプラットフォーム(Windows、UNIX、Linux)上での1つのCell Manager。
  - ファイルシステムのバックアップのみ用の任意のプラットフォーム上での数が無制限のバックアップクライアント(エージェント)。
  - 1つのドライブライセンス(この場合のドライブはテープドライブ)
  - 最大60スロットのライブラリ
  - システムディザスタリカバリオプション
  - 基本レポート(Data Protector GUI内、およびWeb経由)

バックアップターゲット

- **ドライブとライブラリの使用権:**
  - バックアップドライブの使用権 - 1つのData Protectorセル内のスターターパックで使用できるドライブに加え、さらに多くのドライブ数を管理するためのライセンスが含まれています
  - ライブラリの使用権 - スターターパックで使用可能なライブラリに加え、1つのData Protectorセル内でより多くの利用可能な物理スロット数を使用してテープライブラリを管理するための使用ライセンス(LTU)が含まれています。

前述のいずれかのソース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ベース使用権の存在とその数がチェックされます。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。

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。

以下のバックアップターゲットは、容量でライセンスされます。

- UNIXゼロダウンタイムバックアップ使用権(1TB、10TB)
- UNIXゼロダウンタイムバックアップ使用権(非HPEアレイ、1 TB)
- 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ゼロダウンタイムバックアップ使用権(非HPEアレイ、1 TB)
- 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ゼロダウンタイムバックアップ使用権(非HPEアレイ、1 TB)
- 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)

容量ベースのバックアップターゲットのライセンス(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の容量と比較されます。アドバンストバックアップ使用権については、アドバンストバックアップ使用権、次のページを参照してください。

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。

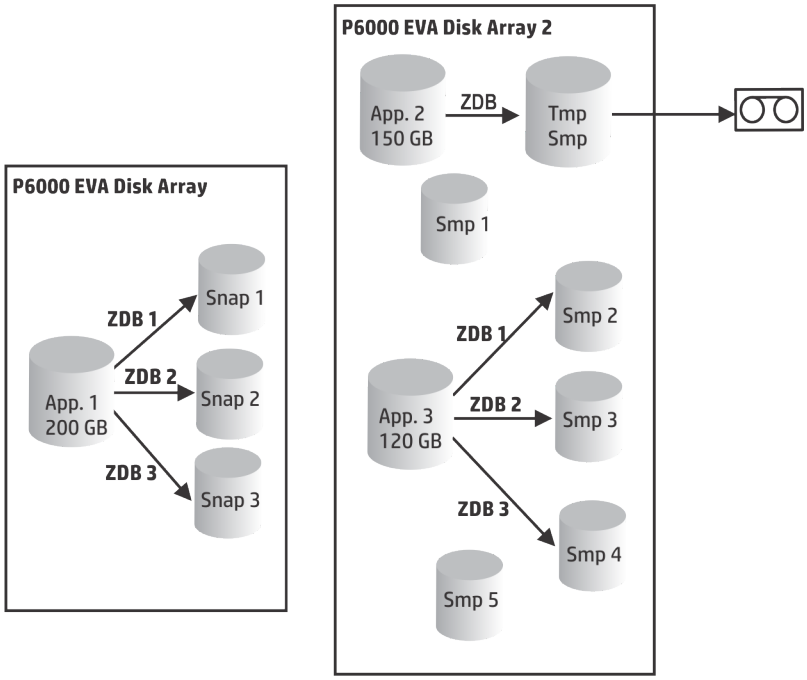
バックアップターゲットに適用される使用容量の計算

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。バックアップセッションは1日に3回実行され、それぞれのセッションにインスタントリカバリオプションが設定されています。一度に3つの複製が保存され、これらが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120 GB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つの複製がローテーションされます。使用容量の計算シナリオ、次のページを参照してください。

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回しかカウントしないので、200GB (App.1) + 120GB (App.3) = 320GBとなります。

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が必要です。仮想テープライブラリ(VTL)には、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。

- 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可能な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。
  - 合成フルバックアップ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。
  - 仮想テープライブラリ(VTL)の使用可能なネイティブ容量は、すべてのHPEData Protectorの保護バックアップにより使用される仮想テープライブラリのディスクのサイズです。このサイズは、VTLにより報告されます。
  - VTLごとに、ディスクまたはテープドライブのライセンスモデルにバックアップを使用するかどうかを選択できます。VTL内では、両方の概念を混合させ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が必要ありませんが、***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SCSI IIライブラリなどの通常のライブラリとして扱い、容量ベースのライセンスを使用しません。容量ベースのライセンスを有効にするには、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をグラフィックユーザーインターフェイス(GUI)を使用して構成する方法は、『*HPE Data Protector ヘルプ*』のキーワード「仮想テープライブラリ」で表示される内容を参照してください。VTLをコマンドラインインターフェイス(CLI)を使用して構成する方法は、後述の例、下を参照してください。

- Manager-of-Manager (MoM)によるライセンスの集中管理では、ディスク用拡張バックアップ機能を使用して各セルに少なくとも1 TBを割り当てる必要があります。

> **注:**
> Data Protectorは、最新の仮想テープライブラリおよびData Protector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ーフェイスが欠けているために、必要なライセンスの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ーフェイス(CLI)で「VTL_2011」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の推定容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:**
> 推定仮想ライブラリ容量消費量の値(`VTLCAPACITY`)は、「`Invalid VTL capacity specified`」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_2011 -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_2011
```

```
#omnidownload -library VTL_2011
NAME "VTL2011"
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
------------------------------------------------------------------
License Category               : Advanced Backup to disk for 1 TB
Licenses Capacity Installed    : 5 TB
使用されているライセンス容量        : 12.0 TB必要な追加ライセンス: 7 TB

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
保護されたデータの合計          1 TB
```

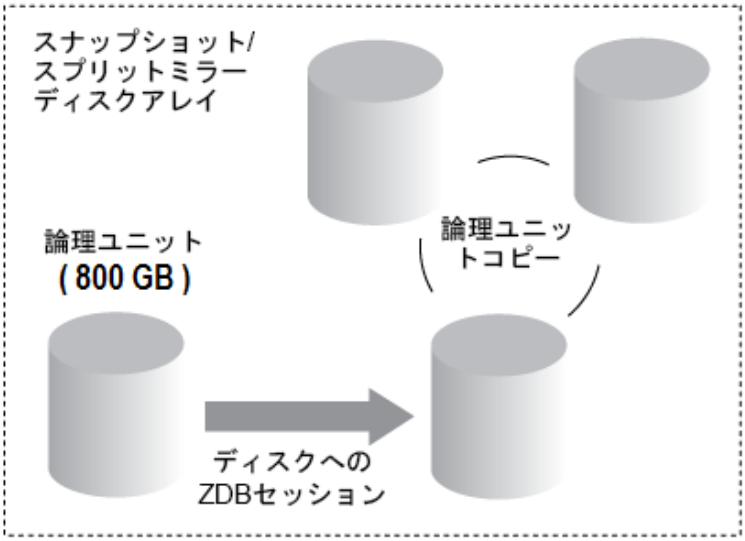
ライセンスを受けた容量ベースのバックアップターゲットの例

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

ディスクへのZDBセッション、下では、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。

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。

ディスクへのZDB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 800 GB = 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3つの複製が保管されます。ここで、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

したがって、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つと「インスタントリカバリ使用権(1TB)」ライセンスが1つあれば十分です。

例 2

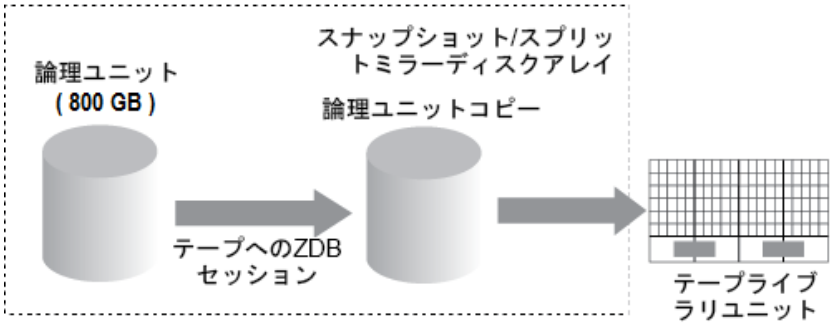
テープへのZDBセッション、下では、800GBの論理ユニット1つからのデータが、テープへのZDB (ZDB-to-Tape)セッションで1日に2度バックアップされる状況が例として示されています。したがって、インスタントリカバリ用のスプリットミラーコピーまたはスナップショットコピー(複製)は保管されません。この場合、容量ベースのライセンスは、以下のように計算します。

ディスクへのZDB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 800 GB = 0.8 TB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。

テープへのZDBセッション



例 3

ディスク+テープへのZDBセッション、次のページでは、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。

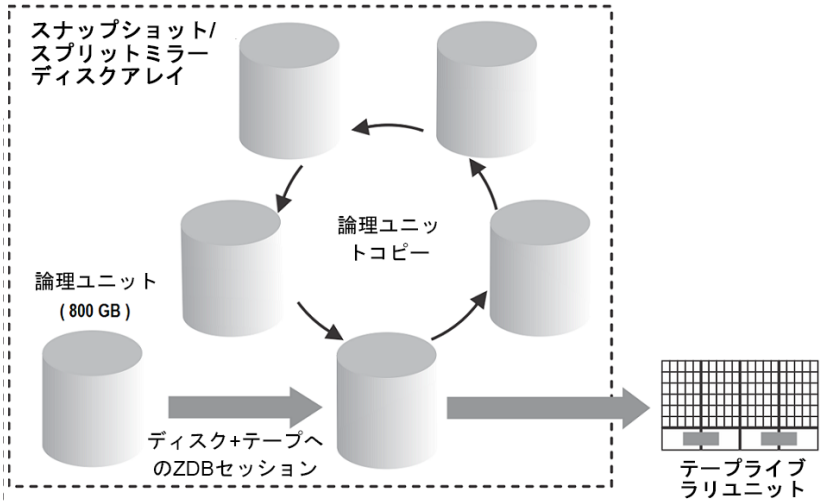
1 x 800 GB = 0.8TB用として「ゼロダウンタイムバックアップ使用権(1TB)」ライセンス

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。ここで、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つと「インスタントリカバリ使用権(1TB)」ライセンスが1つあれば十分です。

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、120GB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 x120GB + 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

インスタントリカバリに備えて、1つの200GBの論理ユニット、1つの120GBの論理ユニット、および1つの300GBの論理ユニット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が保管されるため、以下のライセンスが必要です。

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(1TB)」ライセンス

ディスク+テープへのZDBセッション、上からディスクへのZDBセッション、ページ 279で示した3つの例を1つのセルで構成する場合、「ゼロダウンタイムバックアップ使用権(1TB)」ライセンス1つと、「インスタントリカバリ使用権(1TB)」ライセンス1つで十分対応できます。

機能使用権:

- オンラインバックアップ使用権 - アプリケーションの実行中にアプリケーションサーバー、仮想環境をバックアップする権利。
- 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)
- Manager-of-Managers機能。
- メディアスロット数が60を超えるライブラリ。
- Data Protectorクライアントシステム暗号化使用権(1台)
- NDMPバックアップ。
- 1台のデータベースサーバーのGranular Recovery Extension。

- ゼロダウンタイムバックアップ(ZDB)使用権 - HPストレージシステム用のアレイベースのスナップショットをバックアップする権利。
- インスタントリカバリ(IR)使用権 - アレイベースのスナップショットから作成されたバックアップから復元する権利。
- ディスクへのアドバンストバックアップ使用権 - 1TBのバックアップディスクストレージの使用権が含まれます。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。このライセンスは、Data Protectorのファイルライブラリへのバックアップ、およびData Protectorのディスクへのバックアップデバイスのタイプに必要です。仮想テープライブラリへのバックアップを行うドライブライセンスの代わりに使用することができます。

容量ベースのライセンス

容量ベースの製品構成は、HPEData Protectorによって保護されるプライマリデータのボリュームに基づいており、エンタープライズ保護機能の無制限の使用権が含まれています。容量の測定単位は、"フロントエンドテラバイト"またはフロントエンドTBです。フロントエンドテラバイトの合計数は、Cell Managerのバックアップ対象のすべてのシステムの総データ量として定義されます。システムごとに最大フル(つまり、保護対象ソースデータの量)として測定されます。このライセンスモデルは、既存のインフラストラクチャーに適用できます。新しいインフラストラクチャーは同一ライセンスに自動的に組み込まれます。

CBLには計算に入れるすべての保護されたデータが含まれますが、CBLは現在のライセンスの種類とバックアップで使用された元のライセンスの種類を区別することはできません。バックアップに含まれていない(存在しない)システムを別のメディアにコピーして、そのメディアをCell Managerシステムからエクスポートすることができます。

> **注:**
> IDBオブジェクトはCBLの計算には含まれません。

容量ベースのライセンスを使用する場合、ライセンス構成に以下のモジュールが含まれています。

- Cell ManagersとManager of Managers
- テープドライブとライブラリ
- オンラインバックアップとGranular Recovery Extensions
- 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
- ディスクへのアドバンストバックアップとNDMP

以下は、容量ベースライセンスには含まれず、容量ベースのライセンスとは別売の製品です。

- 暗号化ソフトウェア
- HPE Backup Navigator
- HPE Storage Optimizer
- HPE DP Extended Online Backup
- 非HPEアレイ用のData Protectorダウンタイムバックアップ(ZDB)
- Data Protector管理パックには、HPE Operations ManagerとMicrosoftのSystems Center用のDP Smartプラグインが含まれています。

容量ティア、説明、製品番号については、Data Protector QuickSpecsを確認してください。

容量ベースのライセンスレポート

容量ベースのライセンスモードでは、容量ベースのライセンスの数(1TB単位)、および容量ベースのライセンスでカバーされないライセンス(つまり、ソフトウェア暗号化使用権)の数のみがリストされます。容量ベースのライセンスでカバーされている機能ベースのライセンスは表示されません。

```
#omnicc -check_license -detail

WARNING: Calculation of total protected data size may take some time.

Report generated            : 03/03/2016 1:48:27 AM
Licensing mode              : Server
License server              : host.domain.com
------------------------------------------------------------------------------
---
License Category               : Encryption Extension for one client system
Licenses Installed             : 0
Licenses Used                  : 0
Additional Licenses Required   : 0
------------------------------------------------------------------------------
---
License Category               : HPE Data Protector - capacity based per TB SW
Licenses Capacity Installed    : 9 TB
Licenses Capacity In Use       : 0 TBLicenses Capacity Required : 0 TB
------------------------------------------------------------------------------
---
.
.
.

Summary
-------
Licensing is covered.
Total Protected Data        : 4,00 TB

------------------------------------------------------------------------------
---
Backup Type                                    |       Total Protected Data
------------------------------------------------------------------------------
---

MS Filesystem                                  |       1 GB
MS SQL                                         |       1 GB
SAP                                            |       1 GB
UNIX Filesystem                                |       1 GB

------------------------------------------------------------------------------
```

「保護されているデータ合計」は、すべてのシステムからバックアップされているデータの総量と定義されます。各システムの「保護されているデータ合計」は、以下の合計として測定されます。

- ファイルシステムの各オブジェクトの最大フルバックアップ(合成バックアップを含む)と仮想環境バックアップの合計。
- 各アプリケーション統合バックアップの各データセットの最大フルバックアップの合計。

> **注:**
> 各ファイルシステムと仮想環境の固有オブジェクトは、バックアップ時に作成される実際のオブジェクトです。実際のオブジェクトは、マウントポイント、仮想マシン、仮想マシンのディスクのいずれかです。
>
> 各アプリケーション統合の固有データセットは、異なって識別されます。通常、これはデータベースインスタンスまたはサーバー名です。

制限事項

- 同じデータを複数の異なるエージェントでバックアップする場合、バックアップが複数回計算されます。以下にこのような2重計算の例をいくつか示します。
  - VSSを使用したデータベースのファイルシステムのバックアップと、同じデータベースのアプリケーション統合エージェントのバックアップ。
  - 仮想ホストの仮想環境統合のバックアップと、その仮想マシン(ホスト)内部で実行されるファイルシステムのエージェントのバックアップ。

    > **注:**
    > 2重計算に対処するには、固有オブジェクトをバックアップすることが推奨されます。

- Oracleバックアップのオブジェクト名フォーマットが外的に構成されると、データベース名が、新しいオブジェクト名から解決されない場合があります。こうしたオブジェクトのサイズは、保護されているデータ合計の計算中に正確に処理されない可能性があります。

  > **注:**
  > 保護されているデータ合計のサイズ計算にOracleオブジェクトを正しく追加するには、再構成されたフォーマットにも、`<DBID_*.dbf`として定義されたOracleデータベース名を含めておくことが不可欠です。

- 現時点では、VM内で実行されているインストール済みのDisk Agentを経由して、仮想環境エージェントによってバックアップされたVMware VM、およびVEPAとDisk Agentが同じデータ上で実行されていることを調べる方法がData Protectorにはありません。

ライセンスの種類の選択

機能ベースモデルと容量ベースモデルは同一カスタマーが使用できますが、これらのモデルを同じCell ManagerまたはMoM環境で組み合わせて使用することはできません。一覧される補足製品のライセンスは例外であり、これらのライセンスはData Protectorの機能ベースと容量ベースの両方のライセンス方法でこれらのライセンスを組み合わせることができます。従来の製品構成から容量ベースの製品構成への移行がサポートされています。詳細については、認定されたHewlett Packard Enterprise販売担当者までお問い合わせください。両方のライセンスモデルはあらゆる規模の環境で有効です。

機能ベースのライセンスと容量ベースのライセンスの相違点:

- 機能ベースのライセンスは使用できる機能が少なく、エントリコストを低く抑えることができます。これに対し、容量ベースのライセンスは使用できる機能が多く、モデルの成長に合わせてコストをかけることができます。

- 機能ベースのライセンスは各Cell Managerやテープドライブなどに対して別途ライセンスが必要になり、ユーザーは最初に既存の環境を文書化し、自分の環境を保護するためのライセンスに必要なバックアップソフトウェア機能を選別する必要があります。
- 優れた柔軟性 - 容量ライセンスでは、保護が必要なクライアント上の全データを保護するために必要なライセンスは1つです。
- ただし、長期間にわたってデータを保持し、データに対して膨大な変更を加える予定があるが、必ずしも容量の増大は必要ないという場合、別の懸念を抱える可能性があります。このような場合では、もうひとつの選択肢である容量ベースモデルでは長期間にわたりコストがかかってしまう可能性があります。

機能ベースのライセンスを使用する理由

- 使用できる機能が少なくエントリコストを低く抑えることができる
- 組織内のデータが一定の割合で増加し続ける場合、機能ベースのライセンス方法を使用する方がコスト効果が高い場合があります。

容量ベースのライセンスを使用する理由

- Data Protectorによって保護された保護データ量に基づいている
- さらなるライセンスコストをかけることなく複数のバックアップコピーが可能
- エンタープライズ保護機能の無限の使用が提供される
- 新しいサーバーやストレージ、アプリなどに移行可能な恒久ライセンス
- OPEX管理に優れシンプルなサイジングを実現できる、高い拡張性と手頃な価格で提供される「成長に合わせてコストをかける」ライセンスモデル

ライセンスの取得

この項では、Data Protectorの新しいライセンスキーの取得方法、および既存のライセンスキーに対する新しいパスワードの請求方法について説明します。

新しいライセンスキーの取得

Data Protector 8.0以前で生成されたライセンスキーとパスワードは、ライセンステクノロジの問題のために最新バージョンのData Protectorと互換性がないので、アップグレードする必要があります。

Data Protector10.00以前に生成されたライセンスキーと既存のパスワードは、Data Protector 10.00以降と互換性がありません。Data Protector 10.00にアップグレードする場合は新しいライセンスが必要になります。

> **注:**
> Data Protector 10.00では、期限切れになったライセンスまたは無効なライセンスが表示されなくなりました。

新たに購入したライセンスの場合、パスワードの要求時に製品バージョン「Data Protector 10.00」を選択する必要があります。Data Protector 10.00用に生成されたパスワードは、以前のバージョンのData Protectorでは使用できません。

アップグレード後、Data Protector 10.00は60日間一時パスワードで動作します。一時パスワードでの動作は、新規インストールと変わりません。

重要:
Data Protector 10.00用の*少なくとも1つの新しいライセンスキー*がインストールされるとすぐに、一時パスワードはオフになり、インストールされた有効なキーのみが認識されるようになります。

アップグレード後の一時パスワードのアクティブ化は、一度しか行えません。

ヒント:
既存のライセンスは、アップグレード後も新しい(一時)ライセンスと並んで無効なライセンスとしてレポートされます。これを回避するには、`lic.dat`ファイルの名前を変更します(削除はしません)。

Windowsシステムの場合: ディレクトリ*Data_Protector_program_data*\Config\server\Cellに移動し、ファイルの名前を変更します。

