HP Data Protector A.06.10 Guide d'installation et de choix des licences

Référence: B6960-96067
Première Édition: Novembre 2008

Informations juridiques

© Copyright 1999, 2008 Hewlett-Packard Development Company, L.P.

Logiciel informatique confidentiel. Licence HP valide requise pour la possession, l'utilisation ou la copie. En accord avec les articles FAR 12.211 et 12.212, les logiciels informatiques, la documentation des logiciels et les informations techniques commerciales sont concédés au gouvernement américain sous licence commerciale standard du fournisseur.

Les informations figurant dans le présent document sont sujettes à modification sans préavis. Les seules garanties relatives aux produits et services HP sont décrites dans les déclarations de garantie expresse accompagnant lesdits produits et services. Aucun élément du présent document ne saurait être considéré comme une garantie supplémentaire. HP ne saurait être tenu pour responsable des erreurs techniques ou éditoriales ou des omissions figurant dans le présent document.

Intel, Itanium, Pentium, Intel Inside et le logo Intel Inside sont des marques commerciales ou des marques déposées d'Intel Corporation ou de ses filiales aux Etats-Unis et dans d'autres pays.

Microsoft, Windows, Windows XP et Windows NT sont des marques déposées de Microsoft Corporation aux Etats-Unis.

Adobe et Acrobat sont des marques commerciales d'Adobe Systems Incorporated.

Java est une marque commerciale de Sun Microsystems, Inc. aux Etats-Unis.

Oracle est une marque déposée aux Etats-Unis de Oracle Corporation, Redwood City, Californie.

UNIX est une marque déposée de The Open Group.

Imprimé aux Etats-Unis.

Sommaire

Historique des publications 17
A propos de ce guide 19
Public visé 19
Documentation 19
Guides 19
Aide en ligne 22
Organisation de la documentation 22
Abréviations 22
Tableau de documentation 23
Intégrations 24
Conventions typographiques et symboles 26
Interface utilisateur graphique de Data Protector 27
Informations générales 27
Assistance technique HP 27
Support technique par e-mail 28
Sites Web HP 28
Vos commentaires sur la documentation 28

1 Présentation de la procédure d'installation 29
Description du chapitre 29
Présentation de la procédure d'installation 29
Concept d'installation à distance 32
DVD-ROM d'installation de Data Protector 34
Choix du système Gestionnaire de cellule 35
Choix du système de l'interface utilisateur de Data Protector 37
Interface graphique utilisateur de Data Protector 38

2 Installation de Data Protector sur votre réseau 41
Description du chapitre 41
Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector 42
Installation d'un Gestionnaire de cellule UNIX 44
Définition des paramètres de noyau 45
Procédure d'installation 46
Structure des répertoires installés sous HP-UX, Solaris et Linux 48
Configuration du démarrage et de l'arrêt automatiques 49

Configuration des variables d'environnement 51
Allocation d'espace disque supplémentaire pour l'installation du Gestionnaire de cellule 52
Etape suivante 52
Installation d'un Gestionnaire de cellule Windows 52
Procédure d'installation 54
Après l'installation 59
Dépannage 61
Etape suivante 61
Installation des Serveurs d'installation 61
Installation des Serveurs d'installation pour UNIX 62
Installation d'un Serveur d'installation pour Windows 65
Installation des clients Data Protector 70
Composants Data Protector 73
Installation distante de clients Data Protector 78
Installation à distance via un shell sécurisé 84
Installation de clients Windows 87
Installation locale 89
Connexion d'un périphérique de sauvegarde aux systèmes Windows 92
Installation de clients HP-UX 94
Vérification de la configuration du noyau sous HP-UX 95
Connexion d'un périphérique de sauvegarde aux systèmes HP-UX 96
Installation de clients Solaris 97
Configuration post-installation 99
Connexion d'un périphérique de sauvegarde à un système Solaris 102
Installation de clients Linux 103
Connexion d'un périphérique de sauvegarde à un système Linux 108
Installation des clients ESX Server 109
Installation de clients AIX 110
Connexion d'un périphérique de sauvegarde à un client AIX 111
Installation de clients Siemens Sinix 112
Connexion d'un périphérique de sauvegarde à un système Siemens Sinix . . 112
Installation de clients Tru64 114
Connexion d'un périphérique de sauvegarde à un client Tru64 115
Installation de clients SCO 116
Connexion d'un périphérique de sauvegarde à un système SCO 117
Installation d'un Agent de support pour l'utilisation de la bibliothèque ADIC/GRAU ou de la bibliothèque StorageTek 118
Connexion de lecteurs de bibliothèque 119
Préparation des clients Data Protector à l'utilisation des bibliothèques ADIC/GRAU 119
Installation d'un Agent de support pour l'utilisation de la bibliothèque ADIC/GRAU 120
Préparation des clients Data Protector à l'utilisation des bibliothèques StorageTek 124
Installation d'un Agent de support pour l'utilisation de la bibliothèque StorageTek 125
Installation locale de clients Novell NetWare 126
Installation locale de clients HP OpenVMS 132

Installation de clients MPE/iX . . . 139
Installation locale de clients UNIX . . . 142
Installation des clients d'intégration Data Protector . . . 145
Installation en local . . . 148
Installation distante . . . 148
Installation des intégrations compatibles cluster . . . 148
Clients Microsoft Exchange Server . . . 149
Clients Microsoft SQL Server . . . 149
Clients Microsoft SharePoint Portal Server . . . 150
Clients Sybase . . . 150
Clients Informix Server . . . 150
IBM HACMP Cluster . . . 151
Clients SAP R/3 . . . 151
Clients SAP DB/MaxDB . . . 151
Clients Oracle . . . 152
Clients VMware Virtual Infrastructure . . . 152
Clients DB2 . . . 153
Clients NNM . . . 153
Clients NDMP . . . 153
Clients Microsoft Volume Shadow Copy Service . . . 153
Clients Lotus Notes/Domino Server . . . 154
Cluster Lotus Domino . . . 154
Intégration EMC Symmetrix . . . 154
Intégration EMC Symmetrix avec Oracle . . . 155
Intégration EMC Symmetrix avec SAP R/3 . . . 156
Intégration d'EMC Symmetrix avec Microsoft SQL Server . . . 159
Intégration HP StorageWorks Disk Array XP . . . 159
Intégration HP StorageWorks Disk Array XP avec Oracle . . . 160
Intégration de HP StorageWorks Disk Array XP avec SAP R/3 . . . 161
Intégration HP StorageWorks Disk Array XP avec Microsoft Exchange Server . . . 164
Intégration de HP StorageWorks Disk Array XP avec Microsoft SQL Server . . . 165
Intégration HP StorageWorks Virtual Array . . . 165
Intégration de HP StorageWorks VA avec Oracle . . . 166
Intégration de HP StorageWorks VA avec SAP R/3 . . . 168
Intégration HP StorageWorks VA avec Microsoft Exchange Server . . . 171
Intégration de HP StorageWorks VA avec Microsoft SQL Server . . . 171
Intégration HP StorageWorks Enterprise Virtual Array . . . 171
Intégration de HP StorageWorks EVA avec Oracle . . . 172
Intégration de HP StorageWorks EVA avec SAP R/3 . . . 174
Intégration HP StorageWorks EVA avec Microsoft Exchange Server . . . 177
Intégration de HP StorageWorks EVA avec MS SQL . . . 177
Clients IAP . . . 178
Clients d'auto-migration VLS . . . 179
Installation de l'interface utilisateur localisée de Data Protector . . . 180
Installation de l'interface utilisateur localisée de Data Protector sur les systèmes Windows . . . 180
Installation de l'interface utilisateur localisée de Data Protector sur les systèmes UNIX 182

Dépannage 183
Installation de l'Edition serveur unique de Data Protector 184
Limites de l'Edition serveur unique pour Windows 184
Limites de l'Edition serveur unique pour HP-UX et Solaris 184
Installation des Rapports Web de Data Protector 185
Installation de Data Protector sur MC/ServiceGuard 186
Installation d'un Gestionnaire de cellule compatible cluster 186
Installation d'un client compatible cluster 187
Installation de Data Protector sur Microsoft Cluster Server 187
Installation d'un Gestionnaire de cellule compatible cluster 188
Installation de clients compatibles cluster 197
Installation de clients Data Protector sur un cluster Veritas 200
Installation d'un client 200
Installation de clients Data Protector sur un cluster Novell NetWare 201
Installation d'un client 201
Installation de Data Protector sur un cluster IBM HACMP 203
Installation de clients compatibles cluster 203

3 Gestion de l'installation 205
Description du chapitre 205
Importation de clients dans une cellule 205
Importation d'un serveur d'installation dans une cellule 207
Importation d'un client compatible cluster dans une cellule 208
Microsoft Cluster Server 208
Autres clusters 209
Exportation de clients d'une cellule 211
Considérations sur la sécurité 214
Couches de sécurité 214
Sécurité client 214
Utilisateurs de Data Protector 215
Sécurité du Gestionnaire de cellule 216
Autres aspects de la sécurité 216
Sécurisation de clients 217
Les fichiers allow_hosts et deny_hosts 222
Enregistrement excessif dans le fichier inet.log 223
Vérification stricte du nom d'hôte 223
Activation de la fonction 225
Droit utilisateur de démarrage de spécification de sauvegarde 225
Masquage du contenu des spécifications de sauvegarde 226
Groupement d'hôtes approuvés 226
Surveillance des événements de sécurité 227
Contrôle des correctifs Data Protector installés 228
Contrôle des correctifs Data Protector à l'aide de l'interface graphique utilisateur . 228
Contrôle des correctifs Data Protector à l'aide de l'interface de ligne de commande 229
Désinstallation du logiciel Data Protector 230
Désinstallation d'un client Data Protector 231
Désinstallation du Gestionnaire de cellule et du Serveur d'installation 232

Désinstallation dans un système Windows 232
Désinstallation dans un système HP-UX 234
Désinstallation du Gestionnaire de cellule et/ou du Serveur d'installation configuré(s) sur MC/ServiceGuard 234
Désinstallation dans les systèmes Solaris 237
Désinstallation dans les systèmes Linux 239
Suppression manuelle du logiciel Data Protector sous UNIX 241
Changement de composants logiciels Data Protector 242