```
ren lic.dat lic.bak
```

UNIXシステムの場合: ディレクトリ/etc/opt/omni/server/cellに移動し、ファイルを移動します。

```
mv lic.dat lic.bak
```

パスワードに関する考慮事項

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。

- 一時パスワードは組み込み型になっています。これらは、余分なライセンスパスワードの要件なしで60日間、すべての新規インストールおよびバージョン9.00以降にアップグレードされる既存のすべてのData Protectorインストールで使用できます。また、評価目的で製品版の機能が提供されます。

  60日経過後に一時パスワードの有効期限は切れ、恒久ライセンスキーをインストールしない限り、製品の動作は停止します。

  製品版の評価期間は、正規ライセンスキーの初回インストール時に終了します。ライセンスキーを少なくとも1つインストールすると、ライセンスキーのインストール目的となった機能しか使用できなくなります。
- 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HPE 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。
- セルごとに、Cell Managerライセンスが1つ必要です。
- 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キーまたはパスワード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。

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。

- Instant-On password

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*HPE 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。

既存のData Protectorインストールの場合、Data Protector 9.00以降へのアップグレード後60日間一時パスワードで動作します。この期間中に、アクティブなサポート契約に指定されているように、HPE Password Delivery Centerに新しい恒久パスワードを請求する必要があります。サポート契約でカバーされていない古いライセンスはアップグレードできません。

- 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て恒久パスワードを取得すると、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、HPE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、HPEのライセンスサイトを参照してくださいhttp://enterpriselicense.hpe.com/.

  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、*HPE 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://enterpriselicense.hpe.com/)を利用します。

パスワードの取得およびインストール方法の詳細については、恒久パスワードの取得、下を参照してください。

恒久パスワードの取得

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. 恒久パスワード*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のライセンスフォーム、ページ 289」を参照してください。
2. 請求フォームを送るときと同じ方法で、*HPE 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*HPE Password Delivery Center*サイト(http://enterpriselicense.hpe.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*HPE 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*HPE Password Delivery Center*にファックスで送付します。
     - *HPE 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またはインストール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用インストールパッケージの場合: \Docs\license_forms.txt

上記のフォームを使用して、*HPE Password Delivery Center (HPE 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。

恒久パスワードのインストール

この項では、*HPE Password Delivery Center (HPE 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:

*HPE Password Delivery Center*から恒久パスワードが届き、Cell ManagerにData Protectorユーザーインターフェイ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またはコピーします。

   パスワードは、4文字ごとの可変長グループをスペースで区切ったグループと、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。

   ```
   QB9A AQEA H9PQ KHU2 UZD4 H8S5 Y9JL 2MPL B89H MZVU EUJV KCS9 KHU4 9AC2 CRYP DXMR
   KLLK XVSS GHU6 D2RJ N6KJ 2KG8 PVRJ 37LX DJ2J EWMB A3PG 96QY E2AW WF8E NMXC LNCK
   ZVWM 9AKS PU3U WCZ8 PSJ5 PQKM 5KCC FYDE 4MPM 9GUB C647 WEQX 4NMU BGN5 L8SM 23TX
   ANTR VFPJ PSJL KTQW U8NK H4H4 TB4K L4XQ "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システムの場 合 :*Data_Protector_program_data*\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. 次 のコマンドを実 行 します。

   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、埋 め込 みの改 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 については、omniccのmanページまたは『*HPE 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システムの場 合 :*Data_Protector_program_data*\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Notepad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 については、グラフィカルユーザーインターフェイス用 のパスワードは、パスワード証 明 書 に記 載 されているとおりに入 力 またはコピーします。、前 のページを参 照 してください。

Data Protectorの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。

- オンラインの*Password Delivery Center*サイト(http://enterpriselicense.hpe.com/)にアクセスし、恒 久 パスワードを請 求 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システムまたはインストールメディアに含 まれています。

  HP-UXおよびLinuxシステムの場 合 : /opt/omni/doc/C/license_forms_UNIX

  Windows用 インストールパッケージの場 合 : 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。

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。

Licensing Data	Data Protectorセルに関するライセンス情報を記入します。
Current Cell Manager	現在のCell Managerに関して必要な情報を記入します。
New Cell Manager	新しいCell Managerに関して必要な情報を記入します。
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 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が定義されます。集中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。HPEでは、プライマリIPアドレスを入力することをお勧めしています。 HPE Serviceguard環境またはMicrosoft Cluster環境で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、『*HPE Data Protectorヘルプ*』を参照してください。
The *Password Delivery Center* Fax Numbers	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。
Product License Type	*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。

パスワードの検証

GUIを使用する場合

インストール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**[ライセンス...]**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。**[パスワード情報]**タブをクリックして、インストールされている有効なパスワードの詳細を表示します。無効なパスワードには、期限切れまたは抑制済みのマークが付けられます。

   個々の列と同様にポップアップウィンドウ全体もサイズ変更可能です。

CLIを使用する場合

インストール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。

```
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、注釈(`Password could not be decoded.`)が付きます。

インストール済みライセンスの確認

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]**、**[ライセンス...]**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。

```
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。

既存のライセンスのアップグレード

Data Protectorの既存のお客様の場合、古いライセンスパスワードを最新バージョンのData Protectorにアップグレードするには、現在使用中のライセンスの数量と種類をカバーする有効なサポート契約が締結されている必要があります。

新しいライセンスキーを受け取ったら、それをご使用のData Protector環境にインストールされているライセンスキーの数量および種類と比較する必要があります。ソフトウェアのアップグレードは、十分に有効なライセンスキーの所有を確認した後にのみ行ってください。

受け取った新しいライセンスキーがご使用のData Protector環境に実際にインストールされているライセンスキーの数量より少ないか異なる場合、最新バージョンのData Protectorへのアップグレードをしないでください。ライセンスキーの不足により、ご使用のData Protector環境が動作しなくなる可能性があります。

代わりに、まずHPEの営業担当またはHPEパートナーに問い合わせて、サポート契約の対象となるライセンス機能とData Protector 10.00より以前のバージョンのData Protectorで現在使用している実際のライセンスとのずれを埋めるのに必要な手順を特定してください。

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 ProtectorCell 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。

他のCell Managerシステムへのライセンスの移動

以下の場合は、*HPE 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:
UNIX用の製品ライセンスは、UNIX、Windows、およびNovell NetWareプラットフォームに適用でき、すべてのプラットフォームでその機能が提供されます。一方、Windows用の製品ライセンスは、Windows、Novell NetWare、およびLinuxプラットフォームにしか適用できません。

HP-UX用Cell Manager使用権は、任意のCell Managerプラットフォームに移動して使用できます。一方、WindowsまたはLinux用Cell Manager使用権は、HP-UX Cell Managerプラットフォームに移動して使用することはできません。

他のすべての使用権は、制限なしで任意のCell Managerプラットフォームに移動できます。Cell Managerプラットフォームの種類が使用権に対する何らかの制限を意味することはありません。たとえば、Windows用ドライブ使用権はHP-UX Cell Manager上にインストールできますが、UNIXシステムに接続されているドライブで使用することはできません。

別のCell Managerにライセンスを移動するには:

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、*HPE 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、ページ 300」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。

   または、Password Delivery CenterのWebサイト(http://enterpriselicense.hpe.com/)に移動し、ライセンス移動をオンラインで開始します。
2. 以下のファイルを削除します。

   Windowsシステムの場合:

   Data_Protector_program_data\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、HPE Password Delivery Center (PDData ProtectorC)に送付した後は、移動元のCell Managerからの*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は、新しいパスワードによって置き換えられます。

注:
Data Protectorは、Adaptive Backup and Recovery (ABR)スイートの一部として利用することもできます。ABRスイートは、非構造化ファイル解析および自動ストレージティアリング(Storage Optimizer)と、コアプロテクションエンジン(Data Protector)、レポートおよび動作解析ソフトウェアツール(Backup Navigator)を組み合わせて、リアルタイム解析と最適化に基づいたデータ保護に革新的な手法を提供します。

集中型ライセンス

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については、『*HPE Data Protectorヘルプ*』を参照してください。

> **注:**
> UNIX用の製品ライセンスは、UNIX、Windows、およびNovell NetWareプラットフォームに適用でき、すべてのプラットフォームでその機能が提供されます。一方、Windows用の製品ライセンスは、Windows、Novell NetWare、およびLinuxプラットフォームにしか適用できません。
>
> HP-UX用Cell Manager使用権は、任意のCell Managerプラットフォームに移動して使用できます。一方、WindowsまたはLinux用Cell Manager使用権は、HP-UX Cell Managerプラットフォームに移動して使用することはできません。
>
> 他のすべての使用権は、制限なしで任意のCell Managerプラットフォームに移動できます。Cell Managerプラットフォームの種類が使用権に対する何らかの制限を意味することはありません。たとえば、Windows用ドライブ使用権はHP-UX Cell Manager上にインストールできますが、UNIXシステムに接続されているドライブで使用す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。詳細については、『*HPE Data Protectorヘルプ*』のキーワード「MoM環境」で表示される内容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。

100TBライセンスの一部として、1つのライセンスキーを受け取ります。WebwareまたはHPEライセンスから複数のキーを取得することはできません。この1つのライセンスキーを使用するには、MoM環境で集中型ライセンスを使用する必要があります。別途1TBのLTUを追加購入する必要はなく、各Cell Managerに1TBのLTUが割当てられます(各Cell Managerに100GBが必要な場合でも)。

> **注:**
> 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。詳細については、『*HPE Data Protectorヘルプ*』のキーワード「MoM環境」で表示される内容を参照してください。

ライセンスレポート

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、`Data_Protector_program_data\log\server\Ob2EventLog.txt`(Windowsシステム)または`/var/opt/omni/server/log/Ob2EventLog.txt`(UNIXシステム)のCell Managerにあります。Data

Protectorチェックおよび保守メカニズムの詳細については、『*HPE Data Protectorヘルプ*』のキーワード「イベントログ、Data Protector」で表示される内容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 GUIの起動時にイベントログの通知が表示されます。Data Protectorのイベントログの詳細については、『*HPE Data Protectorヘルプ*』のキーワード「イベントログ、Data Protector」で表示される内容を参照してください。
- Data Protectorセッションの開始時にライセンスがチェックされ、見つからない場合は、レポートされます。

オンデマンドでライセンスレポートを作成する

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`オプションを指定すると、詳細なレポートが生成されます。ライセンスチェック機能により、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、保護されたデータの合計(TB)、および必要な追加ライセンス(容量)の情報が返されます。

`-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。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、保護されたデータの合計(TB)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、レポートの生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。
>
> 詳細については、`omnicc`のmanページまたは『*HPE Data Protector Command Line Interface Reference*』を参照してください。

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。

- Instant-On password

  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*HPE 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。

  既存のData Protectorインストールの場合、Data Protector 10.00以降へのアップグレード後60日間一時パスワードで動作します。この期間中に、アクティブなサポート契約に指定されているように、HPE Password Delivery Centerに新しい恒久パスワードを請求する必要があります。サポート契約でカバーされていない古いライセンスはアップグレードできません。

- 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て恒久パスワードを取得すると、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、HPE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、HPEのライセンスサイトを参照してくださいhttp://enterpriselicense.hpe.com/.

  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、*HPE 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://enterpriselicense.hpe.com/)を利用します。

パスワードの取得およびインストール方法の詳細については、恒久パスワードの取得とインストール、下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

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. 恒久パスワード*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、ページ 300」を参照してください。
2. 製品構成の詳細については、「Data Protectorの製品構成とライセンス、ページ 301」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、*HPE 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HPE Password Delivery Center*サイト(http://enterpriselicense.hpe.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*HPE 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HPE Password Deliv*ery Centerにファックスで送付します。*
- HPE Password Delivery Cente*r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またはインストール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`

  上記のフォームを使用して、*HPE Password Delivery Center (HPE 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。

この項では、*HPE Password Delivery Center (HPE 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

*HPE Password Delivery Center*から恒久パスワードが届き、Cell ManagerにData Protectorユーザーインターフェイ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またはコピーします。

   パスワードは、4文字ごとの可変長グループをスペースで区切ったグループと、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。

   ```
   QB9A AQEA H9PQ KHU2 UZD4 H8S5 Y9JL 2MPL B89H MZVU EUJV KCS9 KHU4 9AC2 CRYP DXMR
   KLLK XVSS GHU6 D2RJ N6KJ 2KG8 PVRJ 37LX DJ2J EWMB A3PG 96QY E2AW WF8E NMXC LNCK
   ZVWM 9AKS PU3U WCZ8 PSJ5 PQKM 5KCC FYDE 4MPM 9GUB C647 WEQX 4NMU BGN5 L8SM 23TX
   ANTR VFPJ PSJL KTQW U8NK H4H4 TB4K L4XQ "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システムの場合:`Data_Protector_program_data\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. 次のコマンドを実行します。

   ```
   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、埋め込みの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。例および詳細については、`omnicc`のmanページまたは『*HPE 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システムの場合:`Data_Protector_program_data\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。パスワードの例については、グラフィカルユーザーインターフェイス用の前のページ「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またはコピーします。、ページ 310」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

インストール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**[ライセンス...]**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。**[パスワード情報]**タブをクリックして、インストールされている有効なパスワードの詳細を表示します。無効なパスワードには、期限切れまたは抑制済みのマークが付けられます。

   個々の列と同様にポップアップウィンドウ全体もサイズ変更可能です。

CLIを使用する場合

インストール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。

```
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、注釈(`Password could not be decoded.`)が付きます。

インストール済みライセンスの確認

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]**、**[ライセンス...]**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。

```
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、HPE Password Del*ivery 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:**
> UNIX用の製品ライセンスは、UNIX、Windows、およびNovell NetWareプラットフォームに適用でき、すべてのプラットフォームでその機能が提供されます。一方、Windows用の製品ライセンスは、Windows、Novell NetWare、およびLinuxプラットフォームにしか適用できません。
>
> HP-UX用Cell Manager使用権は、任意のCell Managerプラットフォームに移動して使用できます。一方、WindowsまたはLinux用Cell Manager使用権は、HP-UX Cell Managerプラットフォームに移動して使用することはできません。
>
> 他のすべての使用権は、制限なしで任意のCell Managerプラットフォームに移動できます。Cell Managerプラットフォームの種類が使用権に対する何らかの制限を意味することはありません。たとえば、Windows用ドライブ使用権はHP-UX Cell Manager上にインストールできますが、UNIXシステムに接続されているドライブで使用することはできません。

別のCell Managerにライセンスを移動するには

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、*HPE 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、ページ 300」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。

または、Password Delivery CenterのWebサイト(http://enterpriselicense.hpe.com/)に移動し、ライセンス移動をオンラインで開始します。

2. 以下のファイルを削除します。

   Windowsシステムの場合:

   Data_Protector_program_data\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、HPE Password Delivery Center (PDData ProtectorC)に送付した後は、移動元のCell Managerから*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については、『*HPE Data Protectorヘルプ*』を参照してください。

> **注:**
> UNIX用の製品ライセンスは、UNIX、Windows、およびNovell NetWareプラットフォームに適用でき、すべてのプラットフォームでその機能が提供されます。一方、Windows用の製品ライセンスは、Windows、Novell NetWare、およびLinuxプラットフォームにしか適用できません。
>
> HP-UX用Cell Manager使用権は、任意のCell Managerプラットフォームに移動して使用できます。一方、WindowsまたはLinux用Cell Manager使用権は、HP-UX Cell Managerプラットフォームに移動して使用することはできません。
>
> 他のすべての使用権は、制限なしで任意のCell Managerプラットフォームに移動できます。Cell Managerプラットフォームの種類が使用権に対する何らかの制限を意味することはありません。たとえば、Windows用ドライブ使用権はHP-UX Cell Manager上にインストールできますが、UNIXシステムに接続されているドライブで使用す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。詳細については、『*HPE Data Protectorヘルプ*』のキーワード「MoM環境」で表示される内容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:**
> 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。詳細については、『*HPE Data Protectorヘルプ*』のキーワード「MoM環境」で表示される内容を参照してくださ

い。

Data Protector 10.00へのライセンス移行

Data Protector 8.1以降のサポート契約を結んでいるお客様は、サポート契約の対象となる全ライセンスの新しいライセンスキーを含め、Data Protector 10.00を無料で受け取ることができます。

Data Protector 10.00には、期限が切れたライセンス、または同じ製品バージョンで使用されないライセンスは表示されません。

ソフトウェアサポートオンライン(SSO) https://softwaresupport.hpe.com/でMyUpdatesポータルに移動できます。

ここから、お客様のアクティブなサポート契約(SAID)に従って、利用可能なソフトウェアとライセンスキーのダウンロードにアクセスできます。

SAIDに関連付けられているすべてのソフトウェアが表示されるので、Data Protector 10.00の前にあるボックスをオンにして、**[Get updates]**をクリックできます。というメッセージがあることに注意してください。

以下の3つのタブが表示されます。

- **Get software**: ソフトウェアをダウンロードできます。
- **Get licenses**: Data Protector 9.00以降に割り当てられるLTUを取得できます。
- **Get documentation:** 製品ドキュメントをダウンロードできます。

[Get license]リンクをクリックすると、HPE Software Licensing Portal (http://enterpriselicense.hpe.com/)の更新請求(update order)に移動します。ここで、Service Agreement Identifier (SAID)にある使用権と数量のライセンスキーを取得できます。

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。

- オンラインの*Password Delivery Center*サイト(http://enterpriselicense.hpe.com/)にアクセスし、恒久パスワードを請求します。
- 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システムまたはインストールメディアに含まれています。

  HP-UXシステムおよびLinuxシステムの場合:`/opt/omni/doc/C/license_forms_UNIX`

  Windowsインストールパッケージの場合:`DriveLetter: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。

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。

Licensing Data	Data Protectorセルに関するライセンス情報を記入します。
Current Cell Manager	現在のCell Managerに関して必要な情報を記入します。
New Cell Manager	新しいCell Managerに関して必要な情報を記入します。
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 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が定義されます。集中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。HPEでは、プライマリIPアドレスを入力することをお勧めしています。 HPE Serviceguard環境またはMicrosoft Cluster環境で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、『*HPE Data Protectorヘルプ*』を参照してください。
The *Password Delivery Center* Fax Numbers	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。
Product License Type	*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。

Data Protectorの製品構成とライセンス

パスワードに関する考慮事項

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。

- 一時パスワードは組み込み型になっています。これらは、余分なライセンスパスワードの要件なしで60日間、すべての新規インストールおよびバージョンData Protector 10.00以降にアップグレードされる既存のすべてのData Protectorインストールで使用できます。また、評価目的で製品版の機能が提供されます。

  60日経過後に一時パスワードの有効期限は切れ、恒久ライセンスキーをインストールしない限り、製品の動作は停止します。

  > **重要:**
  > 製品版の評価期間は、正規ライセンスキーの初回インストール時に終了します。ライセンスキーを少なくとも1つインストールすると、ライセンスキーのインストール目的となった機能しか使用できなくなります。

- 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*HPE 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。
- セルごとに、Cell Managerライセンスが1つ必要です。
- 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キーまたはパスワード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:**
> 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、またはセル間でライセンスを移動する場合(この場合、MoM機能を使用しない)は、*HPE 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。HPE 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」*の項を参照してください。

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。

- Instant-On password

  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*HPE 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。

  既存のData Protectorインストールの場合、Data Protector 10.00以降へのアップグレード後60日間一時パスワードで動作します。この期間中に、アクティブなサポート契約に指定されているように、HPE Password Delivery Centerに新しい恒久パスワードを請求する必要があります。サポート契約でカバーされていない古いライセンスはアップグレードできません。
- 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て恒久パスワードを取得すると、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、HPE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、HPEのライセンスサイトを参照してくださいhttp://enterpriselicense.hpe.com/.