4 Mise à niveau vers Data Protector A.06.10 247
Description du chapitre 247
Présentation de la mise à niveau 247
Séquence de mise à niveau 248
Conversion nécessaire des noms de fichier de la base de données IDB 249
Auto-migration des clés de cryptage 250
Mise à niveau à partir de Data Protector A.05.10, A.05.50 et A.06.00 250
Mise à niveau du Gestionnaire de cellule et du Serveur d'installation UNIX 251
Mise à niveau d'un Gestionnaire de cellule 251
Mise à niveau d'un Serveur d'installation 254
Mise à niveau du Gestionnaire de cellule et du Serveur d'installation Windows . . 256
Vérification des changements de configuration 261
Mise à niveau des clients 263
Mise à niveau de l'intégration Oracle 265
Mise à niveau de l'intégration SAP R/3 267
Mise à niveau de l'intégration du serveur Informix sur des systèmes UNIX . . 268
Mise à niveau de l'intégration du serveur Informix sur des systèmes Windows . 269
Mise à niveau de l'intégration Sybase sur des systèmes UNIX 270
Mise à niveau de l'intégration Sybase sur des systèmes Windows 272
Mise à niveau de l'intégration de HP StorageWorks EVA 273
Mise à niveau du module de récupération automatique après sinistre 275
Mise à niveau des autres intégrations 276
Mise à niveau dans un environnement MoM 276
Conversion des noms de fichiers de la base de données IDB 277
Conversion de l'IDB dans un Gestionnaire de cellule sous Windows 281
Conversion de l'IDB dans un Gestionnaire de cellule sous UNIX 283
Mise à niveau à partir de l'Edition serveur unique 284
Mise à niveau des versions antérieures de l'Edition serveur unique (SSE) vers Data Protector A.06.10 Edition serveur unique (SSE) 284
Mise à niveau de Data Protector A.06.10 Edition serveur unique (SSE) vers Data Protector A.06.10 285
Mise à niveau du Gestionnaire de cellule 285
Mise à niveau de plusieurs installations 285
Mise à niveau à partir de HP StorageWorks Application Recovery Manager A.06.00 . 286
Sauvegarde de la base de données interne après la mise à niveau 287
Mise à niveau de spécifications de sauvegarde 287
Changements dans l'utilisation de la commande omnib 287
Mise à niveau de Windows NT vers une nouvelle version de Windows 288

Mise à niveau de Solaris 8 vers Solaris 9 288
Migration de HP-UX 11.x (PA-RISC) vers HP-UX 11.23/11.31 (IA-64) 289
Informations spécifiques à MoM 292
Détails relatifs au Serveur d'installation 293
Migration d'un système Windows 32 bits/64 bits vers un système Windows 64 bits/Windows Server 2008 294
Informations spécifiques à MoM 297
Détails relatifs au Serveur d'installation 298
Mise à niveau du Gestionnaire de cellule configuré sur MC/ServiceGuard 298
Mise à niveau du Gestionnaire de cellule configuré sur Microsoft Cluster Server 302

5 Attribution de licences Data Protector 307
Description du chapitre 307
Introduction 307
Vérification et signalement des licences manquantes 307
Licences liées au Gestionnaire de cellule 308
Licences basées sur les entités 308
Licences basées sur la capacité 309
Calcul de la capacité utilisée 310
Licence de sauvegarde avancée sur disque 314
Extension de sauvegarde sur HP IAP 314
Exemples de licences basées sur la capacité 314
Production d'un rapport de licences sur demande 318
Quelles sont les licences disponibles ? 319
A propos des mots de passe 320
Mots de passe Data Protector 321
Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP AutoPass 322
Autres moyens d'obtenir et d'installer des mots de passe permanents 325
Vérification du mot de passe 328
Recherche du nombre de licences installées 329
Déplacement des licences vers un autre système Gestionnaire de cellule 329
Gestion centralisée des licences 330
Outil de commande Data Protector 331

6 Résolution des problèmes d'installation 333
Description du chapitre 333
Problèmes de résolution de noms lors de l'installation du Gestionnaire de cellule Windows 333
Vérification des connexions DNS dans la cellule Data Protector 334
Utilisation de la commande omnicheck 335
Résolution des problèmes d'installation et de mise à niveau de Data Protector 336
Problèmes lors de l'installation à distance des clients Windows 338
Résolution des problèmes d'installation du Gestionnaire de cellule Data Protector sous Solaris 338
Résolution des problèmes d'installation des clients UNIX 340
Résolution des problèmes d'installation des clients Windows XP 340

Résolution des problèmes d'installation des clients Windows Vista et Windows Server 2008 . . . 341
Vérification de l'installation du client Data Protector . . . 342
Résolution des problèmes de la mise à niveau . . . 343
Procédure de mise à niveau manuelle . . . 345
Utilisation des fichiers journaux . . . 345
Installation en local . . . 345
Installation distante . . . 346
Fichiers journaux Data Protector . . . 346
Création de traces d'exécution de l'installation . . . 347

A Annexe A . . . 349
Structure de produit et licences de Data Protector A.06.10 . . . 349
Packs Starter . . . 350
Supports . . . 351
Manuels . . . 351
Extensions de lecteur et de bibliothèque . . . 352
Extensions fonctionnelles . . . 354
Editions serveur unique (SSE) . . . 363
Licence . . . 363
Migration . . . 363
Supports . . . 364
Manuels . . . 364
Migration de licence vers Data Protector A.06.10 . . . 364
Data Protector A.05.10, A.05.50 et A.06.00 . . . 365
Présentation de la licence graphique . . . 365
Formulaires d'attribution de licences Data Protector . . . 369

B Annexe B . . . 373
Dans cette annexe . . . 373
Installation sur des systèmes HP-UX, Solaris et Linux à l'aide d'outils natifs . . . 373
Installation d'un Gestionnaire de cellule sur un système HP-UX à l'aide de swinstall 373
Installation d'un Gestionnaire de cellule sur des systèmes Solaris à l'aide de pkgadd 375
Installation du Gestionnaire de cellule sur des systèmes Linux à l'aide de rpm . . . 377
Installation d'un Serveur d'installation sur un système HP-UX à l'aide de swinstall . 379
Installation d'un Serveur d'installation sur des systèmes Solaris à l'aide de pkgadd 380
Installation d'un Serveur d'installation sur des systèmes Linux à l'aide de rpm . . . 384
Installation des clients . . . 387
Mise à niveau sur des systèmes HP-UX, Solaris et Linux à l'aide d'outils natifs . . . 388
Mise à niveau de Data Protector sur les systèmes HP-UX à l'aide de swinstall . . . 388
Mise à niveau de Data Protector sur les systèmes Solaris à l'aide de pkgadd . . . 389
Mise à niveau de Data Protector sur des systèmes Linux à l'aide de rpm . . . 390
Paramétrage du protocole TCP/IP sur les systèmes Windows . . . 391
Installation et configuration du protocole TCP/IP sous Windows . . . 392
Vérification de la configuration TCP/IP . . . 395
Modification du nom du Gestionnaire de cellule . . . 397

Modification du numéro de port par défaut 398
Modification du numéro de port par défaut de Data Protector 398
Modification du numéro de port par défaut pour l'interface graphique Java . . 400
Préparation d'un serveur NIS 401
Utilisation de pilotes de bandes et de pilotes de robots sous Windows 402
Création de fichiers de périphérique (adresses SCSI) sous Windows 406
Configuration de robot SCSI sous HP-UX 407
Création de fichiers de périphérique sous HP-UX 412
Configuration des paramètres du contrôleur SCSI 414
Recherche des adresses SCSI non utilisées sous HP-UX 414
Recherche des ID SCSI cibles inutilisés sous Solaris 416
Mise à jour de la configuration des périphériques et pilotes sur un système Solaris . . . 417
Mise à jour des fichiers de configuration 417
Création et vérification de fichiers de périphérique 420
Recherche des ID SCSI cibles inutilisés sur un système Windows 421
Configuration des ID SCSI sur une bibliothèque HP StorageWorks 330fx 422
Connexion de périphériques de sauvegarde 423
Connexion d'un périphérique autonome HP StorageWorks 24 426
Connexion d'un chargeur automatique DAT HP StorageWorks 428
Connexion d'une bibliothèque DLT 28/48 logements HP StorageWorks 430
Connexion d'un lecteur de bandes Seagate Viper 200 LTO Ultrium 434
Vérification de l'installation de l'Agent général de support sous Novell NetWare . . . 436
Identification du périphérique de stockage 437
Test de démarrage de l'Agent général de support 437
Test du démarrage de HPUMA.NLM et de HPDEVBRA.NLM 440
Installation de Data Protector sur Microsoft Cluster avec Veritas Volume Manager . . . 441
Modification du chemin des fichiers de configuration dans Data Protector A.06.10 . . . 442
Fichiers de configuration sous UNIX 442
Fichiers de configuration sous Windows 444
Modifications de la ligne de commande après la mise à niveau vers Data Protector A.06.10 445

Glossaire 467

Index 529

Figures

1 Interface utilisateur graphique de Data Protector 27
2 Cellule Data Protector 32
3 Concept d'installation de Data Protector 34
4 Interface graphique utilisateur de Data Protector 39
5 Procédure d'installation 43
6 Sélection du type d'installation 55
7 Sélection des composants logiciels 56
8 Liste des composants sélectionnés 57
9 Page d'état de l'installation 58
10 Sélection d'AutoPass pour l'installation 59
11 Sélection du type d'installation 67
12 Page de résumé des composants sélectionnés 68
13 Page d'état de l'installation 69
14 Sélection de clients 80
15 Sélection de composants 81
16 Sélection de clients 83
17 Sélection de composants 84
18 Choix du Gestionnaire de cellule 90
19 Page de résumé des composants sélectionnés 91
20 Page de résumé de l'installation 92
21 Fenêtre de configuration du kernel 96
22 Format de nom de fichier de périphérique 114
23 Format de nom de fichier de périphérique 118
24 Sélection du support de langue lors de l'installation 181
25 Installation à distance du support de langue 182

26 Sélection du type d'installation 190
27 Sélection de la ressource de cluster sous Windows Server 2008 191
28 Sélection de la ressource de cluster sur les autres systèmes Windows . . . 192
29 Saisie des informations relatives au compte 193
30 Page de sélection des composants 194
31 Page d'état de l'installation 195
32 Compte utilisateur Data Protector 196
33 Sélection du mode d'installation compatible cluster 198
34 Compte utilisateur Data Protector 199
35 Importation d'un client vers la cellule 207
36 Importation d'un client Microsoft Cluster Server dans une cellule 209
37 Importation d'un client MC/ServiceGuard, Veritas ou Novell NetWare Cluster Services dans une cellule 211
38 Exportation d'un système client 213
39 Sécurisation d'un client 219
40 Activation de la sécurité sur les clients sélectionnés 220
41 Activation de la sécurité pour tous les clients de la cellule 221
42 Vérification des correctifs installés 229
43 Page de résumé des composants sélectionnés 258
44 Page d'état de l'installation 259
45 Sélection d'AutoPass pour l'installation 260
46 Conversion de l'IDB après mise à niveau 282
47 Sélection des composants 303
48 Page de résumé des composants sélectionnés 304
49 Page d'état de l'installation 305
50 Scénario de calcul de la capacité utilisée 311
51 Sessions de sauvegarde avec temps d'indisponibilité nul sur disque . . . 315
52 Sessions de sauvegarde avec temps d'indisponibilité nul sur bande . . . 316
53 Sessions avec temps d'indisponibilité nul sur disque + bande 317
54 Sessions de sauvegarde directe 318