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、*HPE 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://enterpriselicense.hpe.com/)を利用します。

パスワードの取得およびインストール方法の詳細については、恒久パスワードの取得とインストール、下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

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. 恒久パスワード*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、ページ 300」を参照してください。
2. 製品構成の詳細については、「Data Protectorの製品構成とライセンス、ページ 301」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、*HPE 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*HPE Password Delivery Center*サイト(http://enterpriselicense.hpe.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*HPE 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HPE Password Deliv*ery Centerにファックスで送付します。*
     - HPE 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またはインストール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`

       上記のフォームを使用して、*HPE Password Delivery Center (HPE 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。

この項では、*HPE Password Delivery Center (HPE 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

*HPE Password Delivery Center*から恒久パスワードが届き、Cell ManagerにData Protectorユーザーインターフェイ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またはコピーします。

   パスワードは、4文字ごとの可変長グループをスペースで区切ったグループと、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。

   ```
   QB9A AQEA H9PQ KHU2 UZD4 H8S5 Y9JL 2MPL B89H MZVU EUJV KCS9 KHU4 9AC2 CRYP DXMR
   KLLK XVSS GHU6 D2RJ N6KJ 2KG8 PVRJ 37LX DJ2J EWMB A3PG 96QY E2AW WF8E NMXC LNCK
   ZVWM 9AKS PU3U WCZ8 PSJ5 PQKM 5KCC FYDE 4MPM 9GUB C647 WEQX 4NMU BGN5 L8SM 23TX
   ANTR VFPJ PSJL KTQW U8NK H4H4 TB4K L4XQ "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システムの場合:*Data_Protector_program_data*\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. 次のコマンドを実行します。

   ```
   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、埋め込みの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。例および詳細については、omniccのmanページまたは『*HPE 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システムの場 合 :*Data_Protector_program_data*\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 については、グラフィカルユーザーインターフェイス用 の前 のページ「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 またはコピーします。、ページ 310」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

インストール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**[ライセンス...]**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。**[パスワード 情 報]**タブをクリックして、インストールされている有 効 なパスワード の詳 細 を表 示 します。無 効 なパスワードには、期 限 切 れまたは抑 制 済 みのマークが付 けられます。

   個 々 の列 と同 様 にポップアップウィンドウ全 体 もサイズ変 更 可 能 です。

CLIを使 用 する場 合

インストール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。

```
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、注 釈 (`Password could not be decoded.`)が付 きます。

インストール済 みライセンスの確 認

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]**、**[ライセンス...]**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。

   ```
   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、HPE Password Del*ivery 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:**
> UNIX用の製品ライセンスは、UNIX、Windows、およびNovell NetWareプラットフォームに適用でき、すべてのプラットフォームでその機能が提供されます。一方、Windows用の製品ライセンスは、Windows、Novell NetWare、およびLinuxプラットフォームにしか適用できません。
>
> HP-UX用Cell Manager使用権は、任意のCell Managerプラットフォームに移動して使用できます。一方、WindowsまたはLinux用Cell Manager使用権は、HP-UX Cell Managerプラットフォームに移動して使用することはできません。
>
> 他のすべての使用権は、制限なしで任意のCell Managerプラットフォームに移動できます。Cell Managerプラットフォームの種類が使用権に対する何らかの制限を意味することはありません。たとえば、Windows用ドライブ使用権はHP-UX Cell Manager上にインストールできますが、UNIXシステムに接続されているドライブで使用することはできません。

別のCell Managerにライセンスを移動するには

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、*HPE 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、ページ 300」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。

   または、Password Delivery CenterのWebサイト(http://enterpriselicense.hpe.com/)に移動し、ライセンス移動をオンラインで開始します。
2. 以下のファイルを削除します。

   Windowsシステムの場合:

   Data_Protector_program_data\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、HPE Password Delivery Center (PDData ProtectorC)に送付した後は、移動元のCell Managerからの*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については、『*HPE Data Protectorヘルプ*』を参照してください。

> **注:**
> UNIX用の製品ライセンスは、UNIX、Windows、およびNovell NetWareプラットフォームに適用でき、すべてのプラットフォームでその機能が提供されます。一方、Windows用の製品ライセンスは、Windows、Novell NetWare、およびLinuxプラットフォームにしか適用できません。
>
> HP-UX用Cell Manager使用権は、任意のCell Managerプラットフォームに移動して使用できます。一方、WindowsまたはLinux用Cell Manager使用権は、HP-UX Cell Managerプラットフォームに移動して使用することはできません。
>
> 他のすべての使用権は、制限なしで任意のCell Managerプラットフォームに移動できます。Cell Managerプラットフォームの種類が使用権に対する何らかの制限を意味することはありません。たとえば、Windows用ドライブ使用権はHP-UX Cell Manager上にインストールできますが、UNIXシステムに接続されているドライブで使用す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。詳細については、『*HPE Data Protectorヘルプ*』のキーワード「MoM環境」で表示される内容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:**
> 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。詳細については、『*HPE Data Protectorヘルプ*』のキーワード「MoM環境」で表示される内容を参照してください。

ライセンスパスワード

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 ProtectorCell 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。

パスワードに関する考慮事項

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。

- 一時パスワードは組み込み型になっています。これらは、余分なライセンスパスワードの要件なしで60日間、すべての新規インストールおよびバージョン9.00以降にアップグレードされる既存のすべてのData Protectorインストールで使用できます。また、評価目的で製品版の機能が提供されます。

  60日経過後に一時パスワードの有効期限は切れ、恒久ライセンスキーをインストールしない限り、製品の動作は停止します。

  製品版の評価期間は、正規ライセンスキーの初回インストール時に終了します。ライセンスキーを少なくとも1つインストールすると、ライセンスキーのインストール目的となった機能しか使用できなくなります。
- 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HPE 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。
- セルごとに、Cell Managerライセンスが1つ必要です。
- 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キーまたはパスワード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。

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。

- Instant-On password

  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*HPE 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。

  既存のData Protectorインストールの場合、Data Protector 9.00以降へのアップグレード後60日間一時パスワードで動作します。この期間中に、アクティブなサポート契約に指定されているように、HPE Password Delivery Centerに新しい恒久パスワードを請求する必要があります。サポート契約でカバーされていない古いライセンスはアップグレードできません。
- 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て恒久パスワードを取得すると、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、HPE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、HPEのライセンスサイトを参照してくださいhttp://enterpriselicense.hpe.com/.

  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、*HPE 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://enterpriselicense.hpe.com/)を利用します。

パスワードの取得およびインストール方法の詳細については、恒久パスワードの取得、下を参照してください。

恒久パスワードの取得

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. 恒久パスワード*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のライセンスフォーム、ページ 311」を参照してください。
2. 請求フォームを送るときと同じ方法で、*HPE 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*HPE Password Delivery Center*サイト(http://enterpriselicense.hpe.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*HPE 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HPE Password Deliv*ery Centerにファックスで送付します。*
     - HPE 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またはインストール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用インストールパッケージの場合:`Disk_Label:\Docs\license_forms.txt`

       上記のフォームを使用して、*HPE Password Delivery Center (HPE 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。

恒久パスワードのインストール

この項では、*HPE Password Delivery Center (HPE 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:

*HPE Password Delivery Center*から恒久パスワードが届き、Cell ManagerにData Protectorユーザーインターフェイ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またはコピーします。

   パスワードは、4文字ごとの可変長グループをスペースで区切ったグループと、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。

   ```
   QB9A AQEA H9PQ KHU2 UZD4 H8S5 Y9JL 2MPL B89H MZVU EUJV KCS9 KHU4 9AC2 CRYP DXMR
   KLLK XVSS GHU6 D2RJ N6KJ 2KG8 PVRJ 37LX DJ2J EWMB A3PG 96QY E2AW WF8E NMXC LNCK
   ZVWM 9AKS PU3U WCZ8 PSJ5 PQKM 5KCC FYDE 4MPM 9GUB C647 WEQX 4NMU BGN5 L8SM 23TX
   ANTR VFPJ PSJL KTQW U8NK H4H4 TB4K L4XQ "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システムの場合:*Data_Protector_program_data*\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. 次のコマンドを実行します。

   ```
   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、埋め込みの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。例および詳細については、omniccのmanページまたは『*HPE 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システムの場合:*Data_Protector_program_data*\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Notepadなどのエディターを使用して作成します。パスワードの例については、グラフィカルユーザーインターフェイス用のパスワードは、パスワード証明書に記載されているとおりに入力またはコピーします。、上を参照してください。

Data Protectorの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。

- オンラインの*Password Delivery Center*サイト(http://enterpriselicense.hpe.com/)にアクセスし、恒久パスワードを請求します。
- 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システムまたはインストールメディアに含まれています。

  HP-UXおよびLinuxシステムの場合:`/opt/omni/doc/C/license_forms_UNIX`

  Windows用インストールパッケージの場合:`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。

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。
Licensing Data	Data Protectorセルに関するライセンス情報を記入します。
Current Cell Manager	現在のCell Managerに関して必要な情報を記入します。
New Cell Manager	新しいCell Managerに関して必要な情報を記入します。
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 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が定義されます。集中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。HPEでは、プライマリIPアドレスを入力することをお勧めしています。 HPE Serviceguard環境またはMicrosoft Cluster環境で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、『*HPE Data Protectorヘルプ*』を参照してください。
The *Password Delivery Center* Fax Numbers	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。
Product License Type	*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。

パスワードの検証

GUIを使用する場合

インストール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**[ライセンス...]**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。**[パスワード情報]**タブをクリックして、インストールされている有効なパスワードの詳細を表示します。無効なパスワードには、期限切れまたは抑制済みのマークが付けられます。

   個々の列と同様にポップアップウィンドウ全体もサイズ変更可能です。

CLIを使用する場合

インストール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。

```
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、注釈(`Password could not be decoded.`)が付きます。

インストール済みライセンスの確認

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]**、**[ライセンス...]**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。

   ```
   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、HPE Password Del*ivery 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 :**
> UNIX用 の製 品 ライセンスは、UNIX、Windows、およびNovell NetWareプラットフォームに適 用 でき、すべてのプラットフォームでその機 能 が提 供 されます。一 方 、Windows用 の製 品 ライセンスは、Windows、Novell NetWare、およびLinuxプラットフォームにしか適 用 できません。
>
> HP-UX用 Cell Manager使 用 権 は、任 意 のCell Managerプラットフォームに移 動 して使 用 できます。一 方 、WindowsまたはLinux用 Cell Manager使 用 権 は、HP-UX Cell Managerプラットフォームに移 動 して使 用 することはできません。
>
> 他 のすべての使 用 権 は、制 限 なしで任 意 のCell Managerプラットフォームに移 動 できます。Cell Managerプラットフォームの種 類 が使 用 権 に対 する何 らかの制 限 を意 味 することはありません。たとえば、Windows用 ドライブ使 用 権 はHP-UX Cell Manager上 にインストールできますが、UNIXシステムに接 続 されているドライブで使 用 することはできません。

別 のCell Managerにライセンスを移 動 するには:

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、*HPE 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、ページ 300」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。

   または、Password Delivery CenterのWebサイト(http://enterpriselicense.hpe.com/)に移 動 し、ライセンス移 動 をオンラインで開 始 します。
2. 以 下 のファイルを削 除 します。

   Windowsシステムの場 合 :

   Data_Protector_program_data\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、HPE Password Delivery Center (PDData ProtectorC)に送 付 した後 は、移 動 元 のCell Managerから*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は、新 しいパスワードによって置 き換 えられます。

第9章: インストールのトラブルシューティングとアップグレード

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。一般的なトラブルシューティング情報については、『*HPE Data Protectorトラブルシューティングガイド*』を参照してください。

WindowsのCell Managerをインストールする際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Data Protector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Data Protectorから通知されます。

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 properties]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。

対処方法

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、次の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。

対処方法

TCP/IPの設定を確認します。詳細については、デフォルトのData Protector Inetポートの変更、ページ 345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コマンドが提 供されています。このコマンドでは、セル内 のあらゆる接 続のチェックが可 能ですが、Data Protectorセルで重 要な次 の接 続を検 証すれば十 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]
  ```

  ここで、*client* は、Data Protectorクライアントがチェックした名 前です。

- 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 細については、omnicheckman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、出 力メッセージ、次 のページを参 照してください。DNSの名 前解 決で問 題が発 生したことを示 すメッセージが表 示された場 合は、『*HPE 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。

出力メッセージ

出力メッセージ	意味
client_1 cannot connect to *client_2*	*client_2*への接続がタイムアウトしました。
client_1 connects to *client_2*, but connected system presents itself as *client_3*	*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 failed to connect to *client_2*	*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。
checking connection between *client_1* and *client_2*	
all checks completed successfully.	
number_of_failed_checks checks failed.	
client is not a member of the cell.	
client contacted, but is apparently an older version. Hostname is not checked.	

共通の問題のトラブルシューティング

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。

- The Windows Installer Service could not be accessed.
- This application must be installed to run.
- This patch package could not be opened.
- The system cannot open the device or file specified.

Data Protector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。

この問題は、Microsoftインストーラーのアップグレードプロシージャのエラーによるものです。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ーにインストールされるバージョン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をいずれのドメインにも所属していないシステムにインストールすると失敗する

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.
```

対処方法

以下の2通りの対処方法があります。

- Cell Managerをインストールしようとしている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
```

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、Data Protector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

インストールのキャンセル後に、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。

問題

以下のエラーが報告されます

```
"too many open files" error
```

Cell Request Server (CRS) は、多数の開いているファイルまたはソケットをサポートするためにその`ulimit`を調整します。通常は十分対応できます。"開いているファイルが多すぎます"エラーが表示される場合は、OSパラメーターを調整する必要があります。

対処方法

OSパラメーターは次の2つの側面に関係します。

- OSパラメーターは開いているファイルまたはソケットの制限を変更します。
- OSパラメーターは多数のソケット接続が存在するときにパフォーマンスに影響します。

以下のリストは不確定なものです。詳細については、OSのドキュメントを参照してください。

HP-UX

開いているファイルの最大数はカーネル変数によって設定されます。

設定するには、`kctune variable=value`を使用します。

表示するには、`kctune –v variable`または`kcusage`を使用します。

変数	デフォルト	有効な値	注記
maxfiles	2048	32 … 1,048,576 <= maxfiles_lim	プロセスあたりのファイル記述子の初期(ソフト)最大数 ulimit –Sn
maxfiles_lim	4096	32 … 1,048,576 >= maxfiles <= nfile/2	プロセスあたりのファイル記述子のハード最大数 ulimit -Hn
nfile	65,536	2048 … 2,147,483,647 >= 2*maxfiles_lim	ファイル記述子の最大数(システム規模)**注記:** nnn > nfile/2の場合も"ulimit –Hn nnn"は成功する

また、多数のソケットの場合、下の記述に従って`ndd`でネットワークパラメーターを調整します。

```
ndd -h tcp_time_wait_interval
ndd -h tcp_fin_wait_2_timeout
ndd -h /dev/tcp tcp_smallest_anon_port
vi /etc/rc.config.d/nddconf
```

Linux

カーネルパラメーターは以下の場所に保存されます。

```
/etc/sysctl.conf
```

sysctl.confファイルを編集するか、sysctl -w name=valueを呼び出すことができます。また、sysctl -pを使用して実行中のカーネルをロードするか、それに対応するprocfsファイルを修正することができます。たとえば、変数fs.file-maxは/proc/sys/fs/file-maxに一致します。

> **注：**
> デフォルト値は使用可能なメモリによって異なります。

変数	注記
fs.file-max	ファイル記述子の最大数(システム規模)。
net.core.somaxconn	リッスンソケットの保留接続のキューの最大長は増大する場合があります。
net.ipv4.tcp_max_syn_backlog	記憶された接続要求最大数。これは接続クライアントからのACKをまだ受信していません。

また、プリプロセス制限のデフォルト値は次の場所に保存されます。

```
/etc/limits.conf
```

(または)

```
/etc/security/limits.conf
```

UNIXシステムでのインストール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クライアントのインストールまたはアップグレードが失敗し、次のエラーメッセージが表示されることがあります。

```
Installation/Upgrade session finished with errors.
```

UNIXクライアントをリモートで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フォルダー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フォルダー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に十分な空き領域があることを確認した上で、インストール/アップグレード手順を再開します。

ディスクスペース要件は、「Data Protectorクライアントのインストール、ページ 54」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

swagentデーモンをいったん停止してから再起動します。これを行うには、/opt/omni/sbin/swagentdコマンドか、/opt/omni/sbin/swagentd -rコマンドのいずれかを実行して、プロセスを強制終了および再起動します。

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
```

以下を実行します。

```
launchctl load com.hp.omni
```

問題

UNIX用Cell Managerのインストール後にInetプロセスを開始できない

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.
```

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システムの場合 : `ps -ef | grep inetd`

Linuxシステムの場合 : `ps -ef | grep xinetd`

サービスを開始するには、次のコマンドを実行します。

HP-UXシステムの場合 : `/usr/sbin/inetd`

Linuxシステムの場合 : `rcxinetd start`

問題

有効な資格情報でLinuxクライアント上にプッシュインストールを行うと以下のエラーメッセージが表示される

```
[Critical] <iwf1114165.hpeswlab.net>  SSH configuration failed.Either the
credentials were wrong or some error occured.

<iwf1114165.hpeswlab.net> : Skipped  0%

[Critical] <iwf1114165.hpeswlab.net>  Error connecting to client
iwf1114165.hpeswlab.net

Skipping client!

[Normal]  Installation session finished on Mon 14 Nov 2016 03:13:52 PM IST.

Finished installation.
```

対処方法

Linuxクライアント上のssh サービスに対してパスワード認証が有効にされていることを確認します。有効でない合は、以下の手順を実行してください。

1. ssh configファイルに以下の文字列を追加して、認証を有効にします。

   PasswordAuthentication yes
2. sshサービスを再起動します。

Windowsシステムでのインストール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システムへのリモートインストールが失敗し、以下のエラーメッセージが報告されました。

```
[Normal] Connecting to client computer.company.com...

[Normal] Done.

[Normal] Installing the Data Protector bootstrap service on client
computer.company.com...

[Critical] Cannot connect to the SCM (Service Control Manager) on client
computer.company.com: [5] Access is denied.
```

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*

   ユーザーアカウントが、ローカルInet構成にまだ追加されていない必要があります。詳細については、『*HPE 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。

問題

Windowsクライアントのリモートインストールが失敗する(Windows XP)

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エクスプローラー]**または**[マイコンピューター]**を開き、**[ツール]**メニューをクリックして**[フォルダーオプション]**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。

- コンピューターがドメインのメンバーである場合
- `Network access: Sharing and security model for local accounts`セキュリティポリシーが次のように設定されている: `Classic: Local users authenticate as themselves`

問題

Windows 7またはWindows 2008 R2システムが接続されていない場合、デジタル署名の検証が失敗する可能性がある

デジタル署名の検証が、次のエラーメッセージで失敗します:

```
[Critical] <computer.company.com> [70:32] Digital Signature verification of the
install kit failed.
```

対処方法

以下のいずれかの操作を行います。

- インターネット接続を有効にし、適切な証明書が信頼できるルートおよび中間証明機関に自動的にインポートされるまで待ってください。

  (または)

- 切断されたシステム上で信頼できるルート証明書を更新する方法について、以下の記事を参照してください。

  https://support.microsoft.com/en-us/kb/3004394

  https://support.microsoft.com/en-us/kb/2813430

問題

Cell Managerをインストールすると、アプリケーションサーバーサービスが起動しない

アプリケーションサーバーサービスが以下のメッセージを表示して起動しない

```
Timeout reached before Data Protector Application Server started.
```

以下のエラーが、インストールサマリーログファイルに記録されます。

```
Caused by: org.jboss.as.cli.
CommandLineException: The controller is not available at localhost:9999
```

PATHシステム環境変数にディレクトリ%SystemRoot%\system32が含まれないため、インストールプロセスがさまざまなユーティリティにアクセスできません。

対処方法

PATH変数に%SystemRoot%\system32ディレクトリを追加します。

> **注：**
> 次のファイルは、Windowsシステムの%SystemRoot%\system32フォルダーに格納されます(選択したコンポーネントによって異なります)。

BrandChgUni.dll	これは、リソースライブラリです。このライブラリは内部使用されるだけですが、レジストリ設定へのパスを含んでいるため、統合ソフトウェアのライブラリからアクセスできる既定の場所に格納する必要があります。
ob2informix.dll	このライブラリは、Informix Serverデータベースとの統合に使用されます。
snmpOB2.dll	このライブラリは、システムSNMPトラップの実装に使用されます。

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。
- インストール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

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、『*HPE Data Protectorヘルプ*』を参照してください。

インストールが正常に完了しなかった場合は、ログファイルの使用、ページ 331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man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

製品の旧バージョンを長いパスでインストールすると、アップグレードが失敗する

Data Protectorでは、80文字より長いパスへのCell Managerのインストールはサポートされていません。この結果、アップグレードが失敗します。

対処方法

1. インストールパッケージの`x8664\tools\Upgrade`ディレクトリから一時ディレクトリ(`c:\temp`など)に`omnimigrate.pl`スクリプトをコピーします。
2. 次の`omnimigrate`コマンドを使用してIDBをエクスポートします。

   ```
   perl c:\temp\omnimigrate.pl -export -shared_dir c:\output
   ```

   Data ProtectorインストールのデフォルトのコマンドディレクトリにあるPerlバージョンを使用します。
3. Data Protectorの旧バージョンを削除しますが、構成とデータベースデータは残します。*Data_Protector_program_data*`\db40`ディレクトリは削除しないでください。
4. Data Protector 10.00をインストールします。インストール先のパスが80文字以下であることを確認します。
5. 以下を実行して、すべてData Protectorサービスを停止します。

   ```
   omnisv –stop
   ```
6. 古い*Data_Protector_program_data*`\db40`ディレクトリ(このディレクトリは旧バージョンのData Protectorの削除後も残っています)から新しい*Data_Protector_program_data*`\db40`フォルダーにファイルをコピーします。DCBFディレクトリが移動していないことを確認してください。
7. 古い*Data_Protector_program_data*`\Config\Server`フォルダーから新しいフォルダーに構成をコピーします。
   a. 古い構成ディレクトリを新しい構成ディレクトリにコピーします。ただし古いファイルはそのまま残します。ファイルは*Data_Protector_program_data*`\Config\Server\install`ディレクトリからコピーしないでください。
   b. セル構成(クライアント、インストールサーバー)を保持する場合、*Data_Protector_program_data*`\Config\Server\cell\cell_info`および*Data_Protector_program_data*`\Config\Server\cell\installation_servers`ファイルをコピーして上書きします。
8. 次の手順を実行して、新しい通知とグローバルオプションファイルをマージします。
   a. 通知をマージするには、次の`omninotifupg.exe`ツールを実行します。

      ```
      omninotifupg.exe -quiet
      ```
   b. グローバルオプションファイルをマージするには、以下を実行します。

```
mrgcfg.exe –global -except BackupDeviceIdle -rename
DbFVerLimit=DbFnamesDatLimit,SessSucessfulWhenNoObjectsBackedUp
=SessSuccessfulWhenNoObjectsBackedUp
```

上 記 の手 順 を実 行 する代 わりに、以 前 行 ったインストールから手 動 でグローバルオプションファイルをマージすることもできます。

9. Data Protectorサービスを開 始 します。

   ```
   omnisv -start
   ```

10. IDBを新 しいインストールにインポートします。以 下 を実 行 します。

    ```
    omnimigrate.pl -import -shared_dir c:\output -force
    ```

問 題

製 品 の旧 バージョンのインストールパスにサポートされていない文 字 が含 まれていると、アップグレード が失 敗 する

Data Protectorでは、以 下 の文 字 を含 むパスへのCell Managerのインストールはサポートされていません。

- 非ASCII文 字
- "@ "または"# "
- ディレクトリの末 尾 にある"!"

この結 果 、アップグレード が失 敗 します。

対 処 方 法

1. インストールパッケージの`x8664\tools\Upgrade`ディレクトリから一 時 ディレクトリ(`c:\temp`など)に`omnimigrate.pl`スクリプトをコピーします。
2. ASCII名 を使 用 して次 のような2つのディレクトリを作 成 します。

   ```
   c:\output\cdb
   ```

   ```
   c:\output\mmdb
   ```

3. MMDBとCDBをエクスポートします。

   ```
   omnidbutil -writedb -cdb c:\output\cdb -mmdb c:\output\mmdb
   ```

   この処 理 には時 間 がかかる場 合 があります。アップグレード にはこのデータは必 要 ないので、ファイル名 のエクスポート が開 始 されたら、**Ctrl+C**を使 用 して`omnidbutil`プロセスを停 止 できます。
4. 次 の`omnimigrate`コマンド を使 用 してIDBをエクスポートします。

   ```
   perl c:\temp\omnimigrate.pl -exportNonASCII -shared_dir c:\output
   ```

   Data Protectorインストールのデフォルト のコマンド ディレクトリにあるPerlバージョンを使 用 します。
5. ANSI文 字 セットファイル`c:\output\old_cm`を作 成 します。このファイルには以 下 の2つの行 を含 めます。

   ```
   OLDCM_SHORTNAME=OldCmName
   OLDCM_ENDIANNESS=LITTLE_ENDIAN
   ```

   *OldCmName*を、Cell Managerの省 略 名 に置 き換 えます。
6. Data Protectorの旧 バージョンを削 除 しますが、構 成 とデータベースデータは残 します。*Data_Protector_program_data*`\db40`ディレクトリは削 除 しないでください。
7. Data Protectorをインストールします。インストール先 のパスに非ASCII文 字 が含 まれていないことを

確認します。

8. 以下を実行して、すべてData Protectorサービスを停止します。

   ```
   omnisv –stop
   ```

9. 古い*Data_Protector_program_data*\db40ディレクトリ(このディレクトリは旧バージョンのData Protectorの削除後も残っています)から新しい*Data_Protector_program_data*\db40フォルダーにファイルをコピーします。DCBFディレクトリが移動していないことを確認してください。
10. 古い*Data_Protector_program_data*\Config\Serverフォルダーから新しいフォルダーに構成をコピーします。
    a. 古い構成ディレクトリを新しい構成ディレクトリにコピーします。ただし古いファイルはそのまま残します。ファイルは*Data_Protector_program_data*\Config\Server\installディレクトリからコピーしないでください。
    b. セル構成(クライアント、インストールサーバー)を保持する場合、*Data_Protector_program_data*\Config\Server\cell\cell_infoおよび*Data_Protector_program_data*\Config\Server\cell\installation_serversファイルをコピーして上書きします。
11. 次の手順を実行して、新しい通知とグローバルオプションファイルをマージします。
    a. 通知をマージするには、次のomninotifupg.exeツールを実行します。

       ```
       omninotifupg.exe -quiet
       ```

    b. グローバルオプションファイルをマージするには、以下を実行します。

       ```
       mrgcfg.exe –global -except BackupDeviceIdle -rename
       DbFVerLimit=DbFnamesDatLimit,SessSucessfulWhenNoObjectsBackedUp
       =SessSuccessfulWhenNoObjectsBackedUp
       ```

       上記の手順を実行する代わりに、以前行ったインストールから手動でグローバルオプションファイルをマージすることもできます。
12. Data Protectorサービスを開始します。

    ```
    omnisv -start
    ```

13. IDBを新しいインストールにインポートします。以下を実行します。

    ```
    omnimigrate.pl -import -shared_dir c:\output -force
    ```

問題

古い(Raima DBベースの)IDBが破損していると、アップグレードプロセスが中止される

アップグレード中に、IDB内の次の破損フィールドが検出され、修正されます。

- メディアblocks_usedは0に設定される
- メディアblocks_totalはblocks_usedに設定される
- プールmedia_age_limitがデフォルト値(同じメディアクラスを持つデフォルトプールのmedia_age_limit)に設定される
- プールmedia_overwrite_limitがデフォルト値(同じメディアクラスを持つデフォルトプールのmedia_overwrite_limit)に設定される

ただし、IDB内のその他のフィールドが破損していると、アップグレードは中止されます。

対処方法

次の手順を実行して、Data Protectorのインストールを古いバージョンに戻します。

1. 現行バージョンのData Protectorを削除します。
2. 旧バージョンのData Protectorを再インストールします。
3. 古いIDBを復元します。

もう一度アップグレードを試みる前に、古いIDBを修復する必要があります。詳細については、HPEサポートに問い合わせてください。

問題

アップグレード後、`omnidbcheck -bf`が失敗しエラーが表示される

以前のリリースのData Protector、`omnidbcheck -bf`は、実際のサイズとDCバイナリファイル内のメディアのヘッダーサイズの間の不整合によるエラーを正しく報告しませんでした。

`omnidbcheck -bf`は、アップグレードする前にIDBに存在する可能性がある整合性に関するすべてのエラーを正しく報告します。

対処方法

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

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

   詳細については、『*HPE Data Protectorヘルプ*』および『*HPE Data Protectorトラブルシューティングガイド*』の「IDBのDCBF部分の[警戒域]レベルの破損に対処する」を参照してください。詳細については、HPEサポートに問い合わせてください。

問題

Velois IDBが破損していると、アップグレードプロセスが中止される

アップグレード中に、IDB内の次の破損フィールドが検出され、修正されます。

- メディア`blocks_used`は`99`に設定される
- メディア`blocks_total`は`blocks_used`に設定される
- プール`media_age_limit`がデフォルト値(同じメディアクラスを持つデフォルトプールの`media_age_limit`)に設定される
- プール`media_overwrite_limit`がデフォルト値(同じメディアクラスを持つデフォルトプールの`media_overwrite_limit`)に設定される

ただし、IDB内の以下のフィールドのいずれかが破損していると、アップグレードは中止されます。

メディア:`LAST_SEGMENT`

位置:

SEQUENCE_NR

START_SEGMENT

START_OFFSET

LOG_LEVEL

DCBF_OFFSET

DCBF_NUMOFDIRS

DCBF_NUMOFITEMS

DCBF_SIZE

対処方法

次の手順を実行して、Data Protectorのインストールを古いバージョンに戻します。

1. 現行バージョンのData Protectorを削除します。
2. 旧バージョンのData Protectorを再インストールします。
3. 古いIDBを復元します。

もう一度アップグレードを試みる前に、古いIDBを修復する必要があります。詳細については、HPEサポートに問い合わせてください。

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、GUIを使用したData Protectorパッチの確認、ページ 223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

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。

問題

Data Protector 10.00以降のバージョンにアップグレードした後で、復元操作を実行するとDCBFエラーメッセージが表示されるData Protector GUIでの[復元]コンテキストで、オブジェクトを選択してファイルを参照しようとすると、次のメッセージが表示されます。

```
[12:10907] Invalid format of detail catalog binary file
```

ただし、DCBFファイルは実際には破損していないので `omnidbcheck -dc`はエラーを報告しません。これは、バージョンの異なる2つのファイルが読み込まれるためにバージョンが一致しないことが原因で発生します。

対処方法

オプション1:復元セッションのコンテキストに移動し、1つのファイルを復元してみます。

オプション2:メディアをエクスポート/インポートし、DCBFカタログを再作成します。詳細については、『*HPE Data Protectorヘルプ*』の「*メディアのインポート*」および「*メディアのエクスポート*」を参照してください。

オプション3:カタログを移行します。`perl omnimigrate.pl -start_catalog_migration`

> **注:**
> カタログの移行が完全に終了したら(古いカタログがなくなったら)、グローバル変数`SupportOldDCBF`を`0`に変更してください。

問題

Data Protector 10.00以降のバージョンにアップグレードした後で、Data Protector 7.03でバックアップされた個別のディスクを復元用に選択した場合、Data Protector GUIに次のエラーメッセージが表示されます。

オブジェクト`scsi0:<disk number>`にはバージョン情報はありません。このオブジェクトのバックアップが完了していない可能性があります - 復元は不可能です。

復元オブジェクト '<VCenter host> 仮想環境 [<Data center>]'に問題が発生しました。バージョン情報が見つからないか、その他の競合が発生している可能性があります。復元が中止されました。

対処方法

完全な仮想マシンを復元用に選択してください。

問題

アップグレードの際、スケジュールの移行に失敗しました。

対処方法

アップグレードプロセスでスケジュールの移行に失敗した場合、既存のスケジュールを新しいスケジューラーに正常に移行するために、以下のコマンドを手動で実行することができます。

```
omnidbutil -migrate_schedules
```

Windowsシステムでのリモートアップグレードのトラブルシューティング

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.
```

この問題は、インストールサーバーコンピューター上の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ー上のData Protector Inetサービスが実行されている場合に発生します。多くの場合は、ローカルユーザーを使用したときに発生します。

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。

問題

アップグレード後にData ProtectorCell Request Server (CRS)を開始できない

CRSを手動で開始したときに次のエラーメッセージが表示されます。

```
Windows could not start the Data Protector CRS on Local Computer.

For more information, review the System Event Log. If this is a non-Microsoft service, contact the service vendor, and refer to service-specific error code 1007.
```

インストール後に次のエラーメッセージが表示されます。

```
Timeout reached before Data Protector CRS started.
```

対処方法

- `omnisv stop` コマンドを使用してData Protectorサービスを停止します。
- Task Managerを開き、残りのData Protectorプロセスを終了します。
- `omnisv start` コマンドを使用してData Protectorサービスを開始します。

UNIXシステムでのローカルアップグレードの手動処理

通常、UNIX Cell Managerおよびインストールサーバー上のData Protector 8.1以降は、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。「ネイティブツールを使用した、HP-UXおよびLinuxシステムでのアップグレード、ページ340」を参照してください。

クライアントを手動でアップグレードした後で、次の`omnicc`コマンドをCell Manager内で実行して、クライアント情報を更新します。

```
omnicc –update_host [hostname] -accept_host
```

セルに含まれるすべてのクライアント情報を更新するには、次のコマンドを実行します。

```
omnicc –update_all -accept_host
```

`omnicc`コマンドの詳細については、『*HPE Data Protector Command Line Interface Reference*』を参照してください。

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で問題が発生した場合、次のログファイルを確認します。

HP-UX Cell Manager:

- `/var/adm/sw/swinstall.log`
- `/var/adm/sw/swagent.log`(詳細)

Linux 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)
  ここで、
  - *did*(デバッグID)は、デバッグパラメーター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ホストの名前です。
  - *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で問題が発生した場合、次のログファイルを確認します。

UNIXの場合 インストールサーバー:

/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。「インストール実行トレースの作成、次のページ」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 Server 2008およびWindows Server 2012:*Data_Protector_program_data*\log

その他のWindowsシステムの場合:*Data_Protector_home*\log

HP-UXシステム、Solarisシステム、Linuxシステムの場合:/var/opt/omni/logと /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

インストール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	リモートインストールのトレース結 果 が記 録 されます。インストールサーバーに保 存 されます。
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、『*HPE Data Protectorトラブルシューティングガイド*』を参 照 してください。

インストール実 行トレースの作 成

HPEカスタマー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HPEカスタマー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 については、『*HPE Data Protectorトラブルシューティングガイド*』を参 照 してください。

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 1-200 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*
- リモートシステムの場 合 :

  SystemRoot:\Temp\OB2DBG_*did*__INSTALL_SERVICE_*Hostname_DebugNo_DebugPostfix*

付 録A: UNIXシステムネイティブツールを使 用したインストールとアップグレード

この付 録 では、HP-UXシステムのswinstallとLinuxシステムの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。

ネイティブツールを使 用した、HP-UXおよびLinuxシステムへのインストール

> **注:**
> 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。詳 細 は、「ネイティブツールを使 用した、HP-UXおよびLinuxシステムへのインストール、上 」を参 照してください。
>
> リモートインストールパッケージの限 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 のみ、これらのHP-UXおよびLinuxへのネイティブインストール手 順 を使 用してください。

swinstallを使 用したHP-UXシステムでの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

1. ダウンロードしたData Protectorインストールパッケージ(tar)をHP-UXにコピーし、ファイルをローカルディレクトリに展 開します。
2. /usr/sbin/swinstallユーティリティを実 行してください。
3. [Specify Source]ウィンドウで**[Network Directory/CDROM]**を選 択し、**[Source Depot Path]**に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。
4. インストール可 能 な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。
5. **[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 する場 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。