55 Structure du produit HP Data Protector 320
56 Assistant HP AutoPass 325
57 Exemple de résultats fournis par l'outil de commande Data Protector . . . 332
58 Structure du produit HP Data Protector 350
59 Pack Starter pour HP-UX 365
60 Environnement mixte 366
61 61 - 250 emplacements de bibliothèque - exemple 1 366
62 61 - 250 emplacements de bibliothèque - exemple 2 367
63 Sauvegarde en ligne 367
64 Manager-of-Managers 368
65 Sauvegarde avancée sur disque 368
66 Sauvegarde avec temps d'indisponibilité nul 369
67 Edition serveur unique 369
68 Fenêtre Installation SD - Sélection de logiciel 375
69 Fenêtre Propriétés TCP/IP sous Windows 393
70 Paramètres TCP/IP avancés sous Windows 394
71 Suffixe DNS et nom NetBIOS de l'ordinateur sous Windows 395
72 Propriétés du pilote 404
73 Propriétés du changeur de support 405
74 Désactivation des pilotes de robots 406
75 Propriétés du lecteur de bande 407
76 Périphériques SCSI contrôlés 408
77 Gestion des périphériques 408
78 Etat du pilote de passage SCSI (sctl) 409
79 Etat du pilote de passage SCSI - spt 410
80 Liste des périphériques connectés 412
81 Résultats de ioscan -f sur un système HP-UX 415
82 Paramètres du périphérique 422

Tableaux

1 Informations sur cette édition 17
2 Conventions typographiques 26
3 Liste des DVD-ROM Data Protector 35
4 Installation des systèmes client Data Protector 71
5 Installation d'intégrations 72
6 Autres installations 73
7 Codes des composants Data Protector 144
8 Dépendances de composants logiciels Data Protector sous HP-UX 243
9 Dépendances des composants logiciels Data Protector sous Solaris 244
10 Compatibilité EADR et OBDR après une mise à niveau 276
11 Impact de la conversion de noms de fichier sur un Gestionnaire de cellule Windows 278
12 Impact de la conversion de noms de fichier sur un Gestionnaire de cellule UNIX 279
13 Messages retournés 336
14 Numéros de licence des Packs Starter HP Data Protector 350
15 Extensions de lecteur HP Data Protector 352
16 Extensions de lecteur HP Data Protector 353
17 Extensions de bibliothèque HP Data Protector 353
18 Extension en ligne HP Data Protector 354
19 Extension de sauvegarde des fichiers ouverts HP Data Protector 355
20 Extension Manager-of-Managers HP Data Protector 355
21 Extension HP Data Protector Media Operations 356
22 Extension de sauvegarde avancée sur disque HP Data Protector 356
23 Extension de sauvegarde sur HP IAP HP Data Protector 359
24 Extension de sauvegarde avec temps d'indisponibilité nul (ZDB) HP Data Protector 359
25 Extension de restauration instantanée HP Data Protector 360

26 Extension de la sauvegarde directe HP Data Protector 361
27 Sauvegarde directe HP Data Protector à l'aide de NDMP 361
28 Extension de cryptage HP Data Protector 361
29 Manuels imprimés Extensions fonctionnelles HP Data Protector 362
30 Numéros de licence des Packs Starter HP Data Protector SSE 363
31 Contenu du nouveau répertoire /etc/opt/omni/client 443
32 Contenu du nouveau répertoire /var/opt/omni/server 443
33 Contenu du nouveau répertoire répertoire_Data_Protector\Config\client 444
34 Mise à niveau à partir de Data Protector A.05.10 445
35 Mise à niveau à partir de Data Protector A.05.50 452
36 Mise à niveau à partir de Data Protector A.06.00 457
37 Mise à niveau à partir de Application Recovery Manager A.06.00 . . . 462

Historique des publications

Entre les différentes éditions des guides, des mises à jour peuvent être publiées pour corriger des erreurs ou refléter des modifications du produit. Assurez-vous de recevoir les éditions nouvelles ou mises à jour en vous abonnant au service support produit correspondant. Pour plus d'informations, contactez votre représentant HP.

Tableau 1 - Informations sur cette édition

Référence	Edition du guide	Produit
B6960-90058	Août 2002	Data Protector Version A.05.00
B6960-90079	Mai 2003	Data Protector Version A.05.10
B6960-90107	Octobre 2004	Data Protector Version A.05.50
B6960-96002	Juillet 2006	Data Protector Version A.06.00
B6960-96067	Novembre 2008	Data Protector Version A.06.10

A propos de ce guide

Ce guide fournit des informations sur :

- l'installation du produit de réseau Data Protector ;
- les conditions prérequises qui doivent être remplies avant de commencer la procédure d'installation ;
- la mise à niveau et l'attribution de licences.

Public visé

Ce guide s'adresse aux administrateurs responsables de l'installation et de la maintenance de l'environnement informatique, ainsi qu'aux administrateurs de sauvegarde en charge de la planification, de l'installation et de la maintenance de l'environnement de sauvegarde.

Le *Guide conceptuel HP Data Protector* contient des informations sur les concepts fondamentaux du produit. Sa lecture est recommandée en vue d'une meilleure compréhension des bases fondamentales et du modèle conceptuel de Data Protector.

Documentation

Vous pouvez consulter d'autres documents ainsi que l'aide en ligne si vous avez besoin d'informations connexes.

Guides

Les guides de Data Protector sont disponibles sous forme imprimée et au format PDF. Installez les fichiers PDF lors de la procédure d'installation de Data Protector en sélectionnant le composant `Documentation et aide en français` sous Windows ou le composant `OB2-DOCS` sous UNIX. Les guides sont copiés dans le répertoire *`répertoire_Data_Protector`*`\docs` sous Windows et dans le répertoire `/opt/omni/doc/C/` sous UNIX.

Ces documents sont disponibles sur la page Manuals du site Web HP Business Support Center :

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

Dans la section Storage (Stockage), cliquez sur Storage Software (Logiciels de stockage) puis sélectionnez votre produit.

- *Guide conceptuel HP Data Protector*

Ce guide décrit les concepts Data Protector et fournit des informations de fond sur le fonctionnement du logiciel. Il est destiné à être utilisé avec l'aide en ligne qui met l'accent sur les tâches que vous devez réaliser.

- *Guide d'installation et de choix des licences HP Data Protector*
  Ce guide décrit la procédure d'installation de Data Protector en fonction de votre système d'exploitation et de l'architecture de votre environnement. En outre, il contient des informations sur les mises à niveau de Data Protector et sur l'obtention de licences correspondant à votre environnement.
- *Guide de dépannage HP Data Protector*
  Enfin, il décrit comment résoudre les problèmes auxquels vous pouvez être confronté avec Data Protector.
- *Guide de récupération aprs sinistre HP Data Protector*
  Vous y trouverez des instructions pour planifier, préparer et tester des procédures de récupération après sinistre.
- *Guides d'intégration du logiciel HP Data Protector*
  Ces guides décrivent la configuration et l'utilisation de Data Protector dans le cadre de la sauvegarde et de la restauration de différentes bases de données et applications. Ils s'adressent aux opérateurs ou aux administrateurs de sauvegarde. Il existe quatre guides :
  - *Guide d'intégration HP Data Protector pour les applications Microsoft : SQL Server, SharePoint Portal Server, Exchange Server et Volume Shadow Copy Service*
    Ce guide décrit l'intégration de Data Protector avec les applications Microsoft suivantes : Microsoft Exchange Server, Microsoft SQL Server et Volume Shadow Copy Service.
  - *Guide d'intégration HP Data Protector pour Oracle et SAP*
    Ce guide décrit l'intégration de Data Protector avec Oracle, SAP R3 et SAP DB/MaxDB.
  - *Guide d'intégration HP Data Protector pour les applications IBM : Informix, DB2 et Lotus Notes/Domino*
    Ce guide décrit l'intégration de Data Protector avec les applications IBM suivantes : Informix Server, IBM DB2 et Lotus Notes/Domino Server.
  - *Guide d'intégration HP Data Protector pour VMware Virtual Infrastructure, Sybase, Network Node Manager et le serveur NDMP (Network Data Management Protocol)*
    Ce guide décrit l'intégration de Data Protector avec VMware Virtual Infrastructure, Sybase, Network Node Manager et le serveur NDMP (Network Data Management Protocol).
- *Guide d'intégration HP Data Protector pour HP Service Information Portal*
  Ce guide décrit l'installation, la configuration et l'utilisation de l'intégration de Data Protector avec HP Service Information Portal. Il est destiné aux administrateurs de sauvegarde. Il traite notamment de l'utilisation de l'application pour la gestion des services Data Protector.
- *Guide d'intégration HP Data Protector pour HP Reporter*

Ce manuel décrit l'installation, la configuration et l'utilisation de l'intégration de Data Protector avec HP Reporter. Il est destiné aux administrateurs de sauvegarde. Il traite notamment de l'utilisation de l'application pour la gestion des services Data Protector.

- *Guide d'intégration HP Data Protector pour HP Operations Manager sous UNIX*
  Ce guide décrit les procédures de surveillance et de gestion de l'état et des performances de l'environnement Data Protector avec HP Operations Manager et HP Service Navigator sous UNIX.
- *Guide d'intégration HP Data Protector pour HP Operations Manager sous Windows*
  Ce guide décrit les procédures de surveillance et de gestion de l'état et des performances de l'environnement Data Protector avec HP Operations Manager et HP Service Navigator sous Windows.
- *Guide d'intégration de HP Data Protector pour HP Performance Manager et HP Performance Agent*
  Ce guide décrit les procédures de surveillance et de gestion de l'état et des performances de l'environnement Data Protector avec HP Performance Manager (PM) et HP Performance Agent (PA) sous Windows, HP-UX, Solaris et Linux.
- *Guide conceptuel ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*
  Ce guide décrit les concepts Data Protector de sauvegarde avec temps d'indisponibilité nul et de restauration instantanée et fournit des informations de base sur le fonctionnement de Data Protector dans un environnement de sauvegarde avec temps d'indisponibilité nul. Il est destiné à être utilisé avec le *Guide de l'administrateur ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector* et le *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.
- *Guide de l'administrateur ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*
  Ce guide décrit la configuration et l'utilisation de l'intégration de Data Protector avec HP StorageWorks Virtual Array, HP StorageWorks Enterprise Virtual Array, EMC Symmetrix Remote Data Facility, TimeFinder et HP StorageWorks Disk Array XP. Il s'adresse aux opérateurs ou aux administrateurs de sauvegarde. Il traite de la sauvegarde avec temps d'indisponibilité nul, de la restauration instantanée et de la restauration de systèmes de fichiers et d'images disque.
- *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*
  Ce guide décrit la configuration et l'utilisation de Data Protector pour effectuer une sauvegarde avec temps d'indisponibilité nul, une restauration instantanée, ainsi qu'une restauration standard d'Oracle, de SAP R/3, de Microsoft Exchange Server et d'applications de bases de données Microsoft SQL Server. Ce guide décrit également la configuration et l'utilisation de Data Protector pour effectuer une sauvegarde et une restauration avec Microsoft Volume Shadow Copy Service.
- *Guide de l'utilisateur MPE/iX System HP Data Protector*

Ce guide décrit la configuration des clients MPE/iX, ainsi que la sauvegarde et la restauration des données MPE/iX.