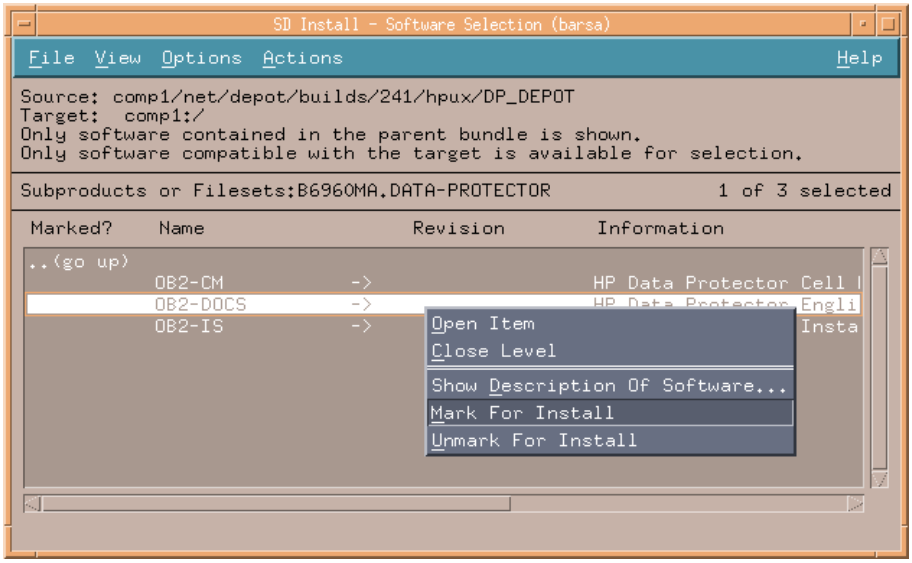
   以 下 のサブプロダクトが含 まれています。

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 とのData Protectorガイドと WebHelp形 式 の『*HPE Data Protector*ヘルプ』を収 録)
OB2-IS	Data Protector インストールサーバー

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。「 [SD install - software selection]ウィンドウ、下 」を参 照してください。

> **注:**
> 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 でユーザーインターフェイスコンポーネント(OMNI-CS)をインストールする必 要 があります。

[SD install - software selection]ウィンドウ



6. [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)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:**
> ネット ワーク上 のテープデバイスからソフト ウェアをインストールするには、まずソースディレクトリをコンピューターにマウントする必 要 があります。

rpmを使 用したLinuxシステムでの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

1. ダウンロードしたData Protectorインストールパッケージ(tar)をLinuxシステムにコピーし、ファイルをローカルディレクトリに展 開します。
2. linux_x86_64/DP_DEPOTディレクトリに移 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.10.00-1.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。

以下のコンポーネント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-TS-CORE	Data Protectorコアテクノロジスタックライブラリ
OB2-CC	Cell Consoleソフトウェア。これには、コマンドラインインターフェイスが含まれます。
OB2-TS-CS	Cell Managerテクノロジスタックライブラリ
OB2-TS-JRE	Data Protectorで使用するJavaランタイム環境
OB2-TS-AS	Data Protectorアプリケーションサーバー
OB2-WS	Data Protector Webサービス
OB2-JCE-DISPATCHER	ジョブコントロールエンジンのディスパッチャー
OB2-JCE-SERVICEREGISTRY	ジョブコントロールエンジンサービスのレジストリ
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形式とのData Protectorガイドと WebHelp形式の『*HPE Data Protectorヘルプ*』を収録)

> **重要:**
> Linuxのコンポーネントは相互に依存しています。これらのコンポーネントは、上記の順序でインストールする必要があります。

4. Data Protectorサービスを再起動します。

```
omnisv stop
omnisv start
```

swinstallを使用したHP-UXシステムでのインストールサーバーのインストール

1. ダウンロードしたData Protectorインストールパッケージ(tar)をHP-UXシステムにコピーし、ファイルをローカルディレクトリに展開します。
2. `/usr/sbin/swinstall`ユーティリティを実行してください。
3. [Specify Source]ウィンドウで**[Network Directory/CDROM]**を選択し、**[Source Depot Path]**に`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。

4. インストール可能なコンポーネントのリスト内で、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システム用の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。

   プロダクトには次のサブプロダクトコンポーネン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形式とのData Protectorガイドと WebHelp形式の『*HPE Data Protectorヘルプ*』を収録)
OB2-IS	Data Protectorインストールサーバー

5. [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。
6. [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。

インストールが終了すると、UNIXのソフトウェアデポは、`/opt/omni/databases/vendor`ディレクトリに置かれます。

> **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インストールパッケージ(tar)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しなければなりません。さらに、Data Protectorクライアント上のコンポーネントはパッチできなくなります。

rpmを使用したLinuxシステムで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. ダウンロードしたData Protectorインストールパッケージ(tar)をLinuxシステムにコピーし、ファイルをローカルディレクトリに展開します。
2. インストールアーカイブが格納されているディレクトリ(この場合は`linux_x86_64/DP_DEPOT`)に移動します。
3. 個々のコンポーネントについて、次のコマンドを実行します。

   `rpm -i package_name-A.10.00-1.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コンポーネント(*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-TS-CORE	Data Protectorコアテクノロジスタックライブラリ
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-TS-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テクノロジスタックソフトウェア
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ッケージ
OB2-MAP	すべてのUNIXシステム用 のMedia Agentリモートインストールパッケージ
OB2-NDMPP	NDMP Media Agentコンポーネント
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ッケージ

さらに、Cell Manager上 ではなく、独 立した環 境 でインストールサーバーをセットアップし、ユーザーインターフェイスを使 用する場 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ーフェイスが含 まれます。

4. これらのコンポーネントのインストールが完 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 コンポーネントで必 要 となるリモートインストールパッケージ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 ソフトウェアのインストールで必 要 になります。
OB2-TS-PEGP	PEGASUSテクノロジスタックコンポーネント
OB2-OR8P	Oracle用 統 合 ソフトウェアコンポーネント
OB2-MYSQLP	MySQL用 統 合 ソフトウェアコンポーネント
OB2-POSTGRESQLP	PostgreSQL用 統 合 ソフトウェアコンポーネント
OB2-SAPP	SAP用 統 合 ソフトウェアコンポーネント
OB2-SAPDBP	SAP MaxDB用 統 合 ソフトウェアコンポーネント
OB2-SAPHANAP	SAP HANA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-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-EMCVNXP	EMC VNX用統合ソフトウェアコンポーネント
OB2-EMCVMAXP	EMC VMAX用統合ソフトウェアコンポーネント
OB2-SMISAP	HPE P6000/HPE 3PAR SMI-S Agentコンポーネント
OB2-SSEAP	HPE P9000 XP Agentコンポーネント
OB2-NETAPPP	NetAppストレージプロバイダー
OB2-VEPAP	Virtual Environment Protection Agentコンポーネント
OB2-SODAP	StoreOnceソフトウェア重複排除コンポーネント
OB2-AUTODRP	自動ディザスタリカバリコンポーネント
OB2-VMWAREGRE-AGENTP	VMware Granular Recovery Extensionコンポーネント
OB2-DOCSP	英語版ドキュメント(ガイド、ヘルプ)コンポーネント
OB2-FRAP	フランス語版ドキュメント(ガイド、ヘルプ)コンポーネント
OB2-JPNP	日本語版ドキュメント(ガイド、ヘルプ)コンポーネント
OB2-CHSP	簡体字中国語版ドキュメント(ガイド、ヘルプ)コンポーネント

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、UNIX Cell Managerのインストール Cell Manager、ページ 27を参照してください。

インストールが終了すると、UNIXのソフトウェアデポは、`/opt/omni/databases/vendor`ディレクトリに置かれます。

> **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、Linuxインストールパッケージ(tar)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しなければなりません。

> **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/`
>
> 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。

次に行う手順

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。「UNIXシステム用のインストールサーバーのインストール、ページ 42」を参照してください。

   > **注:**
   > 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ッケージ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ッケージを確認できます。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ッケージをインストールまたは削除したときは必ず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。「ネイティブツールを使用した、HP-UXおよびLinuxシステムへのインストール、ページ 334」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、ページ 54」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、ページ 54を参照してください。

ネイティブツールを使用した、HP-UX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インストールパッケージから実行する必要があります。

Cell Managerも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 については、UNIXおよびMac OS X システムでのローカルインストール、ページ 102またはリモートインストール、ページ 94を参 照してください。

アップグレード手 順

次を使 用してData Protector 10.00にアップグレードするには `swinstall`

1. 既 存 のIDBをエクスポートします。
   a. インストールパッケージから一 時 ディレクトリに`omnimigrate.pl`スクリプトをコピーします。

      ```
      cp -p MountPoint/hpux/DP_DEPOT/DATA-PROTECTOR/OMNI-
      CS/opt/omni/sbin/omnimigrate.pl /tmp
      ```

   b. 次 の`omnimigrate.pl`コマンドを使 用してIDBをエクスポートします。

      ```
      /opt/omni/bin/perl /tmp/omnimigrate.pl -shared_dir
      /var/opt/omni/server/exported-export
      ```

2. `root`でログインし、`omnisv -stop`コマンドを実 行してData Protectorサービスを停 止します。

   `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。

3. 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 には、swinstallを使 用したHP-UXシステムでのCell Managerのインストール、ページ 334またはswinstallを使 用したHP-UXシステムでのインストールサーバーのインストール、ページ 336で説 明されている手 順 に従います。

   インストール手 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 :**
   > 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*。

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 については、UNIXおよびMac OS X システムでのローカルインストール、ページ 102またはリモートインストール、ページ 94を参 照してください。

アップグレード手 順

次を使 用してData Protector 10.00にアップグレードするには rpm

1. a. インストールパッケージから一 時 ディレクトリにomnimigrate.plスクリプトをコピーします。

   ```
   cp -p MountPoint/hpux/DP_DEPOT/DATA-PROTECTOR/OMNI-
   CS/opt/omni/sbin/omnimigrate.pl /tmp
   ```

   b. 次 のomnimigrate.plコマンドを使 用してIDBをエクスポートします。

   ```
   /opt/omni/bin/perl /tmp/omnimigrate.pl -shared_dir
   /var/opt/omni/server/exported-export
   ```

2. rootでログインし、omnisv -stopコマンドを実 行してData Protectorサービスを停 止します。

   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。

3. 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。

4. 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

5. Cell Managerをアップグレードする場 合 、rpmを使 用してCell Managerをインストールします。詳 細 な手 順 は、rpmを使 用したLinuxシステムでのCell Managerのインストール、ページ 335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 、Linuxインストールパッケージを使 用します。詳 細 な手 順 は、rpmを使 用したLinuxシステムでのインストールサーバーのインストール、ページ 337を参 照してください。

付録B: システムの準備と保守作業

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、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ーフェイ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。また、これ以外の状況でも発生する可能性があります。

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(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)は、`/opt/omni/sbin` (HP-UX、Solaris、Linuxシステム)または`/usr/omni/bin` (その他UNIXシステム)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`をネットワークサービスとして登録解除するには、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` コマンドや`ipconfig/ifconfig`コマンドを使用してTCP/IP構成を確認できます。

一部のシステムでは、`ping`コマンドをIPv6のアドレスに対して使用することができないので、代わりに`ping6`コマンドを使用してください。

TCP/IPの設定を確認するには

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: ***Windows systems:*** `ipconfig /all`

UNIX システムの場合: `ifconfig`*interface*または`ifconfig -a`または`nestat -i`(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ー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*と入力すると、ソフトウェアのインストールおよび構成状況が表示されます。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。host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。
   - クライアントでは、Cell Managerと、Media Agentがインストールされている各クライアントに対してpingコマンドを実行します。

   > **注:**
   > 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:**
   > 上記の名前解決が動作していない場合は、Data Protectorを正しくインストールすることはできません。
   >
   > また、Windowsコンピューターの名前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がインストールされ、Data Protectorセルが作成された後で、DNSチェックツールを使って、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でセル内の他のクライアントに対するDNS接続を解決できるかどうか、およびその逆をチェックします。これを行うには、`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、『*HPE Data Protector Command Line Interface Reference*』を参照してください。

デフォルトのData Protectorポートの変更

デフォルトのData Protector Inetポートの変更

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、Data Protector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、Inetはポート番号5555/5565を使用します。この特定のポートを別のプログラムが使用していないことを確認するには、UNIXシステムの場合はローカルの/etc/servicesファイル、Windowsシステムの場合はローカルに実行されるnetstat -aコマンドの出力を調べてください。ポートが別のプログラムによって使用されている場合、未使用ポートを使用するようにInetの構成を変更する必要があります。セル内のすべてのシステムが同じポートを使用するように、セルの各システムでこの再構成を実行する必要があります。

インストールサーバーとしても機能するCell Managerまたはスタンドアロンのインストールサーバーでの変更が完了すると、このインストールサーバーを使用してリモートインストールされるすべてのクライアントが、新しいポートを自動的に使用します。したがって、セルの作成時に、Inetポートの変更作業が非常に簡単になります。

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

UNIXシステム

Cell Manager、インストールサーバー、またはData Protectorクライアントとして使用する予定のUNIXシステムでInetポートを変更するには、次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、インストールサーバー、またはData Protectorクライアントとしてすでに使用しているUNIXシステムでInetポートを変更するには、次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 5565/tcp # DATA-PROTECTOR
   ```

   番号5565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に存在している場合は、目的のポート番号でファイルの内容を更新します。
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コマンドを実行します。
4. Cell ManagerのInetの設定を変更するには、Portグローバルオプションに新しい値を設定します。
5. Cell ManagerのInetの設定を変更するには、Data Protectorサービスを再開します。

```
- omnisv stop
- omnisv start
```

Windowsシステム

Cell Manager、インストールサーバー、またはData Protectorクライアントとして使用する予定のWindowsシステムでInetポートを変更するには、次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ーを開きます。
2. HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\ OpenView\OmniBackII\Commonキーの下に、レジストリエントリInetPortを次のように作成します。

   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 (string)

   レジストリエントリの値: *PortNumber*

Cell Manager、インストールサーバー、またはData Protectorクライアントとしてすでに使用しているWindowsシステムでInetポートを変更するには、次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ーを開きます。
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フォルダーのParametersサブフォルダーについても同様の手順を繰り返します。
4. Windowsのコントロールパネルで、**[管理ツール]**、**[サービス]**の順に開き、**Data Protector Inet**サービスを選択して、ツールバーの**[再起動]**アイコンをクリックしてサービスを再度開始します。

UNIXシステムでデフォルトのData Protector IDBポートおよびユーザーアカウントを変更する

UNIXシステムの場合、インストールはomnisetup.shスクリプトで実行され、対話形式ではありません。インストールを開始する前に、/tmp/omni_tmp/DP.datファイルのポート値を変更する必要があります。

次のポートエントリは次のIDBサービスに対応しています。

- HPE Data Protector IDB (hpdp-idb)サービスポート: PGPORT
- HPE Data Protector IDB接続プーラー (hpdp-idb-cp)ポート: PGCPORT
- HPE Data Protectorアプリケーションサーバー(hpdp-as)サービスポート: APPSSPORT
- HPE Data Protectorアプリケーションサーバー(hpdp-as)管理ポート: APPSNATIVEMGTPORT

PGOSUSER変数を設定することで、IDBを実行するデフォルトのユーザーアカウントを変更できます。

DP.datファイルの例:

```
PGPORT=7112
PGCPPORT=7113
PGOSUSER=hpdp
```

```
APPSSPORT=7116
APPSNATIVEMGTPORT=7119
```

Data ProtectorインストールのためのWindows Server 2008またはWindows Server 2012上で実行するMicrosoftサーバークラスターの準備

Windows Server 2008上またはWindows Server 2012オペレーティングシステムで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。Data Protectorセルの役割とWindowsオペレーティングシステムリリースのクラスター対応のどの組み合わせがサポートされているかについては、最新のサポート一覧 (https://softwaresupport.hpe.com/)を参照してください。

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。

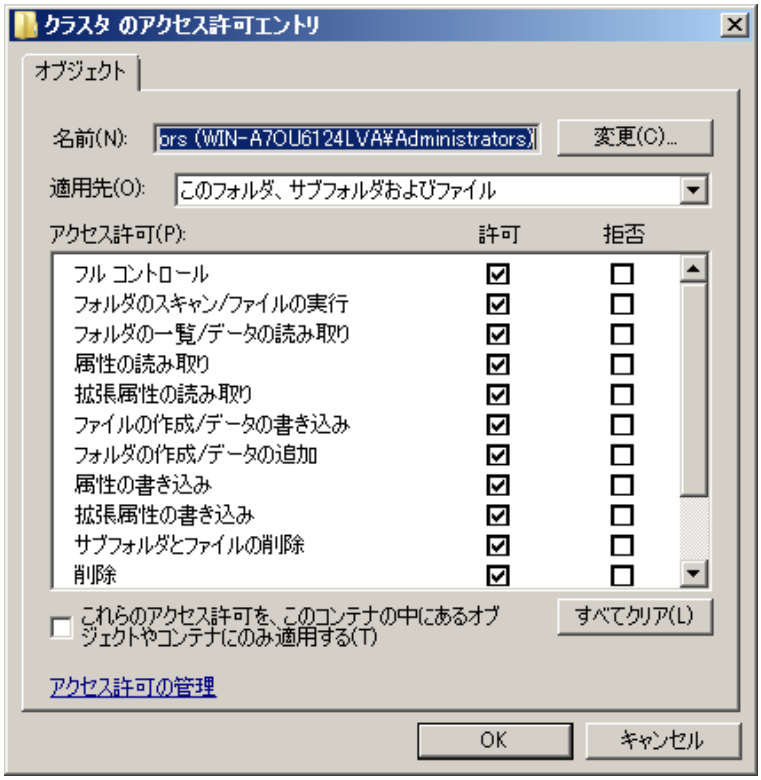
準備の手順

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、File and Printer Sharingプログラム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エクスプローラーを起動して、*WitnessDiskLetter*:\Clusterフォルダー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**[サブコンテナー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エクスプローラーで*WitnessDiskLetter*:\Clusterフォルダー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、ClusterフォルダーおよびAdministratorsローカルユーザーグループの適切なアクセス許可、次のページで示す設定と一致することを確認してください。

ClusterフォルダーおよびAdministratorsローカルユーザーグループの適切なアクセス許可



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`Cluster Access Point`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ーを追加します。**[共有フォルダーの追加]**をクリックして共有フォルダーの準備ウィザードを開始します。
   a. [共有フォルダーの場所]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、ページ 178を参照してください。

インストールが完了したら、Data Protector Inetサービスを有効にして、Microsoftのリソースドライバーではなく専用のリソースドライバー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でomnisv -maintenanceコマンドを実行して、保守モードを開始します。
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オプション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ファイルオプション数の使用に関する詳細については、『*HPE Data Protectorトラブルシューティングガイド*』を参照してください。
3. omnisv -maintenance –stopコマンドを実行して、保守モードを終了します。

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

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 5565/tcp # Data Protector for Data Protector inet server

   ポート5565を使用できない場合は、5565を別の値に置き換えてください。デフォルトのData Protector Inetポートの変更、ページ 345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:**
> 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 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。詳細については、man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クライアント上でNISkill -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。手順については、セルからのクライアントのエクスポート、ページ 194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。

> **注:**
> 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システムの場合

UNIX用Cell Managerでは、以下の操作を行ってください。

1. コンピューターまたはドメイン名を変更します。

   > **注:**
   > どのメンバーでも、両方向で、新しいホスト名がDNSによって解決されることを確認します。名前の解決が機能しない場合は、この手順を続行しないでください。

2. 次のコマンドを実行します。

```
omnisv stop
```

> **注:**
> 古いホスト名のインスタンスが、次のファイル内に存在しないことを確認します。
>
> ```
> /etc/opt/omni/client/components
> ```

以下のコマンドを実行することができます。

```
"grep -rn /etc/opt/omni/client/components -e "<OLD_HOSTNAME_FQDN>""
```

3. 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/config
   ```

   ```
   /etc/opt/omni/server/cell/installation_servers
   ```

   ```
   /etc/opt/omni/server/users/UserList
   ```

4. 次のコマンドを実行して証明書を再生成します。

   ```
   # perl -CA /opt/omni/sbin/omnigencert.pl -server_id <NEW_HOSTNAME_FQDN> -
   server_san dns:<short_hostname>,dns:< NEW_HOSTNAME_FQDN > -user_id hpdp -store_
   password <STORE_PASSWORD>
   ```

   > **注:**
   > キーストアパスワードは、以下のコマンドを実行するとわかります。
   >
   > ```
   > # grep keystorePassword
   > ```
   >
   > ```
   > /etc/opt/omni/client/components/webservice.properties
   > ```

5. 次のコマンドを実行します。

   ```
   omnisv start
   ```

6. 以下のコマンドを実行してCell Managerの名を変更します。

   ```
   omnidbutil -change_cell_name
   ```

7. Data Protector GUIを使用してCell Managerに接続し、新しい証明書を承認します。
8. Cell Managerにテープデバイスが接続されている場合は、**[デバイス/メディア]**に移動し、テープデバイスのプロパティでホスト名を変更します。
9. 構成されたファイルデバイスの場合:
   a. 構成されたデバイスを表示するには、次を使用します。

      ```
      "omnidownload -list_libraries [-detail]" and "omnidownload -dev_info"
      ```

   b. ライブラリでホスト名を変更するには、`# omnidownload -library <LIBRARY_NAME> >/tmp/file_lib.txt`に移動し、`file_lib.txt`ファイルを次のように編集します。

      ```
      # omniupload -modify_library <LIBRARY_NAME> -file /tmp/file_lib.txt
      ```

   c. デバイスでホスト名を変更するには、`# omnidownload -device <DRIVE_NAME> >/tmp/writer_0.txt`に移動し、`writer_0.txt`ファイルを次のように編集します。

      ```
      # omniupload -modify_device <DRIVE_NAME> -file /tmp/writer_0.txt
      ```

10. Data Protector IDBのバックアップ仕様を削除し、新しいバックアップ仕様を再作成します。
11. ホスト名の変更によって影響を受ける、その他のバックアップ仕様を変更します。

12. 以下のファイルで変更されたCellサーバーのホスト名でUNIXまたはLINUXクライアントを更新します。

    /etc/opt/omni/client/cell_server

13. 以下のレジストリで変更されたCellサーバーのホスト名でWindowsクライアントを更新します。

    HKEY_LOCAL_MACHINE -> SOFTWARE -> Hewlett Packard -> OpenView -> OmniBack II -> Site -> CellServer

14. 次の構成ファイルで古いホスト名の有無をチェックします。

    # grep -rn /etc/opt/omni -e "<OLD_HOSTNAME_FQDN>"

    > **注:**
    > 古いホスト名を次の位置で表示すれば問題ありません。
    >
    > /etc/opt/omni/server/dr/p1s -> If the system recovery data has been stored in the past.
    >
    > /etc/opt/omni/server/certificates -> old certificate
    >
    > /etc/opt/omni/client/certificates -> old certificate

15. IDBの内容をチェックし、それを次のファイルにエクスポートします。

    /opt/omni/sbin/omnidbutil -writedb /tmp

    <ENTER>

    > **注:**
    > dpidb.datファイルには、内部データベースの主要パートが含まれています。古いホスト名がそのまま残っている可能性があるテーブルは、次のとおりです。
    >
    > dp_frontend_application
    >
    > dp_catalog_object
    >
    > dp_catalog_object_datastream (in case the old device name(s) contain the old hostname)
    >
    > dp_management_session
    >
    > dp_medmng_library (in case the current device name(s) contain the old hostname)
    >
    > dp_medmng_media_pool (in case the old pool name(s) contain the old hostname)
    >
    > dp_medmng_cartridge (in case the old pool name(s) contain the old hostname)

    また、dpjce.datファイルには、ジョブコントロールエンジン(JCE)データベースが含まれます。ここには、スケジューラーに不可欠な、いくつかのURLエントリがあります。このファイル内に古いホスト名が存在してはなりません。

    jce_service_descriptionテーブルで古いホスト名を検索する場合、以下の手順に従ってください。

    a. hpjceデータベースにログインします。

       > **注:**
       > データベースの資格情報は、次の場所にあります。
       >
       > /etc/opt/omni/server/idb/idb.config ファイル

```
# grep PGSUPERPASSWORD /etc/opt/omni/server/idb/idb.config
PGSUPERPASSWORD='a2ZudGV4cjBpdTZnMg==';
# export PGPASSWORD=`echo 'a2ZudGV4cjBpdTZnMg==' | base64 -d`
# echo $PGPASSWORD
kfntexr0iu6g2
```

b. 接続を作成します。以下の手順を実行します。
   i. コマンドプロンプトで、bin位置(/opt/omni/idb/bin/)に移動します。
   ii. 次のコマンドを実行し、hpdpユーザーを使用してhpjceデータベースにログインします。

```
# /opt/omni/idb/bin/psql -h localhost -p 7112 -U hpdp hpdpidb
psql (9.1.9)
Type "help" for help.
```

   iii. 現在の内容をチェックするため、hpjceデータベースで次のコマンドを実行します。

```
hpjce=# select url from jce_service_description;
```

> **注:**
> ホスト名の変更が必要な場合、次のコマンドを実行します。
>
> ```
> hpjce=# update jce_service_description
> hpjce-# set url=replace(url, 'old_hostname', 'new_hostname');
> hpjce=# \q
> ```

Windowsシステムの場合

Windows用Cell Managerで、以下の操作を行ってください。

1. コンピューターまたはドメイン名を変更します。

> **注:**
> どのメンバーでも、両方向で、新しいホスト名がDNSによって解決されることを確認します。
> 名前の解決が機能しない場合は、この手順を続行しないでください。

2. 次のコマンドを実行します。

```
omnisv stop
```

3. 以下のレジストリキーで、Cell Manager名を変更します。

```
HKEY_LOCAL_
MACHINE\SOFTWARE\HewlettPackard\OpenView\OmniBackII\Site\CellServer\newnameHKE
Y_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\Packages\newname
```

4. 次のファイルに移動して、古いホスト名のインスタンスがまだ存在ないことを確認します。

```
Data_Protector_program_data\Config\client\components
```

> **注:**
> Windowsの`find in file`機能を使用します。

5. 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_program_data\Config\Server\users\UserList
```

Data_Protector_program_data\Config\Server\config

Data_Protector_program_data\Config\Server\cell\cell_info

Data_Protector_program_data\Config\Server\cell\installation_servers

6. C:\Program Files\OmniBack\binフォルダーから次のコマンドを実行して証明書を再生成します。

   perl omnigencert.pl -server_id <NEW_HOSTNAME> -server_san

   dns:<hostname>,dns:<FQDN> -user_id hpdp -store_password <PASSWORD>

   > **注:**
   > キーストアパスワードは、次の場所でわかります。
   >
   > *Data_Protector_program_data*\Config\client\components\webservice.properties

7. 次のコマンドを実行します。

   omnisv start

8. 以下のコマンドを実行してIDBのCell Manager名を変更します。

   omnidbutil -change_cell_name

9. Data Protector GUIを使用してCell Managerに接続し、新しい証明書を承認します。
10. Cell Managerにテープデバイスが接続されている場合は、**[デバイス/メディア]**に移動し、テープデバイスのプロパティでホスト名を変更します。
11. 構成されたファイルデバイスの場合:
    a. 構成されたデバイスを表示するには、次を使用します。

       "omnidownload -list_libraries [-detail]" and "omnidownload -dev_info"

    b. ライブラリでホスト名を変更するには、"omnidownload -library <LIBRARY_NAME> > c:\temp\file_lib.txt"に移動し、file_lib.txtファイルを次のように編集します。

       omniupload -modify_library <LIBRARY_NAME> -file c:\temp\file_lib.txt

    c. デバイスでホスト名を変更するには、"omnidownload -device <Device Name> > c:\temp\device.txt"に移動し、device.txtファイルを次のように編集します。

       omniupload -modify_device <Device Name> -file c:\temp\device.txt

12. Data Protector IDBのバックアップ仕様を削除し、新しいバックアップ仕様を再作成します。
13. ホスト名の変更によって影響を受ける、その他のバックアップ仕様を変更します。
14. 以下のファイルで変更されたCellサーバーのホスト名でUNIXまたはLINUXクライアントを更新します。

    /etc/opt/omni/client/cell_server

15. 以下のレジストリで変更されたCellサーバーのホスト名でWindowsクライアントを更新します。

    HKEY_LOCAL_MACHINE -> SOFTWARE -> Hewlett Packard -> OpenView -> OmniBack II -> Site -> CellServer

16. Windowsの"find in file"機能を使用して次の構成ファイルをチェックし、古いホスト名を検索します。

    Data_Protector_program_data\Config

> **注:**
> 古いホスト名を次の位置で表示すれば問題ありません。
>
> *Data_Protector_program_data*\Config\Server\dr -> 過去にシステムリカバリが保存済みの場合
>
> *Data_Protector_program_data*\Config\Server\certificates -> 古い証明書
>
> *Data_Protector_program_data*\Config\client\certificates -> 古い証明書

17. IDBの内容をチェックし、それを次のファイルにエクスポートします。

    ```
    omnidbutil -writedb e:\idb_export
    <ENTER>
    ```

    > **注:**
    > dpidb.datファイルには、内部データベースの主要パートが含まれています。古いホスト名がそのまま残っている可能性があるテーブルは、次のとおりです。
    >
    > dp_frontend_application
    >
    > dp_catalog_object
    >
    > dp_catalog_object_datastream (in case the old device name(s) contain the old hostname)
    >
    > dp_management_session
    >
    > dp_medmng_library (in case the current device name(s) contain the old hostname)
    >
    > dp_medmng_media_pool (in case the old pool name(s) contain the old hostname)
    >
    > dp_medmng_cartridge (in case the old pool name(s) contain the old hostname)

    また、dpjce.datファイルには、ジョブコントロールエンジン(JCE)データベースが含まれます。ここには、スケジューラーに不可欠な、いくつかのURLエントリがあります。このファイル内に古いホスト名が存在してはなりません。

    jce_service_descriptionテーブルで古いホスト名を検索する場合、以下の手順に従ってください。

    a. hpjceデータベースにログインします。

       > **注:**
       > データベースの資格情報は、*Data_Protector_program_data*\Config\Server\idb\idb.configファイル内にあります。次のリンクを使って、PGSUPERPASSWORDをデコードできます。
       >
       > https://www.base64decode.org

    b. 接続を作成します。以下の手順を実行します。

       i. コマンドプロンプトで、bin位置(C:\Program Files\OmniBack\idb\bin)に移動します。

       ii. 次のコマンドを実行し、hpdpユーザーを使用してhpjceデータベースにログインします。

           ```
           .\psql -h localhost -p 7112 -d hpjce -U hpdp <Enter the decoded password>
           ```

       iii. 現在の内容をチェックするため、hpjceデータベースで次のコマンドを実行します。

```
hpjce=# select url from jce_service_description;
```

> **注:**
> ホスト名の変更が必要な場合、次のコマンドを実行します。
>
> ```
> hpjce=# update jce_service_description
> hpjce-# set url=replace(url, 'old_hostname', 'new_hostname');
> hpjce=# \q
> ```

ジョブコントロールエンジン(JCE)データベースのホスト名の変更

UNIXシステムの場合

JCEデータベースのホスト名をPGADMIN3で変更するには、次の手順を実行します。

1. `/var/opt/omni/server/db80/pg/pg_hba.conf`ファイルに移動します。
2. `host all all 127..0.0.1/32 md5`を`host all all 10.17.0.0/16 md5`に変更します。
   (または)
   `host all all 127..0.0.1/32 md5`を特定のホスト(`host all all 10.17.16.121/32 md5`)のみに接続するように変更します。
3. `pg config`ファイルを再読み込みし、以下のコマンドを実行します。
   ```
   su hpdp
   /opt/omni/idb/bin/pg_ctl reload -D /var/opt/omni/server/db80/pg
   ```
4. pgAdmin3に接続します。

Windowsシステムの場合

PGADMIN3でコマンドラインを使用してJCEデータベースのホスト名を変更するには、次の手順を実行します。

1. 次のコマンドを実行します。
   ```
   omnidbutil –set_passwd hpdp
   ```
2. パスワードを設定します。
3. `C:\Program Files\OmniBack\idb\bin`フォルダーに移動し、**pgadmin3.exe**を実行します。
   pgAdmin3プログラムが起動します。
4.  プラグインをクリックして、サーバーを追加します。
   [新しいサーバ登録]ウィンドウが表示されます。
5. [新しいサーバ登録]ウィンドウで、以下の手順を実行します。

a. [名前]フィールドに、localまたは要件に合わせた名前を入力します。

たとえば、jce_service_descriptionのように入力します。

b. [ホスト]フィールドに、localhostと入力します。

c. [Port]フィールドに、7112と入力します。

d. [サービス]フィールドは、空のままにします。

e. [DBメンテナンス]フィールドで、hpdpidbを選択します。

f. [ユーザ名]フィールドに、hpdpと入力します。

g. [パスワード]フィールドに、手順1でomnidbutil –set_passwd hpdpコマンドを使って設定したパスワードを入力します。

6. **[OK]**をクリックします。

7. [オブジェクトブラウザ]領域で、追加したサーバーを展開します([データベース] > [hpjce] > [スキーマ] > [hpjce_app] > [テーブル] と展開します)。

たとえば、jce_service_descriptionテーブル名が表示されます。jce_service_descriptionをクリックします。

8. ツールバーの[SQL]ボタンを選択します。

次のコマンドでSQLエディターが表示されます。

```
UPDATE jce_service_description
SET url=replace (url, ‘old_hostname’, ‘new_hostname’);
```

たとえば、old_hostnameとしてtestHostname.1、new_hostnameとしてtestHostnameを使用できます。次に、[再生]ボタンを使用してこのコマンドを実行します。

[データ出力]タブに、変更された行数を示すメッセージが表示されます。

CLIの使用

PGADMIN3を使用せずにJCEデータベースのホスト名を変更するには、次の手順を実行します。

1. 次のコマンドを実行します。

Windowsシステムの場合:

```
C:\Program Files\OmniBack\idb\psql --port=7112 -U hpdp -d hpjce -h localhost
```

UNIXシステムの場合:

```
/opt/omni/idb/bin/psql --port=7112 -U hpdp -d hpjce -h localhost
```

2. 取得する情報に応じて、以下のコマンドを実行します。

```
hpjce=# select url from jce_service_description;
hpjce=# update jce_service_description
hpjce-# set url=replace(url, 'old_hostname', 'new_hostname');
hpjce=# \q
```

Windows Cell Managerでの大型バックアップセッションの実行

Windows Cell Manager上で実行するバックアップセッション数が多い場合は、Windowsレジストリでデスクトップヒープの制限を調整してください。デスクトップヒープは、次のレジストリキーで制御されます。

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session
Manager\SubSystems\Windows
```

このレジストリキーのデフォルト値は、次のとおりです。

```
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1
ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4
ProfileControl=Off MaxRequestThreads=16
```

Data Protectorは、`SharedSection`パラメーターの影響を受けます。その値は、次のとおりです。

- `1024`: すべてのデスクトップに共通する共有ヒープサイズ。この値を変更して、デスクトップヒープの枯渇に関連する問題を解決しないでください。
- `20480`: 対話型のウィンドウステーションに関連する各デスクトップのデスクトップヒープのサイズ。
- `768`: 非対話型のウィンドウステーションに関連する各デスクトップのデスクトップヒープのサイズ。

`SharedSection`パラメーターの3番目の値(`768`)を`20480`に設定してください。修正済みのWindowsレジストリキーの値は、次のようになります。

```
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,20480,20480 Windows=On SubSystemType=Windows ServerDll=basesrv,1
ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4
ProfileControl=Off MaxRequestThreads=16
```

> **注:**
> これはキロバイト単位なので、非常に大きい値は設定しないでください。

新しい値を設定したら、システムを再起動する必要があります。

付録C: デバイスとメディア関連タスク

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、デバイスドライバー構成、SCSIロボティクスの管理、SCSI環境類の保持が含まれます。

Windowsシステムでのテープドライバーおよびロボティクスドライバーの使用

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ー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ーは、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HPE 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。HPE 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、メディアチェンジャーデバイス用にロードされるネイティブドライバー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。

テープドライバー

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、ドライバー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

コンピューターが起動すると、デバイスドライバー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。ネイティブのテープドライバーは、別途ロードする必要はなく、更新が可能です。

ネイティブのテープドライバーを更新または置換するには

1. Windowsのコントロールパネルで、**[管理ツール]**をダブルクリックします。
2. **[管理ツール]**ウィンドウで**[コンピューターの管理]**をダブルクリックします。**[デバイスマネージャー]**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ーを確認するには、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. **[ドライバー]**タブを選択し、**[ドライバーの更新]**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ーを更新するか、別のドライバーに置き換えるかを、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:**
> ドライバーがネイティブテープドライバーを使用しないで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、次のような変更が必要になります。`scsi1:0:4:0 > tape3:0:4:0)`.
>
> 詳細は、Windowsシステム上でのデバイスファイル(SCSIアドレス)の作成、ページ 361を参照してください。

ロボティクスドライバー

Windowsでは、テープライブラリを有効にすると、対応するロボティクスドライバーが自動的にロードされます。Data Protectorでライブラリロボティクスを使用するには、対応するドライバーを無効化する必要があります。