- *Guide de l'utilisateur Media Operations HP Data Protector*
  Ce guide vous indique comment procéder au suivi et à la gestion des supports de stockage hors ligne. Il décrit l'installation et la configuration de l'application, la réalisation des opérations quotidiennes relatives aux supports et la production de rapports.
- *Références, notes de publication et annonces produits HP Data Protector*
  Ce guide fournit une description des nouveautés de HP Data Protector A.06.10. Il fournit également des informations sur les configurations prises en charge (périphériques, plates-formes et intégrations de bases de données en ligne, SAN et ZDB), les correctifs requis, les limites, ainsi que les problèmes connus et leurs solutions. Une version mise à jour des configurations prises en charge est disponible à l'adresse suivante : http://www.hp.com/support/manuals
- *Références, notes de publication et annonces produits HP Data Protector pour les intégrations HP Operations Manager, HP Reporter, HP Performance Manager, HP Performance Agent et HP Service Information Portal*
  Ce guide remplit une fonction similaire pour les intégrations énumérées.
- *Références, notes de publication et annonces produits HP Data Protector Media Operations*
  Ce guide remplit une fonction similaire pour Media Operations.

Aide en ligne

Data Protector comporte une aide en ligne contextuelle (F1) et des rubriques d'aide pour les plates-formes Windows et UNIX.

Vous pouvez accéder à l'aide en ligne à partir du répertoire de niveau supérieur situé sur le DVD d'installation sans procéder à l'installation de Data Protector :

- *Windows* : décompressez `DP_help.zip` et ouvrez `DP_help.chm`.
- *UNIX* : décompressez le fichier d'archive `DP_help.tar.gz` et accédez au système d'aide en ligne à partir de `DP_help.htm`.

Organisation de la documentation

Abréviations

Les abréviations utilisées dans le tableau décrivant l'organisation de la documentation sont expliquées ci-dessous. Les titres des guides contiennent tous les mots "HP Data Protector".

Abréviation	Guide
CLI	Référence à l'interface de ligne de commande
Concepts	Guide conceptuel
DR	Guide de récupération après sinistre
GS	Guide de démarrage rapide
Aide	Aide en ligne
IG-IBM	Guide d'intégration — applications IBM
IG-MS	Guide d'intégration — applications Microsoft
IG-O/S	Guide d'intégration — Oracle, SAP R/3 et SAP DB/MaxDB
IG-OMU	Guide d'intégration — HP Operations Manager, UNIX
IG-OMW	Guide d'intégration — HP Operations Manager, Windows
IG-PM/PA	Guide d'intégration — Performance Manager et Performance Agent
IG-Report	Guide d'intégration — HP Reporter
IG-SIP	Guide d'intégration — HP Service Information Portal
IG-Var	Guide d'intégration — VMware, Sybase, Network Node Manager et serveur NDMP
Install	Guide d'installation et de choix des licences
MO GS	Guide de démarrage Media Operations
MO RN	Références, notes de publication et annonces produits Media Operations
MO UG	Guide de l'utilisateur Media Operations
MPE/iX	Guide de l'utilisateur MPE/iX System
PA	Références, notes de publication et annonces produits
Dépan.	Guide de dépannage
ZDB Admin	Guide de l'administrateur ZDB
Concept ZDB	Guide conceptuel ZDB
ZDB IG	Guide d'intégration ZDB

Tableau de documentation

Le tableau suivant indique où trouver différents types d'informations. Les cases grisées signalent des documents à consulter en priorité.

								Guides intégration							ZDB			MO				
	Aide	GS	Concepts	Install.	Dépan.	DR	PA	MS	O/S	IBM	Var	OV	OVOU	OVOW	Concept	Admin	IG	GS	Utilisat.	PA	MPE/iX	CLI
Sauvegarde	X	X	X					X	X	X	X				X	X	X				X	
CLI																						X
Concepts/ Méthodes	X		X					X	X	X	X	X	X	X	X	X	X				X	
Récup. sinistre	X		X			X																
Installation/ Mise à niveau	X	X		X			X					X	X	X				X	X		X	
Rest. instantanée	X		X												X	X	X					
Licences	X			X			X												X			
Limites	X				X		X	X	X	X	X			X			X			X		
Nouvelles fonctions	X						X															
Stratégie planif.	X		X									X			X							
Procédures/ Tâches	X			X	X	X		X	X	X	X	X	X	X		X	X		X			
Recommandations			X				X								X					X		
Condit. requises				X			X	X	X	X	X			X				X	X	X		
Restauration	X	X	X					X	X	X	X					X	X				X	
Matrices support							X															
Configurations prises en charge															X							
Dépannage	X			X	X			X	X	X	X	X				X	X					

Intégrations

Le tableau ci-dessous vous permet de repérer le guide à consulter pour obtenir des détails sur une intégration particulière :

Intégration	Guide
HP Operations Manager pour UNIX/pour Windows	IG-OMU, IG-OMW
HP Performance Manager	IG-PM/PA
HP Performance Agent	IG-PM/PA
HP Reporter	IG-R
HP Service Information Portal	IG-SIP
HP StorageWorks Disk Array XP	tous les ZDB
HP StorageWorks Enterprise Virtual Array (EVA)	tous les ZDB
HP StorageWorks Virtual Array (VA)	tous les ZDB
IBM DB2 UDB	IG-IBM
Informix	IG-IBM
Lotus Notes/Domino	IG-IBM
Media Operations	Utilisateur MO
MPE/iX System	MPE/iX
Microsoft Exchange Server	IG-MS, ZDB IG
Boîte aux lettres Microsoft Exchange unique	IG-MS
Microsoft SQL Server	IG-MS, ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	IG-MS, ZDB IG
Serveur NDMP	IG-Var
Network Node Manager (NNM)	IG-Var
Oracle	IG-O/S
Oracle ZDB	ZDB IG
SAP DB	IG-O/S
SAP R/3	IG-O/S, ZDB IG
Sybase	IG-Var
Symmetrix (EMC)	tous les ZDB
VMware	IG-Var

Conventions typographiques et symboles

Tableau 2 - Conventions typographiques

Convention	Elément
Texte bleu : Tableau 2 à la page 26	Renvois et adresses électroniques
Texte souligné en bleu : http://www.hp.com	Adresses de sites Web
Italiques	Texte mis en évidence
`Police non proportionnelle`	• Noms de fichier et de répertoire • Informations affichées par le système • Code • Commandes et leurs arguments, valeurs des arguments
`Police non proportionnelle + italiques`	• Variables de code • Variables de commande
	Texte rédigé avec une police non proportionnelle et mis en évidence

ATTENTION :

Le non-respect de ces instructions présente des risques, tant pour le matériel que pour les données qu'il contient.

IMPORTANT :

Explications ou instructions spécifiques.

REMARQUE :

Informations complémentaires.

CONSEIL :

Conseils et raccourcis utiles.

Interface utilisateur graphique de Data Protector

L'interface utilisateur graphique de Data Protector se présente de la même façon sous Windows et UNIX. Vous pouvez utiliser l'interface d'origine de Data Protector (sous Windows uniquement) ou l'interface Java de Data Protector. Pour en savoir plus sur l'interface utilisateur graphique de Data Protector, reportez-vous à l'aide en ligne.

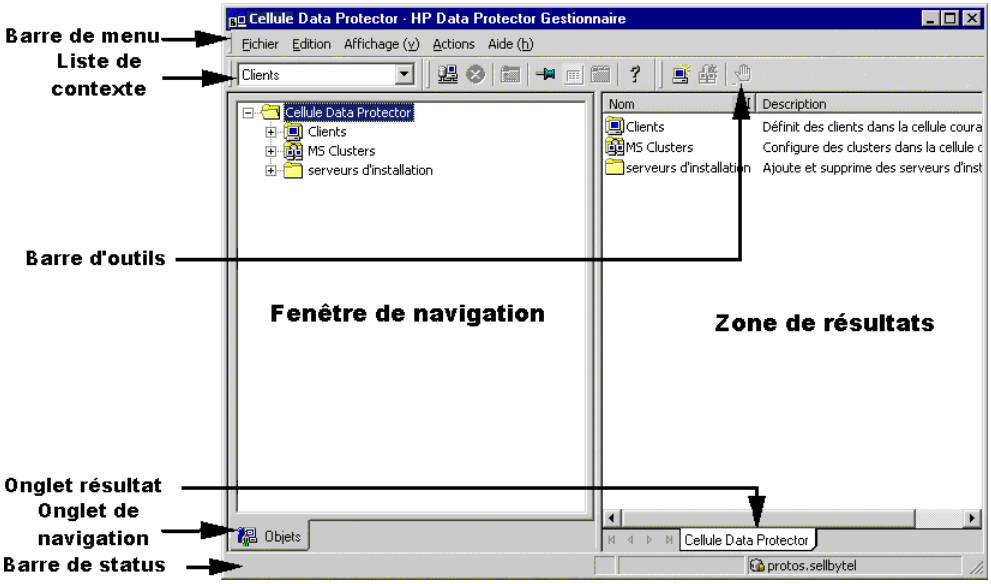

Figure 1 - Interface utilisateur graphique de Data Protector

Informations générales

Vous trouverez des informations générales sur Data Protector à l'adresse suivante : http://www.hp.com/go/dataprotector.

Assistance technique HP

Pour plus d'informations sur l'assistance technique fournie dans les différentes régions du monde, consultez le site Web HP à l'adresse suivante :

http://www.hp.com/support

Avant de contacter HP, assurez-vous de disposer des informations suivantes :

- Nom et numéro de modèle
- Numéro d'enregistrement auprès de l'assistance technique (le cas échéant)

- Numéro de série du produit
- Messages d'erreur
- Type de système d'exploitation et niveau de révision
- Vos questions, aussi détaillées que possible

Support technique par e-mail

HP vous recommande d'enregistrer votre produit sur le site Web Subscriber's Choice for Business :

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

Suite à l'enregistrement, vous recevrez un e-mail vous informant des améliorations apportées au produit, des nouvelles versions de pilotes, des mises à jour de microprogrammes et d'autres ressources disponibles pour le produit.

Sites Web HP

Pour plus d'informations, consultez les sites Web HP suivants :

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

Vos commentaires sur la documentation

HP souhaite connaître votre opinion.

Pour nous faire parvenir vos commentaires et suggestions sur la documentation des produits, veuillez envoyer un message à DP.DocFeedback@hp.com. Toutes les soumissions deviennent propriété de HP.

1 Présentation de la procédure d'installation

Description du chapitre

Ce chapitre offre un aperçu de la procédure d'installation de Data Protector et des concepts qui s'y appliquent. Ce chapitre présente également le Gestionnaire de cellule Data Protector et Data Protector.