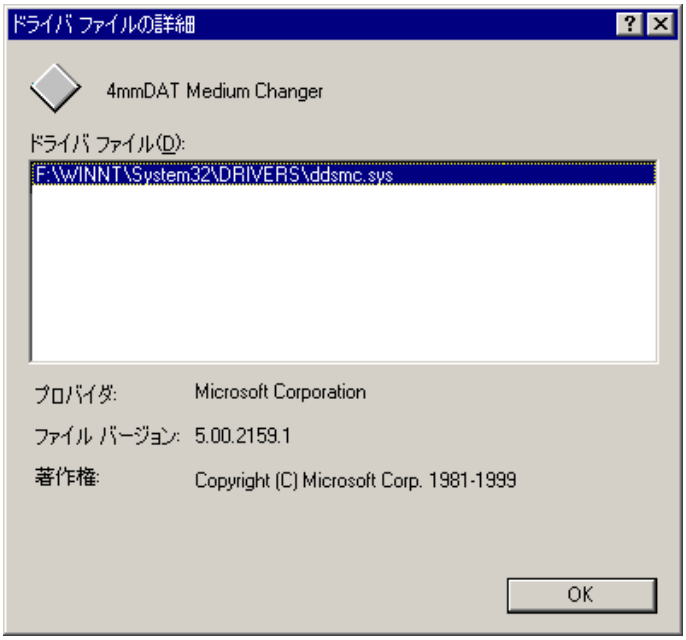
ここでは、4mm DDSテープを使用するHPE 1557Aテープライブラリを例に取り上げます。

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ー(ddsmc.sys)を無効にするには

1. Windowsのコントロールパネルで、**[管理ツール]**をダブルクリックします。
2. [管理ツール]ウィンドウで**[コンピューターの管理]**をダブルクリックします。**[デバイスマネージャー]**をクリックします。
3. [デバイスマネージャー]ウィンドウの結果エリアで、[メディアチェンジャー]を展開します。
4. 現在ロードされているドライバーを確認するには、**[4mm DDS Medium Changer]**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。

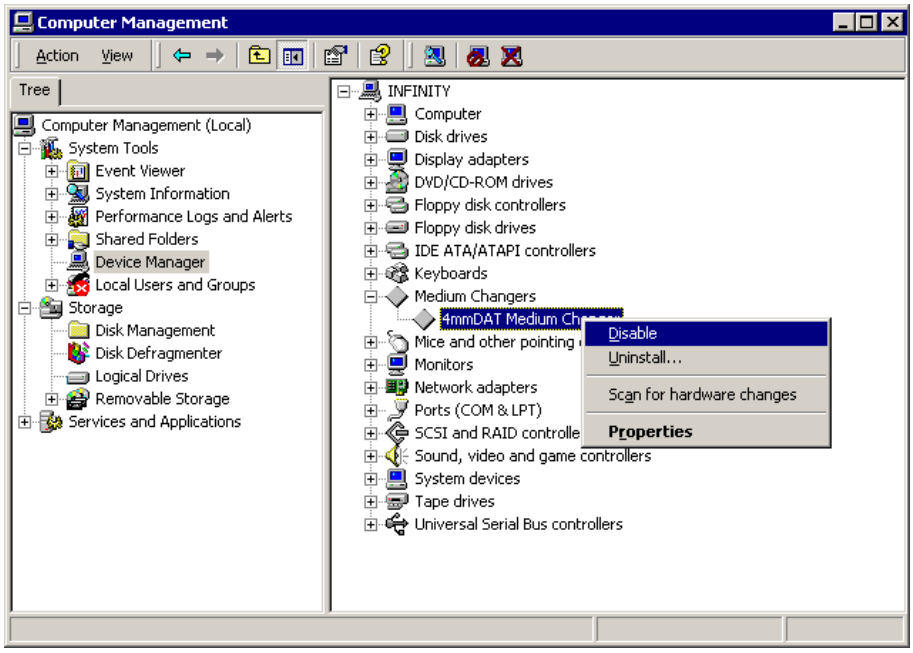
   [ドライバー]タブを選択し、**[ドライバーの詳細]**をクリックします。以下のウィンドウが表示されます。

   メディアチェンジャーのプロパティ



   ネイティブロボティクスドライバーを無効にするには、**[4mm DDS Medium Changer]**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。

   ロボティクスドライバーの無効化



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システム上でのデバイスファイル(SCSIアドレス)の作成

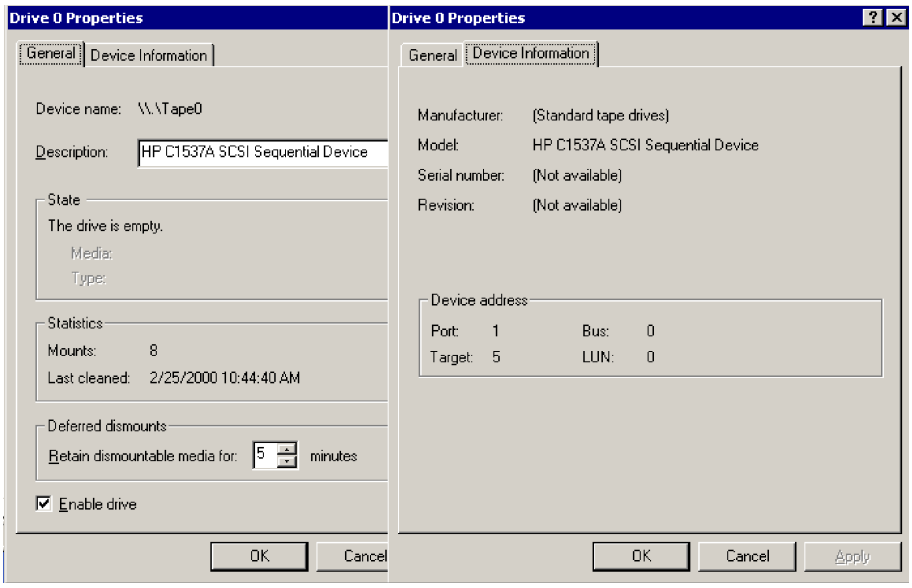
テープデバイスファイル名の構文は、ネイティブテープドライバーをテープドライブに対してロード(`tapeN:B:T:L`)またはアンロード(`scsiP:B:T:L`)するかによって異なります。

Windowsでネイティブテープドライバーを使用している場合

Windowsシステムに接続され、ネイティブテープドライバー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**[コンピューターの管理]**をダブルクリックします。[リムーバブル記憶域]と[物理的な場所]を順に展開します。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ーがロードされていれば、[一般]プロパティページにデバイスファイル名が表示されます。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。テープドライブプロパティ、下を参照してください。

テープドライブプロパティ



テープドライブプロパティ、前の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ーを使用している場合	`Tape0 or Tape0:0:5:0`
ネイティブテープドライバーを使用していない場合	`scsii1:0:5:0`

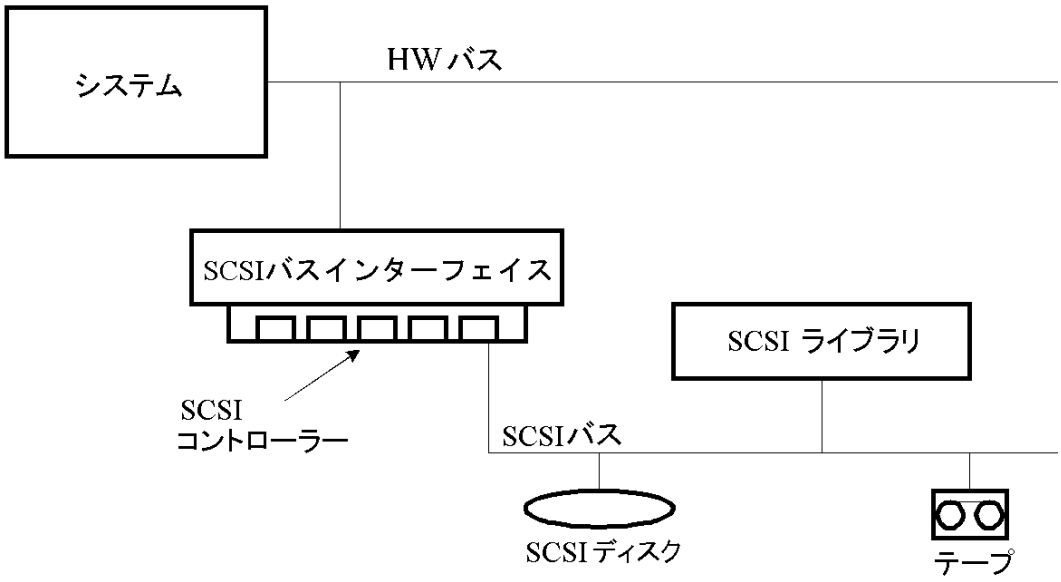
光磁気デバイス

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。

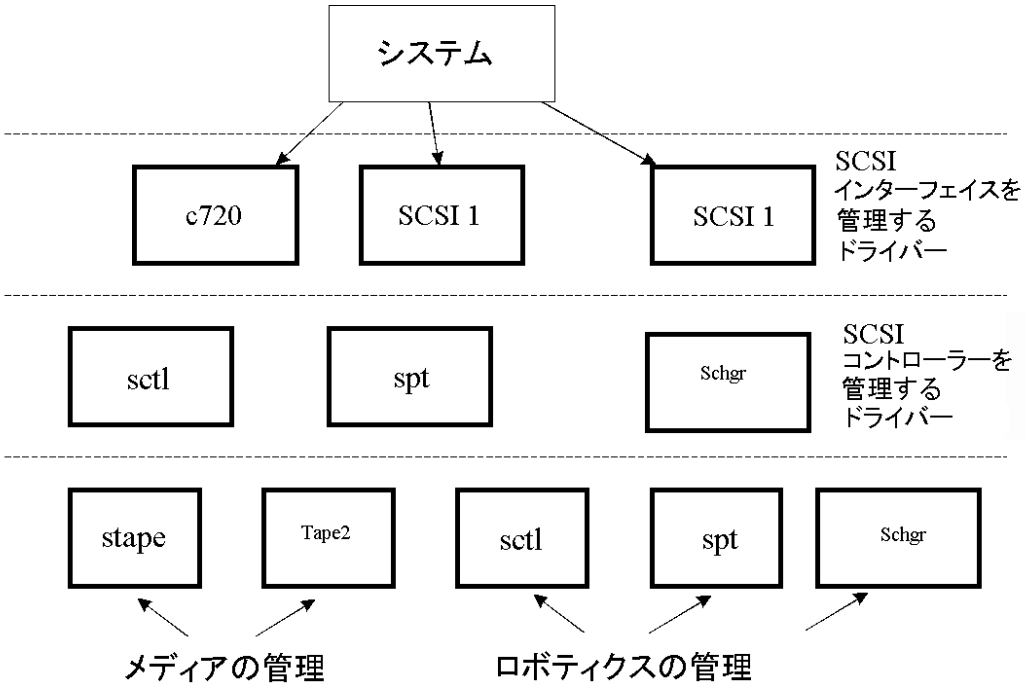
HP-UXシステム上のSCSIロボティクス構成

HP-UXシステムでは、SCSIパススルードライバーを使ってテープライブラリデバイス(HPE 12000eなど)のSCSIコントローラーおよび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。

SCSI制御デバイス



デバイスの管理



使用されるSCSIロボティクスドライバーの種類は、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オートチェンジャードライバー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ー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HPE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ーを使用します。このドライバーは、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ーが現在の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ーを*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、*HPE 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。HP-UXクライアントのインストール、ページ 71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ー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`コマンドを使用します。

SCSIパススルードライバー(sctl)のステータス

```
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
```

SCSIパススルードライバー(sctl)のステータス、上では、SCSIパススルードライバー`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ーは`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コントローラー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、コントローラーは`sctl`によって管理されています。

SCSIパススルードライバーsptのステータス

```
# 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
#
```

SCSIパススルードライバーsptのステータス、前の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ーsptによって制御されています。このデバイスは、HPE 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ーsptが正しく割り当てられています。

sctl、spt、またはschgrのドライバー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ー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ーを*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ーが、現在の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、以下のコマンドを実行してください。

   ```
   grep SCSIRoboticDriver system
   ```

   ここで、*SCSIRoboticDriver*にはspt、sctl、またはschgrを指定します。ドライバーが現在の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. エディターを使って、

   ```
   driver H/W Path spt
   ```

   /stand/build/systemファイルにドライバーステートメントを追加します。*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。

   HPE 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ー行を追加する必要があります。

schgrドライバーを構成する場合は、ドライバー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システム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HPE 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。

SCSIパススルードライバーsptのステータス、ページ 364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。

接続済みデバイスのリスト

```
# 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
# 
```

この例のSCSIバスインターフェイスは、scsi1システムドライバーによって制御されています。これは、SCSI NIOインターフェイスです。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ーsptを使用する必要があります。このドライバーはすでにインストールされており、HPE 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:**
> SCSI NIOベースのバスインターフェイスを使用しない場合は、sptドライバーではなく、sctlドライバーが必要になります。

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ー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、どちらのドライバーの場合も共通です)。

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
```

接続済みデバイスのリスト、前のページの例の場合、このコマンドを実行すると、メジャー番号が返されます。75.

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、メジャー番号が返されます。203.

どちらのSCSIパススルードライバーの場合も、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バスインターフェイ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
```

sctl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コントローラーのパラメーターの設定

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コントローラー上で追加の構成が必要になる場合があります。

WindowsシステムでAdaptec SCSIコントローラーやAdaptecチップセット搭載のSCSIコントローラーのパラメーターを設定するには、そのコントローラーのレジストリ値を編集します。

1. 以下のレジストリ値の設定: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:**
> 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システム上の未使用の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システムでは、/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。

HP-UXシステム上で実行したioscan -fコマンドの出力、下は、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。

HP-UXシステム上で実行したioscan -fコマンドの出力

```
# 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
# 
```

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。

HP-UXシステム上で実行したioscan -fコマンドの出力、上に示す例では、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コントローラーに使用されています。

> **注:**
> 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コントローラー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ドライバー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ーspt によって制御されています。説明を見ると、デバイスがHPE 12000eライブラリであることを確認できます。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ライブラリで簡単に識別できます。

SCSIバス全体は、scsi1インターフェイ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

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に指示さ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ー構成の更新

構成ファイルの更新

デバイスおよびドライバーの構成には、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st (SCSIテープ)ドライバーで使用されます。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*";

     ここで、

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番目のパラメーターである`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:**
> 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;
```

ここで、

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`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HPE 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る必要があるファイルです。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、HPE 24x6などの一部の例外もあります。

1. sstドライバー(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、以下のエントリを追加します。

   ```
   name="sst" class="scsi" target=X lun=Y;
   ```

   ここで、

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. ドライバーを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ー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。

   ```
   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. 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

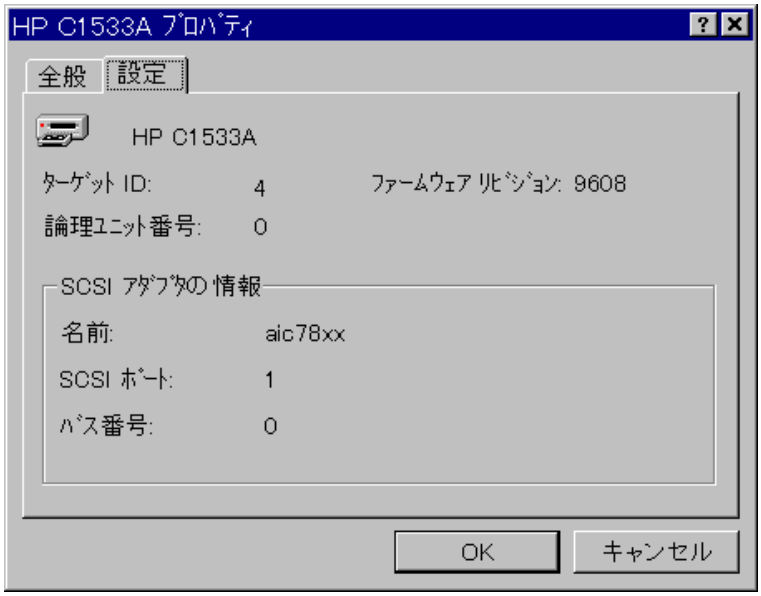
Windowsシステム上の未使用のSCSIターゲットIDの取得

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

1. Windowsのコントロールパネルで、**[SCSIアダプター]**をクリックします。
2. SCSIアダプター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。デバイスの設定、下を参照してください。

   デバイスに割り当てられた`SCSI Target IDs`と`LUNs(Logical Unit Numbers)`を把握しておいてください。この方法で、どの`SCSI Target ID`と`LUNs`がすでに使用されているかを調べることができます。

デバイスの設定



HPE 330fxライブラリでの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

HPE 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 IDs *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。リモートインストール、ページ 94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システム上の未使用のSCSIアドレスの取得、ページ 368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、ページ 370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、前の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、必要なドライバーがすでに*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、ページ 73を参照してください。

     SCSIパススルードライバーを構成する必要がある場合は、HP-UXシステム上のSCSIロボティクス構成、ページ 362を参照してください。

   - Solarisシステムに接続する場合は、必要なドライバー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ー構成の更新、ページ 370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ーを構成する場合は、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ーをロードまたは無効化します。Windowsシステムでのテープドライバーおよびロボティクスドライバーの使用、ページ 359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ー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ー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。例: scsi1:0:4:0 > tape3:0:4:0).

適切なデバイスファイル名の詳細については、Windowsシステム上でのデバイスファイル(SCSIアドレス)の作成、ページ 361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、通常はデバイス上のスイッチを使用して設定できます。詳細については、使用するデバイスのドキュメントを参照してください。

   設定例は、HPE 330fxライブラリでのSCSI IDの設定、ページ 374を参照してください。

   サポート対象デバイスの詳細については、https://softwaresupport.hpe.com/を参照してください。

   > **注:**
   > AdaptecSCSIアダプター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アダプターメニューを表示し、**[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、コンピューター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。

   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。デフォルトのData Protectorコマンドディレクトリに移動して、`devbra -dev`コマンドを実行します。

   `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HPE DDSテープデバイス(ネイティブテープドライバー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、HPE DDSテープデバイス(ネイティブテープドライバー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。

HP-UXシステムの場合: `/usr/sbin/ioscan -fn`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、新しく接続されたデバイスに正しい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システムの起動時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システム上のデバイスファイルの作成、ページ 366を参照してください。

Solarisシステムの場合: `ls -all`コマンドを`/dev/rmt`ディレクトリで実行すると、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、新しく接続されたデバイスに正しい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システムの場合: : `ls -all`コマンドを`/dev/rmt`ディレクトリで実行すると、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、新しく接続されたデバイスに正しい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。

AIXシステムの場合: `lsdev -C`コマンドを実行すると、接続済みのデバイスを対応するデバイスファイルとともに示す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。詳細な手順は、『*HPE Data Protector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り、テープドライブがデータを受信する速度が向上します。

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システム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(テープドライバーがロードされている場合はtape2:0:1:0C)。デバイスがハードウェア圧縮をサポートしている場合は、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システム上で無効化するには、デバイスやドライブのSCSIアドレスの末尾にNを追加してください(例: scsi:0:3:0:N)。

ハードウェア圧縮をUNIXシステム上で有効化/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。詳細については、デバイスやオペレーティングシステムのドキュメントを参照してください。

次に行う手順

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。構成タスクの詳細については、『*HPE Data Protectorヘルプ*』のキーワード「構成、バックアップデバイス」で表示される内容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。リモートインストール、ページ 94を参照してください。

この後の項では、HP HPE Standalone 24テープデバイス、HPE 12000eライブラリ、およびHPE DLTライブラリ28/48スロットを、HP-UXシステムとWindowsシステムに接続する場合の手順を説明します。

HPE 24スタンドアロンデバイスの接続

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

HPE 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

1. 必要なドライバー(`stape` または`tape2`)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、ページ 73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システム上の未使用のSCSIアドレスの取得、ページ 368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。

   詳細については、使用するデバイスのドキュメントを参照してください。
4. デバイス、コンピューター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。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。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。

次に行う手順

デバイスを適切に接続した後、「*HPE Data Protectorヘルプ*」のキーワード「構成、バックアップデバイス」で、新たに接続したデバイスに対するData Protector*バックアップデバイス*の構成手順を参照してください。

Windowsシステムに接続する場合

HPE 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

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、ページ 374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。詳細については、使用するデバイスのドキュメントを参照してください。
3. デバイス、コンピューター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。Data Protectorコマ

ンドディレクトリに移動して、devbra -devコマンドを実行します。

devbraコマンドの出力リストに、新しく接続したHPE 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

デバイスを適切に接続した後、「*HPE Data Protectorヘルプ*」のキーワード「構成、バックアップデバイス」で、新たに接続したデバイスに対するData Protectorバックアップデバイスの構成手順を参照してください。

HPE DATオートローダーの接続

HPE 12000eとDAT24x6のライブラリはいずれも、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

HPE 12000eライブラリデバイスをHP-UXシステムに接続するには

1. オートローダーの裏側のモードスイッチを次の値に設定してください: 6.
2. 必要なドライバー(stape またはtape2)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、ページ 73を参照してください。
3. 必要なSCSIパススルードライバー((sctlまたはspt)が*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確認*します。HP-UXシステム上のSCSIロボティクス構成、ページ 362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システム上の未使用のSCSIアドレスの取得、ページ 368を参照してください。

   > **注:**
   > HPE 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番号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。詳細については、使用するデバイスのドキュメントを参照してください。
6. デバイス、コンピューター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システム上のデバイスファイルの作成、ページ 366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。

次に行う手順

ライブラリデバイスを適切に接続した後、「*HPE Data Protectorヘルプ*」のキーワード「構成、バックアップデバイス」で、新たに接続したデバイスに対するData Protectorバックアップデバイスの構成手順を参照してください。

Windowsシステムに接続する場合

HPE 12000eライブラリデバイスをWindowsシステムに接続するには

1. オートローダーの裏側のモードスイッチを次の値に設定してください: `6`.
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、ページ 374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。詳細については、使用するデバイスのドキュメントを参照してください。

   > **注:**
   > HPE 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番号を割り当てるように設計されています。

4. デバイス、コンピューター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。デフォルトのData Protectorコマンドディレクトリに移動して、`devbra -dev`コマンドを実行します。

   `devbra`コマンドの出力リストに、HPE 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。

次に行う手順

ライブラリデバイスを適切に接続した後、「*HPE Data Protectorヘルプ*」のキーワード「構成、バックアップデバイス」で、新たに接続したデバイスに対するData Protectorバックアップデバイスの構成手順を参照してください。

HPE DLTライブラリ28/48スロットの接続

HPE 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。80～600GB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HPE DLTライブラリ28/48スロットを接続するには

1. 必要なドライバー(`stape` または`tape2`) ドライバーがすでに*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、ページ 73を参照してください。
2. 必要なSCSIパススルードライバー(`sctl` または`spt`)が*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*ことを確認します。HP-UXシステム上のSCSIロボティクス構成、ページ 362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システム上の未使用のSCSIアドレスの取得、ページ 368を参照してください。

   > **注:**
   > HPE 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。詳細については、使用するデバイスのドキュメントを参照してください。
5. デバイス、コンピューター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システム上のデバイスファイルの作成、ページ 366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。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
   ```

   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。

次に行う手順

HPE DLT Library 28/48スロットライブラリデバイスを適切に接続した後、「*HPE Data Protectorヘルプ*」のキーワード「構成、*バックアップデバイス*」で、新たに接続したデバイスに対するData Protector*バックアップデバイス*の構成手順を参照してください。

Solarisシステムに接続する場合

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。

Solarisシステム上でHPE C5173-7000ライブラリデバイスを構成するには

1. sstドライバー(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. ドライバーを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。

   ```
   cd /dev/rmt rm *
   ```

4. 次を押して、システムを停止します。**Stop** + **A**.
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. sstドライバー(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。、上でコピーした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:**
> 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。(/kernel/drv/st.confファイルを開いて、以下の行を追加します。、前のページを参照)。

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

HPE DLT Library 28/48スロットライブラリデバイスを適切に接続した後、「*HPE Data Protectorヘルプ*」のキーワード「構成、バックアップデバイス」で、新たに接続したデバイスに対するData Protectorバックアップデバイスの構成手順を参照してください。

Windowsシステムに接続する場合

WindowsシステムにHPE DLTライブラリ28/48スロットを接続するには

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、ページ 374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。詳細については、使用するデバイスのドキュメントを参照してください。

   > **注:**
   > HPE 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、コンピューター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。デフォルトのData Protectorコマンドディレクトリに移動して、devbra -devコマンドを実行します。

   devbraコマンドの出力リストに、HPE 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。

次に行う手順

HPE DLT Library 28/48スロットライブラリデバイスを適切に接続した後、「*HPE Data Protectorヘルプ*」のキーワード「構成、バックアップデバイス」で、新たに接続したライブラリデバイスに対するData Protectorバックアップデバイスの構成手順を参照してください。

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

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コントローラー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:**
   > 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コントローラーを使用することをお勧めします。また、Ultra2 SCSIコントローラーまたはUltra3 SCSIコントローラー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。これらのファイルは、次のコマンドを使用して一覧表示できます。`ls -all`.

この次に行う作業

Seagate Viper 200 LTO Ultrium Tapeドライブを適切に接続した後、「*HPE Data Protectorヘルプ*」のキーワード「構成、バックアップデバイス」で、新たに接続したデバイスに対するData Protectorバックアップデバイスの構成手順を参照してください。

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

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、ページ 374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。詳細については、使用するデバイスのドキュメントを参照してください。
1. デバイス、コンピューター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。デフォルトのData Protectorコマンドディレクトリに移動して、`devbra -dev`コマンドを実行します。

   `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。

次に行う手順

Seagate Viper 200 LTO Ultrium Tapeドライブを適切に接続した後、「*HPE Data Protectorヘルプ*」のキーワード「構成、バックアップデバイス」で、新たに接続したデバイスに対するData Protectorバックアップデバイスの構成手順を参照してください。

> **注:**
> 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`パラメーターを指定します。
>
> ```
> scsi2:0:0:0C
> ```

付録D: 詳細

> **注:**
> このドキュメントセットはHPEサポートWebサイト(https://softwaresupport.hpe.com/)で利用できます。このドキュメントセットには最新の更新情報および修正情報が記載されています。

Data Protectorドキュメントセットには、次の場所からアクセスできます。

- Data Protectorインストールディレクトリ

  Windowsシステムの場合:*Data_Protector_home*\docs

  UNIXシステムの場合:/opt/omni/doc/C
- Data ProtectorGUIの**[ヘルプ]**メニュー
- HPEサポートWebサイト(https://softwaresupport.hpe.com/)

Data Protectorドキュメントを表示するための要件

Data Protectorガイドやヘルプを表示するには、サポートされているPDFドキュメントビューアーとWebブラウザーをインストールする必要があります。サポートされているアプリケーションとバージョンを以下に示します。HPEは、お使いのオペレーティングシステムで利用可能な最新バージョンを使用することをお勧めします。

- ガイドを表示するには、Adobe Readerが必要です。以下のバージョンがサポートされます。

  Windows、SolarisおよびLinuxシステムの場合:

  - Adobe Reader 9以降

    http://get.adobe.com/reader/からダウンロードできます。

  HP-UXシステムの場合:

  - Adobe Reader 7以降

    ftp://ftp.adobe.com/pub/adobe/reader/unis/7x/7.0.9/enu/からダウンロードできます。

  その他のPDFドキュメントビューアーでも本要件を満たす場合がありますが、テストは行っていません。
- ヘルプの表示には、Data ProtectorのGUIプロセスと同じアカウントで実行可能なWebブラウザーが必要です。Webブラウザーで、JavaScriptを有効にしてください。サポートされているWebブラウザーを以下に示します。

  Windowsシステムの場合:

  - Windows Internet Explorer 8.0以降 [1]

    ローカルPCに格納されたWebサイトでは、互換表示を無効にする必要があります。

    http://windows.microsoft.com/ja-jp/internet-explorer/download-ieからWindows Internet Explorerをダウンロードできます。

[1] これも、Microsoft Exchange Server用HPE Data Protector Granular Recovery Extensionのヘルプを表示するための要件です。

- Mozilla Firefox 17.0.5 (延長サポート版)以降
  http://www.mozilla.org/en-US/firefox/organizations/all.htmlからダウンロードできます。

その他のWebブラウザーでも本要件を満たす場合がありますが、テストは行っていません。

ヘルプ

Data Protectorをインストールしていない場合でも、任意のインストールパッケージ(zip/tar)の最上位ディレクトリからヘルプにアクセスできます。

Windowsシステムの場合:DP_help.chmを開いています。

UNIXシステムの場合:圧縮されたtarファイルDP_help.tar.gzをアンパックし、DP_help.htmを開きます。

ドキュメントマップ

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

											インテグレーションガイド					ZDBガイド		GREガイド		
	管理者	ヘルプ	スタートアップ	コンセプト	インストール	トラブルシューティング	DR	CLI	PA	用統合ソフトウェアVSS	MSFT	Oracle/SAP	IBM	Sybase/NDMP	仮想環境	ZDB管理者	ZDB IG	Exchange	SharePoint	VMware
管理タスク	X	X																		
バックアップ		X	X	X						X	X	X	X	X	X	X	X			
CLI								X												
コンセプト、テクニック		X		X						X	X	X	X	X	X	X	X	X	X	X
ディザスタリカバリ				X			X													
インストール、アップグレード			X		X				X											
インスタントリカバリ				X	X											X	X			
ライセンス					X				X											
制限事項		X			X	X			X	X	X	X	X	X	X		X			
新機能		X							X											
計画戦略		X		X																
手順、タスク	X	X			X	X	X			X	X	X	X	X	X	X	X	X	X	X
推奨事項				X					X											
要件					X				X	X	X	X	X	X	X					
復元	X	X	X	X						X	X	X	X	X	X	X	X	X	X	X
サポートされている構成				X																
トラブルシューティング		X			X	X				X	X	X	X	X	X	X	X	X	X	X

略称

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

略称	ドキュメント	
Admin	管理者ガイド	このガイドはData Protectorの管理タスクを説明しています。
CLI	Command Line Interface Reference	このガイドでは、Data Protectorのコマンドラインインターフェイス、コマンドオプション、およびそれらの使用方法を説明し、基本コマンドラインの例を示します。
Concepts	コンセプトガイド	このガイドでは、Data Protectorのコンセプトとゼロダウンタイムバックアップ(ZDB)のコンセプトを解説するとともに、Data Protectorの動作原理を詳細に説明しています。これは、タスク指向のヘルプとともに使用するように、作成されています。
DR	ディザスタリカバリガイド	このガイドでは、ディザスタリカバリのプランニング、準備、テスト、および実行の方法について説明します。
Getting Started	スタートアップガイド	このガイドでは、Data Protectorでの操作をすぐに開始するための情報を記載しています。インストールの前提条件を一覧し、基本的なバックアップ環境のインストールと構成の手順、およびバックアップと復元の実行手順を記載しています。また、詳細な情報を記載しているリソースについても一覧しています。
GRE Guide	Granular Recovery Extensionユーザーガイド - Microsoft SharePoint Server、ExchangeおよびVMware	このガイドでは、次の製品用のData Protector Granular Recovery Extensionの構成方法と使用方法について説明します。 • Microsoft SharePoint Server • Exchange Server • VMware vSphere
ヘルプ	ヘルプ	
Install	インストールガイド	このガイドでは、実際の環境のオペレーティングシステムとアーキテクチャーに応じたData Protectorソフトウェアのインストール方法を説明します。また、Data Protectorのアップグレード方法と、環境に応じた適切なライセンスの取得方法も説明します。

略称	ドキュメント	
インテグレーションガイド	インテグレーションガイド	このガイドでは、Data Protectorを次のプリケーションと統合する方法を説明します。 • **MSFT:**Microsoft SQL Server、Microsoft SharePoint Server、およびMicrosoft Exchange Server。 • **IBM:**Informix Server、IBM DB2 UDB、およびLotus Notes/Domino Server。 • **Oracle/SAP:**Oracle Server、SAP R3、SAP MaxDB、およびSAP HANA Appliance。 • **Sybase/NDMP:**SybaseおよびNetwork Data Management Protocol Server。 • **仮想環境:**VMware vSphere、VMware vCloud Director、Microsoft Hyper-V、およびCitrix XenServerとの仮想環境統合
Integration VSS	Integration Guide for Microsoft Volume Shadow Copy Service	このガイドでは、Data ProtectorとMicrosoftボリュームシャドウコピーサービスとの統合について説明します。
PA	製品案内、ソフトウェアノートおよびリファレンス	このガイドでは、最新リリースの新機能について説明しています。また、インストール要件、必要なパッチ、制限事項、報告されている問題とその回避方法などの情報も記載しています。
トラブルシューティング	トラブルシューティングガイド	このガイドでは、Data Protectorの使用時に発生する可能性がある問題をトラブルシューティングする方法について説明します。
ZDB Admin	ZDB管理者ガイド	このガイドでは、Data ProtectorとHPE P4000 SANソリューション、HPE P6000 EVAディスクアレイファミリ、HPE P9000 XPディスクアレイファミリ、HPE 3PAR StoreServ Storage、NetApp Storage、EMC Symmetrix Remote Data FacilityおよびEMC TimeFinderとの統合を構成し、使用する方法を説明します。このガイドは、バックアップ管理者やオペレーターを対象としています。ファイルシステムとディスクイメージのゼロダウンタイムバックアップ、イ

略称	ドキュメント	
		ンスタントリカバリ、および復元についても説明します。
ZDB IG	ZDBインテグレーションガイド	このガイドでは、Oracle Server、SAP R/3、Microsoft Exchange Server、およびMicrosoft SQL Serverの各データベース、およびVMwareの仮想環境についてゼロダウンタイムバックアップ、インスタントリカバリ、標準的な復元を実行するためのData Protectorの構成方法と使用方法について説明します。

統合

ソフトウェアアプリケーション統合

ソフトウェアアプリケーション	ガイド
IBM DB2 UDB	インテグレーションガイド
Informix Server	インテグレーションガイド
Lotus Notes/Domino Server	インテグレーションガイド
Microsoft Exchange Server	インテグレーションガイド、ZDB IG、GRE Guide
Microsoft Hyper-V	インテグレーションガイド
Microsoft SharePoint Server	インテグレーションガイド、ZDB IG、GRE Guide
Microsoft SQL Server	インテグレーションガイド、ZDB IG
Microsoftボリュームシャドウコピーサービス(VSS)	Integration VSS
Network Data Management Protocol (NDMP) Server	インテグレーションガイド
Oracle Server	インテグレーションガイド、ZDB IG
SAP HANA Appliance	インテグレーションガイド
SAP MaxDB	インテグレーションガイド

ソフトウェアアプリケーション	ガイド
SAP R/3	インテグレーションガイド、ZDB IG
Sybase Server	インテグレーションガイド
VMware vCloud Director	インテグレーションガイド
VMware vSphere	インテグレーションガイド、ZDB IG、GRE Guide

ディスクアレイシステム統合

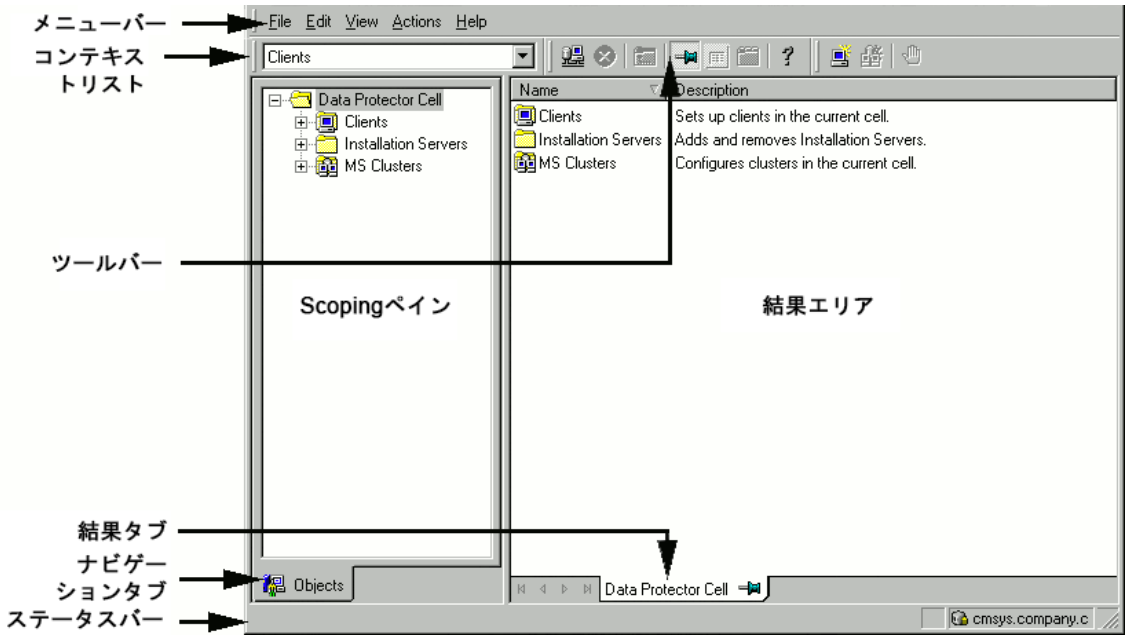
以下のディスクアレイシステムファミリとの統合に関する詳細については、該当するガイドを参照してください。

ディスクアレイファミリ	ガイド
EMC Symmetrix	すべてのZDB
HPE P4000 SANソリューション	コンセプト、ZDB Admin、インテグレーションガイド
HPE P6000 EVAディスクアレイファミリ	すべてのZDB、インテグレーションガイド
HPE P9000 XPディスクアレイファミリ	すべてのZDB、インテグレーションガイド
HPE 3PAR StoreServ Storage	コンセプト、ZDB Admin、インテグレーションガイド
NetApp Storage	すべてのZDB

Data Protectorグラフィカルユーザーインターフェイス

Data Protectorでは、Microsoft Windowsオペレーティングシステムにグラフィカルユーザーインターフェイスを提供します。詳細については、『*HPEHP Data Protectorヘルプ*』を参照してください。

Data Protectorグラフィカルユーザーインターフェイス



フィードバックを送信

このドキュメントに関するご意見は、ドキュメンテーションチームまで電子メールでお送りください。お使いのシステムに電子メールクライアントが設定されている場合は、上のリンクをクリックすると、電子メールウィンドウが開き、件名行に次の情報が入力されます。

インストールガイド (Data Protector 10.00)に関するフィードバック

本文にご意見、ご感想を記入の上、**[送信]**をクリックしてください。

電子メールクライアントが利用できない場合は、上記の情報をコピーしてWebメールクライアントの新規メッセージに貼り付け、AutonomyTPFeedback@hpe.com宛にお送りください。

お客様からのご意見、ご感想をお待ちしています。