Présentation de la procédure d'installation

Un environnement de sauvegarde Data Protector est un ensemble de systèmes doté d'une stratégie de sauvegarde commune dans le même fuseau horaire et sur le même LAN/SAN. Cet environnement réseau est appelé une cellule Data Protector. Une cellule type se compose d'un Gestionnaire de cellule, d'un Serveur d'installation, de clients et de périphériques de sauvegarde.

Le Gestionnaire de cellule est le système principal qui gère la cellule à partir d'un point central. Il contient la base de données interne (IDB) de Data Protector et exécute le logiciel central de Data Protector et les gestionnaires de session.

La base de données IDB se charge du suivi des fichiers sauvegardés et de la configuration de la cellule.

Le Serveur d'installation (IS) est un ordinateur ou un composant Gestionnaire de cellule comprenant le référentiel du logiciel Data Protector utilisé pour les installations de clients distants. Cette fonction de Data Protector facilite considérablement le processus d'installation du logiciel, en particulier pour les clients distants.

Une cellule comprend généralement un Gestionnaire de cellule et plusieurs clients. Un système ordinateur devient un Data Protector client dès que l'un des composants logiciels Data Protector est installé sur le système. L'installation de composants clients sur un système dépend du rôle de ce dernier dans votre environnement de sauvegarde. Les composants Data Protector peuvent être installés en local sur un seul système ou sur plusieurs systèmes à partir de Serveurs d'installation.

Le composant Interface utilisateur est nécessaire pour accéder aux fonctions de Data Protector et permet d'exécuter l'ensemble des tâches de configuration et d'administration. Il doit être installé sur des systèmes utilisés pour l'administration des sauvegardes. Data Protector offre une interface graphique utilisateur (GUI) et une interface de ligne de commande (CLI).

Pour les systèmes client dont les disques doivent être sauvegardés, les composants de l'Agent de disque Data Protector correspondant doivent être installés. L'agent de disque vous permet de sauvegarder des données à partir du disque client ou de les restaurer.

Un composant Agent de support doit être installé sur les systèmes client connectés à un périphérique de sauvegarde . Ce logiciel gère les périphériques et les supports de sauvegarde. On distingue deux Agents de support Data Protector : : l'Agent de support général et l'Agent de support NDMP. L'Agent de support NDMP ne doit être installé que sur des systèmes client qui contrôlent la sauvegarde de données d'un serveur NDMP (systèmes client contrôlant des lecteurs dédiés NDMP). Dans tous les autres cas, les deux Agents de support sont interchangeables.

Avant d'installer Data Protector sur votre réseau, définissez les éléments suivants :

- Le système sur lequel le Gestionnaire de cellule sera installé. Pour connaître les systèmes d'exploitation et les versions pris en charge, reportez-vous aux matrices de support sur le site http://www.hp.com/support/manuals.
  Il ne peut y avoir qu'un seul Gestionnaire de cellule par cellule. L'exécution de Data Protector exige qu'un Gestionnaire de cellule soit installé.
- Les systèmes qui seront utilisés pour accéder aux fonctions de Data Protector via l'interface utilisateur, et qui doivent être dotés du composant Interface utilisateur.
- Les systèmes qui seront sauvegardés et qui doivent être dotés du composant Agent de disque pour la sauvegarde des systèmes de fichiers et du composant Agent d'application approprié pour les intégrations de bases de données en ligne.
- Les systèmes auxquels les périphériques de sauvegarde seront connectés et qui devront être dotés d'un composant Agent de support.
- Le ou les systèmes sur lesquels le ou les serveurs d'installation Data Protector seront installlés. Deux types de serveurs d'installation (IS) sont disponibles pour l'installation des logiciels distants : l'un pour les clients UNIX et l'autre pour les clients Windows.
  Le choix de l'ordinateur utilisé pour le Serveur d'installation est indépendant du Gestionnaire de cellule et du ou des systèmes sur lesquels l'Interface utilisateur est installée. Le Gestionnaire de cellule et le Serveur d'installation peuvent se trouver sur le même système (s'ils sont tous deux destinés à la même plate-forme) ou sur des systèmes différents.
  Un Serveur d'installation peut être partagé par plusieurs cellules Data Protector.

REMARQUE :

Le Serveur d'installation pour Windows doit être installé sur un système Windows. Le Serveur d'installation pour UNIX doit être installé sur un système HP-UX, Solaris ou Linux. Reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector* pour connaître les versions de système d'exploitation prises en charge.

IMPORTANT :

Lorsque vous installez un Gestionnaire de cellule, un Serveur d'installation ou un client Data Protector sur des systèmes Solaris, assurez-vous de bien sauvegarder tous les fichiers se trouvant dans le répertoire `/usr/omni` dans un autre répertoire. L'installation de Data Protector supprime tous les fichiers se trouvant dans le répertoire `/usr/omni`.

Une fois que vous avez déterminé les rôles des systèmes dans votre future cellule Data Protector, la procédure d'installation comprend les étapes générales suivantes :

1. Vérification des conditions préalables à l'installation.
2. Installation du Gestionnaire de cellule Data Protector.
3. Installation du (des) Serveur d'installation et de l'Interface utilisateur.
4. Installation des systèmes client, soit à distance (option recommandée, si possible), soit en local à partir du DVD-ROM.

REMARQUE :

Il est impossible d'installer à distance un client client Data Protector sur un système Windows si un Serveur d'installation est déjà installé sur ce système. Pour installer un Serveur d'installation et un ou plusieurs composants client sur le même système, vous devez effectuer une installation client en local à partir du DVD-ROM d'installation Windows Data Protector. Dans la fenêtre Installation personnalisée, sélectionnez tous les composants client de votre choix ainsi que le composant Serveur d'installation.

L'installation à distance n'est pas possible non plus avec les systèmes client Windows Me/XP Edition familiale, MPE et Novell NetWare. Ceux-ci doivent être installés localement.

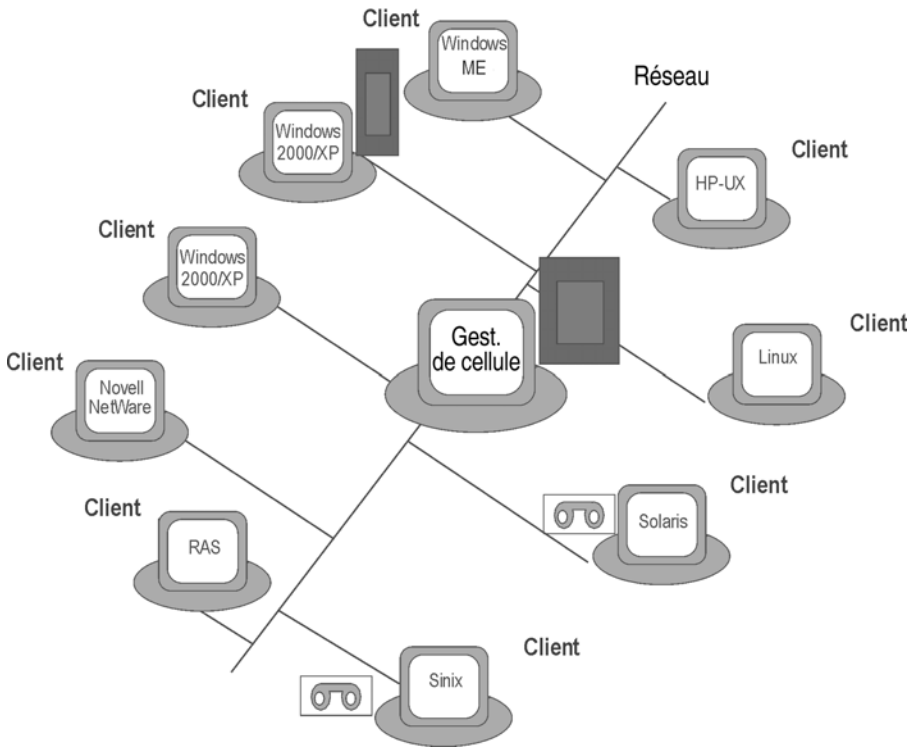

Figure 2 - Cellule Data Protector

Concept d'installation à distance

Une fois que vous avez installé le Gestionnaire de cellule Data Protector, l'Interface utilisateur et le(s) Serveur d'installation (au moins un Serveur d'installation est nécessaire pour chaque plate-forme, UNIX et Windows), vous pouvez distribuer le logiciel Data Protector aux clients utilisant des systèmes d'exploitation pour lesquels l'installation à distance est prise en charge. Reportez-vous à la Figure 3 à la page 34.

Chaque fois que vous effectuez une installation à distance, vous accédez au Serveur d'installation via l'interface utilisateur graphique. Le composant Interface utilisateur peut être installé sur le Gestionnaire de cellule, mais ce n'est pas obligatoire. Il serait plus prudent d'installer cette interface sur plusieurs systèmes afin de pouvoir accéder au Gestionnaire de cellule à partir de différents emplacements.

Le logiciel client peut être distribué sur tout système Windows, à l'exception des versions Me/XP Edition familiale, à partir d'un Serveur d'installation pour Windows.

Les systèmes client sous Windows Me/XP Edition familiale doivent être installés en local à partir du DVD-ROM Data Protector pour Windows.

Data Protector prend également en charge les clients Novell NetWare, même si l'installation client à distance est impossible. L'installation s'effectue via un système Windows relié au réseau Novell.

Le logiciel client peut être installé à distance sur un système d'exploitation UNIX pris en charge, tels que HP-UX, Solaris, Sinix, Linux et AIX à partir d'un Serveur d'installation pour UNIX. Pour obtenir la liste des plates-formes prises en charge, reportez-vous au document Références, notes de publication et annonces produits HP Data Protector.

Pour les systèmes d'exploitation UNIX pour lesquels l'installation à distance n'est pas prise en charge, ou si vous n'installez pas un Serveur d'installation pour UNIX, vous pouvez installer les clients UNIX localement, à partir du DVD-ROM d'installation de Data Protector UNIX.

Notez qu'il existe quelques exceptions qui requièrent une installation à distance uniquement.

Pour plus d'informations sur les méthodes d'installation disponibles pour les différents clients Data Protector, reportez-vous à la section "Installation des clients Data Protector" à la page 70.

Pour connaître la procédure d'installation locale des clients UNIX, reportez-vous à la section "Installation locale de clients UNIX" à la page 142.

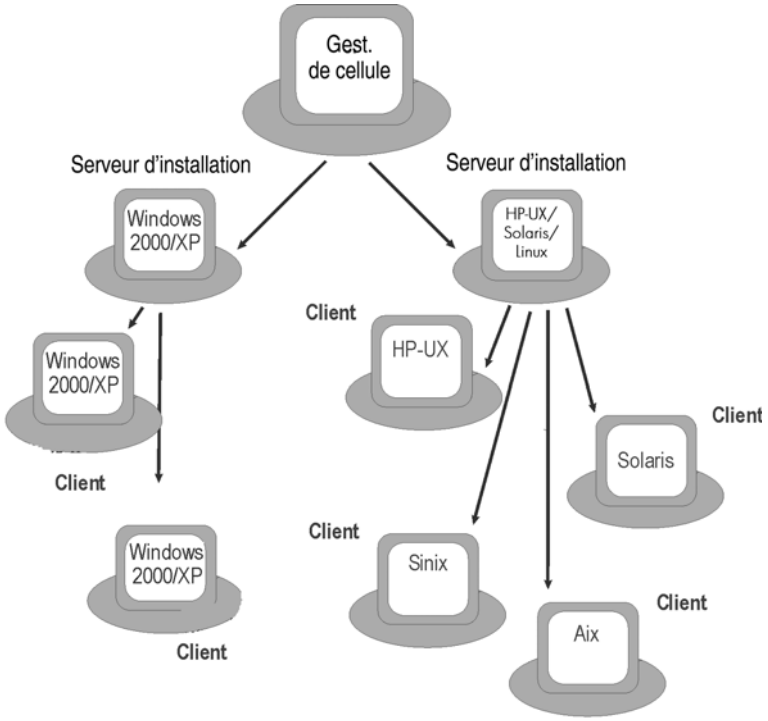

Figure 3 - Concept d'installation de Data Protector

DVD-ROM d'installation de Data Protector

Data Protector prend en charge différents systèmes d'exploitation sur plusieurs architectures de processeur. Par conséquent, deux DVD-ROM sont nécessaires pour couvrir toutes les plates-formes. Le Tableau 3 à la page 35 recense les composants qui figurent sur les DVD-ROM.

Tableau 3 - Liste des DVD-ROM Data Protector

N° de DVD	Titre du DVD-ROM	Sommaire
1	Pack Starter Data Protector pour Windows Comprend Media Operations et les agents pour les clients NetWare, MPE et HP OpenVMS	• Gestionnaire de cellule et Serveur d'installation pour Windows sur les systèmes 32 bits et 64 bits (AMD64/Intel EM64T) • AutoPass[1] • Tous les manuels en anglais au format PDF (dans le répertoire DOCS) • Clients Windows IA64 • Clients Novell NetWare • Clients OpenVMS (systèmes Alpha et IA64) • Clients MPE • Produit de démonstration pour plates-formes Windows • Informations sur le produit • Packages d'intégration logicielle HP • Package d'installation pour Media Operations
2	Pack Starter Data Protector pour HP-UX Comprend des agents pour les clients HP-UX, Solaris et Linux	• Gestionnaire de cellule et Serveur d'installation pour HP-UX (PA-RISC, IA64) • Clients pour d'autres systèmes UNIX • Tous les manuels en anglais au format PDF (dans le répertoire DOCS) • Packages d'intégration logicielle HP
3	Pack Starter Data Protector pour Solaris et Linux Comprend des agents pour les clients HP-UX, Solaris et Linux	• Gestionnaire de cellule et Serveur d'installation pour Solaris et Linux • Clients pour d'autres systèmes UNIX • AutoPass[2] • Tous les manuels en anglais au format PDF (dans le répertoire DOCS) • Packages d'intégration logicielle HP

[1]AutoPass n'est pas disponible sur les systèmes d'exploitation Windows 2003 x64, Windows Vista x64 et Windows Server 2008 x64.
[2]AutoPass n'est pas disponible sous Linux.

Choix du système Gestionnaire de cellule

Le Gestionnaire de cellule est le système le plus important de la cellule Data Protector. Le Gestionnaire de cellule effectue les tâches suivantes :

- gère la cellule à partir d'un seul point central ;
- contient la base de données IDB (fichiers contenant des informations sur les sessions de sauvegarde, de restauration et de gestion des supports) ;
- exécute le logiciel central Data Protector ;
- exécute le Gestionnaire de session qui démarre et arrête les sessions de sauvegarde et de restauration et inscrit les informations sur les sessions dans la base de données IDB.

Avant de décider sur quel système de votre environnement installer le Gestionnaire de cellule, il convient de connaître les éléments suivants :

- Plates-formes prises en charge
  Vous pouvez installer le Gestionnaire de cellule sur la plate-forme Windows, HP-UX, Solaris ou Linux. Pour connaître les versions des plates-formes prises en charge, reportez-vous au site http://www.hp.com/support/manuals.
- Fiabilité du système Gestionnaire de cellule
  Dans la mesure où le Gestionnaire de cellule contient la base de données IDB et où la sauvegarde et la restauration sont impossibles en cas de panne du Gestionnaire de cellule, il est important de choisir un système très fiable pour cette installation.
- Croissance de la base de données et et espace disque requis
  Le Gestionnaire de cellule contient la base de données interne (IDB) de Data Protector. Celle-ci comprend des informations sur les données sauvegardées et les supports correspondants, sur les messages de session et les périphériques.En fonction de votre environnement, la base peut atteindre une taille significative. Par exemple, si la majorité des sauvegardes concerne des systèmes de fichiers, la base IDB représenterait généralement 2 % de l'espace disque occupé par les données sauvegardées. Vous pouvez utiliser le tableau `IDB_capacity_planning.xls` (présent sur le support d'installation de Data Protector) afin d'estimer la taille de la base de données IDB.
  Reportez-vous à *l'index de l'aide en ligne (rubrique "croissance et performances de l'IDB")* pour plus d'informations sur la planification et la gestion de la taille et de la croissance de la base de données.
  Reportez-vous au document *Références, notes de publication et annonces produits HP Data Protector* pour connaître l'espace disque minimal requis pour la base IDB.

REMARQUE :

Vous n'êtes pas obligé d'utiliser le Gestionnaire de cellule comme système de l'interface graphique utilisateur. Vous pouvez par exemple disposer d'un Gestionnaire de cellule UNIX, mais d'un composant Interface utilisateur installé sur un client Windows.

Etape suivante

Pour connaître la configuration minimale requise de votre futur système Gestionnaire de cellule, reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 42.

Choix du système de l'interface utilisateur de Data Protector

Data Protector fournit une interface graphique utilisateur et une interface de ligne de commande (CLI) pour les plates-formes Windows, HP-UX, Solaris et Linux. L'interface utilisateur est installée en tant que composant logiciel Data Protector.

Le système sélectionné pour contrôler la cellule sera utilisé par un administrateur réseau ou un opérateur de sauvegarde.

Toutefois, dans un environnement informatique très important, il peut être préférable d'exécuter l'interface utilisateur sur plusieurs systèmes ; dans le cas d'un environnement mixte, il est conseillé de l'installer sur plusieurs plates-formes.

Par exemple, si vous disposez d'un réseau UNIX mixte et que l'interface utilisateur est installée sur au moins un système Solaris ou HP-UX, vous pouvez exporter l'affichage de cette interface utilisateur vers tout autre système UNIX exécutant un serveur X. Cependant, pour maintenir un bon niveau de performances, il est recommandé d'installer l'interface graphique de Data Protector sur tous les systèmes utilisés pour contrôler la cellule Data Protector.

Si vous travaillez dans un bureau très vaste où de nombreux systèmes Windows doivent être sauvegardés, il peut être plus pratique de contrôler les opérations locales de sauvegarde et de restauration à partir d'un système Windows local. Dans ce cas, installez le composant Interface utilisateur sur un système Windows. Par ailleurs, l'interface graphique utilisateur de Data Protector sur les systèmes Windows est plus simple à gérer dans les environnements hétérogènes, car il n'est pas nécessaire de modifier les paramètres régionaux.

Sur les plates-formes du Gestionnaire de cellule UNIX, vous pouvez utiliser l'interface utilisateur graphique Java de Data Protector lorsqu'elle est prise en charge ou la commande `omniusers` pour créer un compte utilisateur distant sur le Gestionnaire de cellule. Vous pouvez alors utiliser ce compte utilisateur pour démarrer l'interface graphique utilisateur de Data Protector et vous connecter au Gestionnaire de cellule ou à n'importe quel autre système sur lequel l'interface graphique de Data Protector a été installée. Pour plus de détails, reportez-vous à la page `omniusers` du manuel.

Pour connaître les versions des systèmes d'exploitation prises en charge pour l'interface utilisateur, reportez-vous au site http://www.hp.com/support/manuals. Pour plus d'informations sur la prise en charge des différentes langues et l'utilisation de caractères non-ASCII dans les noms de fichier, recherchez dans l'index de l'aide en ligne : "paramètres de langue, personnalisation".

Une fois l'interface utilisateur installée sur un système de la cellule, vous pouvez accéder à distance au Gestionnaire de cellule à partir de ce système. Vous n'êtes pas obligé d'utiliser l'interface graphique utilisateur sur le Gestionnaire de cellule.

Interface graphique utilisateur de Data Protector

L'interface graphique utilisateur de Data Protector est un outil puissant qui permet d'accéder facilement aux fonctions de Data Protector. La fenêtre principale contient plusieurs vues, telles que Clients, Utilisateurs, Périphériques et supports, Sauvegarde, Restauration, Copie et consolidation, Rapports, Moniteur, Restauration instantanée et Base de données interne, lesquelles vous permettent d'exécuter toutes les tâches associées.

Par exemple, la vue Clients vous permet d'installer les clients à distance en précisant tous les systèmes cible et en définissant les chemins et les options d'installation envoyés au système du Serveur d'installation spécifié. Lorsque l'installation du système client est en cours, seuls les messages spécifiques à l'installation s'affichent dans la fenêtre du moniteur.

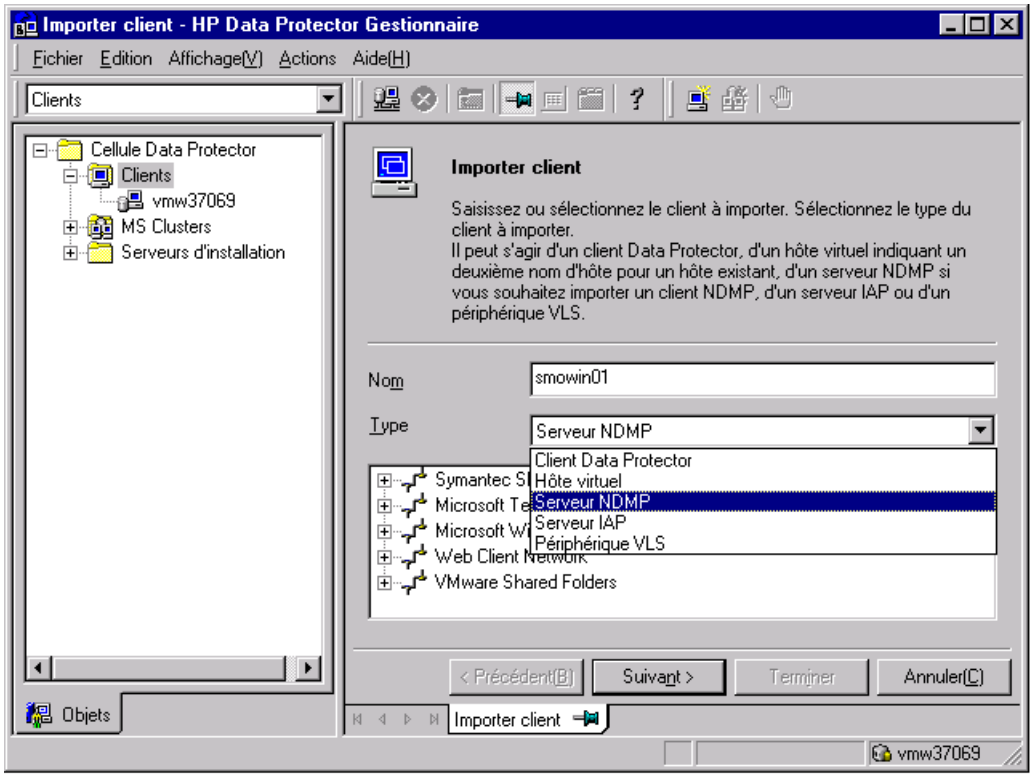

Figure 4 - Interface graphique utilisateur de Data Protector

Reportez-vous également à la Figure 1 à la page 27 de la préface, qui définit les principales zones de l'interface utilisateur de Data Protector.

REMARQUE :

Sur les systèmes UNIX, avant de lancer l'interface utilisateur graphique de Data Protector, il faut définir des paramètres régionaux sur le système sur lequel elle s'exécute. Cela vous permettra de changer l'encodage de caractères dans l'interface graphique et de choisir celui adapté pour afficher correctement les caractères non-ASCII dans les noms de fichiers et les messages de session. Reportez-vous à l'index de l'aide en ligne "paramétrage, paramètre régional pour l'interface graphique utilisateur sous UNIX" pour plus d'informations.

2 Installation de Data Protector sur votre réseau

Description du chapitre

Ce chapitre contient des instructions détaillées sur les opérations suivantes :

- Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 42.
- Installation des clients Data Protector. Reportez-vous à la section "Installation des clients Data Protector" à la page 70.
- Installation des clients d'intégration Data Protector. Reportez-vous à la section "Installation des clients d'intégration Data Protector" à la page 145.
- Installation de l'interface utilisateur Data Protector localisée. Reportez-vous à la section "Installation de l'interface utilisateur localisée de Data Protector" à la page 180.
- Installation de l'Edition serveur unique Data Protector. Reportez-vous à la section "Installation de l'Edition serveur unique de Data Protector" à la page 184.
- Installation du composant Rapports Web Data Protector. Reportez-vous à la section "Installation des Rapports Web de Data Protector" à la page 185.
- Installation de Data Protector sur MC/ServiceGuard. Reportez-vous à la section "Installation de Data Protector sur MC/ServiceGuard" à la page 186.
- Installation de Data Protector sur Microsoft Cluster Server. Reportez-vous à la section "Installation de Data Protector sur Microsoft Cluster Server" à la page 187.
- Installation de clients Data Protector sur un cluster Veritas. Reportez-vous à la section "Installation de clients Data Protector sur un cluster Veritas" à la page 200.
- Installation de clients Data Protector sur un cluster Novell NetWare. Reportez-vous à la section "Installation de clients Data Protector sur un cluster Novell NetWare" à la page 201.

Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector

Pour connaître le déroulement de la procédure d'installation, reportez-vous à la Figure 5 à la page 43 et à la :

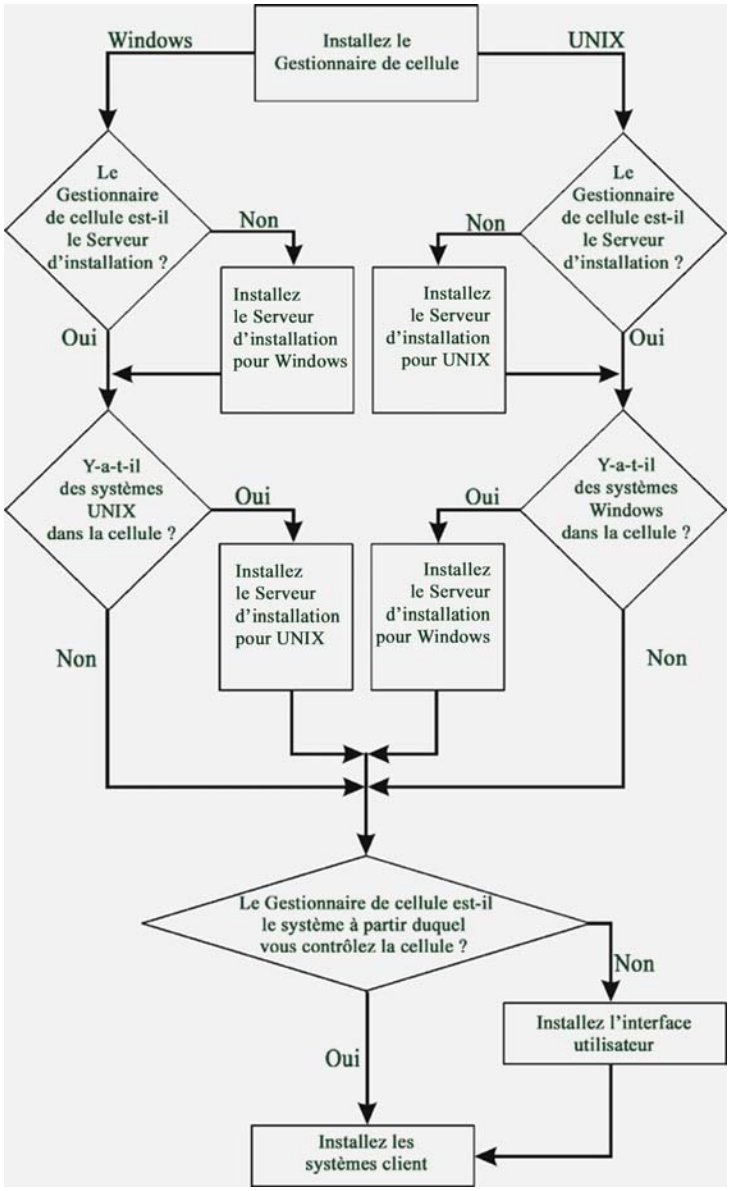

Figure 5 - Procédure d'installation

Si vous installez le Gestionnaire de cellule et le Serveur d'installation sur le même système, vous pouvez effectuer cette tâche en une seule étape.

IMPORTANT :

Tous les fichiers de configuration et d'informations sur les sessions d'une cellule Data Protector sont stockés dans le Gestionnaire de cellule. Il est difficile de transférer ensuite ces informations vers un autre système. Par conséquent, assurez-vous que le Gestionnaire de cellule est un système fiable installé dans un environnement stable et contrôlé.

Installation d'un Gestionnaire de cellule UNIX

Cette section fournit des instructions détaillées sur la procédure d'installation d'un Gestionnaire de cellule UNIX. Si vous souhaitez n'installer que le Gestionnaire de cellule Windows, reportez-vous à la section "Installation d'un Gestionnaire de cellule Windows" à la page 52.

Configuration système requise

- Le système HP-UX, Solaris ou Linux qui deviendra le Gestionnaire de cellule doit :
  - Disposer d'un espace disque suffisant pour le logiciel Data Protector. Pour plus d'informations à ce sujet, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*. Pour surmonter les problèmes de manque d'espace, vous pouvez effectuer l'installation sur des répertoires liés ; reportez-vous au préalable aux sections "Structure des répertoires installés sous HP-UX, Solaris et Linux" à la page 48 et "Allocation d'espace disque supplémentaire pour l'installation du Gestionnaire de cellule" à la page 52.
  - Disposer d'un espace disque suffisant (équivalent à environ 2 % des données à sauvegarder) pour la base de données IDB. Pour plus de détails à ce sujet, reportez-vous au document *Références, notes de publication et annonces produits HP Data Protector*. Notez que la conception actuelle de la base de données IDB permet de déplacer les fichiers binaires si la croissance de la base de données rend cette opération nécessaire. Dans l'index de l'aide en ligne, recherchez : "base de données interne (IDB), calcul de la taille".
  - Prendre en charge les noms de fichiers longs. Pour vérifier si votre système de fichiers prend en charge les noms de fichiers longs, utilisez la commande `getconf NAME_MAX` *`répertoire`*.
  - Disposer du démon `inetd`, lequel doit être opérationnel.
  - Disposer du port numéro 5555 (par défaut). Si ce n'estp as le cas, reportez-vous à la section "Modification du numéro de port par défaut de Data Protector" à la page 398.
  - Disposer du protocole TCP/IP, lequel doit être en cours d'exécution. Ce protocole doit pouvoir résoudre les noms d'hôte.
  - Avoir accès à un lecteur de DVD-ROM.

- Reconnaître le Gestionnaire de cellule, en cas d'utilisation d'un serveur NIS. Reportez-vous à la section "Préparation d'un serveur NIS" à la page 401.
- Pour installer le serveur d'interface utilisateur graphique Java, veillez à ce que le numéro de port 5556 soit libre.
- Pour le client d'interface utilisateur graphique Java, vous devez installer Java Runtime Environment (JRE) 1.5.0_06 ou toute version supérieure (version 1.5.0_07), par exemple.

- Vous devez disposer des droits `root` sur le système cible.

REMARQUE :

Sur les plates-formes Gestionnaire de cellule qui ne prennent pas en charge l'interface utilisateur graphique d'origine de Data Protector, vous pouvez utiliser l'interface utilisateur graphique Java de Data Protector ou installer l'interface utilisateur graphique d'origine de Data Protector sur un système qui la prend en charge. Utilisez la commande `omniusers` pour créer un compte utilisateur distant sur le nouveau Gestionnaire de cellule. Vous pouvez alors utiliser ce compte utilisateur avec l'interface graphique utilisateur de Data Protector installée pour lancer l'interface et vous connecter au nouveau Gestionnaire de cellule. Reportez-vous à la page `omniusers` du manuel.

Gestionnaire de cellule compatible cluster

D'autres conditions et étapes sont requises pour l'installation d'un Gestionnaire de cellule compatible cluster. Reportez-vous à la section "Installation d'un Gestionnaire de cellule compatible cluster" à la page 186.

REMARQUE :

Dans un environnement à plusieurs cellules (MoM), la même version de Data Protector doit être installée sur tous les Gestionnaires de cellule.

Recommandation

- *Sur des plates-formes UNIX*, il est recommandé d'utiliser la prise en charge des fichiers volumineux (LFS). Cette recommandation s'applique aux systèmes de fichiers qui contiennent une base de données interne, ainsi qu'aux fichiers binaires DC susceptibles d'occuper un volume supérieur à 2 Go.

Définition des paramètres de noyau

Sous HP-UX, il est recommandé de régler le paramètre de noyau `maxdsiz` (taille maximale des segments de données) ou `maxdsiz_64` (pour les systèmes 64 bits) sur au moins 134 217 728 octets (128 Mo), et le paramètre de noyau `semmnu` (nombre

de structures Undo de sémaphore) sur au moins 256 Mo. Une fois ces modifications effectuées, recompilez le noyau et redémarrez la machine.

Sous Solaris, il est recommandé de régler le paramètre de noyau `shmsys:shminfo_shmmax` (taille maximale des segments de la mémoire partagée (SHMMAX)) situé dans `/etc/system` sur au moins 67 108 864 octets (64 Mo). Une fois la modification effectuée, redémarrez la machine.

Procédure d'installation

CONSEIL :

Si vous installez le Gestionnaire de cellule et le Serveur d'installation sur le même système, vous pouvez exécuter l'installation en une opération en exécutant la commande `omnisetup.sh -CM -IS`.

Pour obtenir une description de la commande `omnisetup.sh`, consultez le fichier `LISEZMOI` se trouvant dans le répertoire *`point_de_montage`*`/LOCAL_INSTALL` sur le DVD-ROM ou le *Guide de rfrence de l'interface de ligne de commande HP Data Protector* se trouvant dans le répertoire *`point_de_montage`*`/DOCS/C/MAN` sur le DVD-ROM.

Suivez la procédure ci-dessous pour installer le Gestionnaire de cellule sur un système HP-UX, Solaris ou Linux :

1. Insérez et montez le DVD-ROM d'installation UNIX sur un point de montage.

   Par exemple :

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

   Vous pouvez installer Data Protector depuis un dépôt sur le disque :

   - Pour copier les répertoires `DP_DEPOT`, `AUTOPASS` et `LOCAL_INSTALL` où se trouvent les fichiers d'installation) sur votre disque local, exécutez la commande suivante :
     ```
     mkdir répertoire
     cp -r /dvdrom/rép_plateforme/DP_DEPOT répertoire
     cp -r /dvdrom/rép_plateforme/AUTOPASS répertoire
     cp -r /dvdrom/rép_plateforme/LOCAL_INSTALL répertoire
     ```
     Où *`rép_plateforme`* est :

`hpux_ia`	HP-UX sur systèmes IA-64
`hpux_pa`	HP-UX sur systèmes PA-RISC

`linux_x86_64`	Systèmes Linux avec AMD64/Intel EM64T
`solaris`	Systèmes Solaris

- Pour copier l'ensemble du DVD-ROM sur votre disque local, exécutez la commande :
  `cp -r /dvdrom`*`rép_image_dvd`*

2. Exécutez la commande `omnisetup.sh`.

Pour lancer cette commande à partir du DVD-ROM, entrez :

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

Pour lancer l'installation à partir du disque :

- Si vous avez copié les répertoires `DP_DEPOT`, `AUTOPASS` et `LOCAL_INSTALL` sur votre disque local dans le *`répertoire`*, exécutez :
  `cd` *`répertoire`*`/LOCAL_INSTALL`
  `./omnisetup.sh -source` *`répertoire`* `-CM`
- Si vous avez copié l'ensemble du DVD-ROM dans *`rép_mage_dvd`*, exécutez la commande `omnisetup.sh` avec le paramètre `-CM` :
  `cd` *`rép_image_ dvd`*`/LOCAL_INSTALL`
  `./omnisetup.sh -CM`

3. *Sous HP-UX et Solaris,* `omnisetup.sh` vous invite à installer ou à mettre à niveau l'utilitaire HP AutoPass si vous souhaitez télécharger et installer les mots de passe correspondant aux licences achetées directement par Internet à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus d'informations sur l'utilitaire AutoPass, reportez-vous à la section "Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP AutoPass" à la page 322 et à l'aide en ligne HP AutoPass. L'installation d'AutoPass est recommandée.

Si AutoPass est installé sous MC/ServiceGuard, il doit être installé sur tous les nœuds.

Lorsque vous y êtes invité, appuyez sur Entrée pour installer ou mettre à niveau AutoPass. Si vous ne souhaitez pas installer ou mettre à niveau AutoPass, entrez n.

Sous Linux, HP AutoPass n'est pas installé.

REMARQUE :

Si vous avez installé le Gestionnaire de cellule sous Solaris 9 ou 10, installez l'Agent de disque à distance sur le Gestionnaire de cellule après l'installation à l'aide d'un Serveur d'installation. L'Agent de disque générique Solaris sera ainsi remplacé par l'Agent de disque Solaris 9 ou Solaris 10. Sous Solaris 10, l'installation à distance de l'Agent de support sur le Gestionnaire de cellule s'avère également nécessaire. Reportez-vous à la section "Installation distante de clients Data Protector" à la page 78 ou à la page de manuel `ob2install`.

Si vous souhaitez installer un Serveur d'installation pour UNIX sur votre Gestionnaire de cellule, vous pouvez le faire à ce stade. Pour plus de détails sur les étapes requises, reportez-vous à la section "Installation des Serveurs d'installation pour UNIX" à la page 62.

Structure des répertoires installés sous HP-UX, Solaris et Linux

Au terme de l'installation, le logiciel central Data Protector réside dans le répertoire `/opt/omni/bin`, et le Serveur d'installation pour UNIX, dans le répertoire `/opt/omni/databases/vendor`. Les sous-répertoires Data Protector et les éléments qu'ils contiennent sont énumérés dans la liste ci-dessous :

IMPORTANT :

Si vous souhaitez installer Data Protector sur des répertoires liés, par exemple :

`/opt/omni/ -> /`*`préfixe`*`/opt/omni/`

`/var/opt/omni/ -> /`*`préfixe`*`/var/opt/omni/`

`/etc/opt/omni/ -> /`*`préfixe`*`/etc/opt/omni/`

Vous devez créer les liens avant l'installation et vous assurer que les répertoires cible existent.

Pour plus d'informations, reportez-vous à la section "Allocation d'espace disque supplémentaire pour l'installation du Gestionnaire de cellule" à la page 52.

`/opt/omni/bin`	Toutes les commandes
`/opt/omni/help/C`	Fichiers d'aide en ligne
`/opt/omni/lbin`	Commandes internes de Data Protector
`/opt/omni/sbin`	Commandes super-utilisateur

`/opt/omni/sbin/install`	Scripts d'installation
`/etc/opt/omni`	Informations de configuration
`/opt/omni/lib`	Bibliothèques partagées pour la compression, le codage de données et la gestion de périphériques
`/opt/omni/doc/C`	Documentation en ligne (facultatif)
`/var/opt/omni/log` et `/var/opt/omni/server/log`	Fichiers journaux
`/opt/omni/lib/nls/C`	Fichiers catalogue de messages
`/opt/omni/lib/man`	Pages de manuel
`/var/opt/omni/tmp`	Fichiers temporaires
`/var/opt/omni/server/db40`	Fichiers IDB. Dans l'index de l'aide en ligne, recherchez : "IDB, emplacement des répertoires".
`/opt/omni/java/server`	Répertoire contenant les fichiers exécutables du serveur d'interface utilisateur graphique Java
`/opt/omni/java/client`	Répertoire contenant les fichiers exécutables du client d'interface utilisateur graphique Java

Configuration du démarrage et de l'arrêt automatiques

La procédure d'installation de Data Protector consiste à configurer le démarrage et l'arrêt automatiques de tous les processus Data Protector à chaque redémarrage du système. Une partie de cette configuration dépend du système d'exploitation.

Les fichiers suivants sont configurés automatiquement :

HP-UX :

`/sbin/init.d/omni`

Script contenant les procédures de démarrage et d'arrêt.

`/sbin/rc1.d/K162omni`

Lien vers le script `/sbin/init.d/omni` qui permet d'arrêter Data Protector.

`/sbin/rc2.d/S838omni`

Lien vers le script `/sbin/init.d/omni` qui permet de démarrer Data Protector.

`/etc/rc.config.d/omni`

Contient une variable `omni` définissant :

`omni=1`	Data Protector est arrêté et démarré automatiquement au réamorçage du système. C'est l'option par défaut.
`omni=0`	Data Protector n'est pas arrêté et démarré automatiquement au réamorçage du système.

Solaris :

`/etc/init.d/omni`

Script contenant les procédures de démarrage et d'arrêt.

`/etc/rc1.d/K09omni`

Lien vers le script `/etc/init.d/omni` qui permet d'arrêter Data Protector.

`/etc/rc2.d/S97omni`

Lien vers le script `/etc/init.d/omni` qui permet de démarrer Data Protector.

Linux :

`/etc/init.d/omni`

Script contenant les procédures de démarrage et d'arrêt.

`/etc/rc`*`niveau_init`*`.d/K10omni`

Lien vers le script `/etc/init.d/omni` qui permet d'arrêter Data Protector. Où *`niveau_init`* est égal à 1 ou 6.

`/etc/rc`*`niveau_init`*`.d/S90omni`

Lien vers le script `/etc/init.d/omni` qui permet de démarrer Data Protector. Où *`niveau_init`* est égal à 2,3,4 ou 5.

Durant l'installation, les fichiers système suivants du Gestionnaire de cellule sont modifiés :

HP-UX :

`/etc/services`

Le numéro de port Data Protector du service est ajouté au fichier.

`/opt/omni/lbin/crs`

Le service CRS de Data Protector est ajouté.

Une fois l'installation terminée, les processus suivants sont exécutés sur le Gestionnaire de cellule :

`/opt/omni/lbin/crs`

Le service `Cell Request Server (CRS)` Data Protector s'exécute sur le système du Gestionnaire de cellule et est lancé lorsque le logiciel du Gestionnaire de cellule est installé sur le système. Il lance et contrôle les sessions de sauvegarde et de restauration dans la cellule.

`/opt/omni/lbin/rds`

Le service `Raima Database Server (RDS)` Data Protector s'exécute sur le système du Gestionnaire de cellule et est lancé lorsque le logiciel du Gestionnaire de cellule est installé sur le système. Le RDS gère la base de données IDB.

`/opt/omni/lbin/mmd`

Le service `Media Management Daemon (MMD)` Data Protector s'exécute sur le Gestionnaire de cellule et est lancé lorsque le logiciel du Gestionnaire de cellule est installé sur le système. Il gère les opérations de gestion des périphériques et des supports.

`/opt/omni/lbin/inetd`

Le service résident de Data Protector qui permet la communication avec les services Data Protector installés sur les autres systèmes du réseau. Le service Inet doit s'exécuter sur tous les systèmes de la cellule Data Protector.

`/opt/omni/lbin/kms`

Le service du `serveur gestionnaire de clés (KMS)` de Data Protector s'exécute sur le Gestionnaire de cellule et est lancé lorsque le logiciel du Gestionnaire de cellule est installé sur le système. Ce service gère les clés pour la fonction de cryptage de Data Protector.

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

Le serveur d'interface utilisateur graphique Java de Data Protector (le service `UIProxy`) s'exécute sur le Gestionnaire de cellule et est lancé lorsque le logiciel du Gestionnaire de cellule est installé sur le système. Le service `UIProxy` est chargé de la communication entre le client de l'interface Java et le Gestionnaire de cellule.

Configuration des variables d'environnement

La procédure d'installation du Gestionnaire de cellule UNIX décrite précédemment installe également l'interface utilisateur de Data Protector.

Avant d'utiliser l'interface utilisateur (l'interface graphique ou l'interface de ligne de commande), ajoutez les éléments suivants à vos variables d'environnement :

`/opt/omni/bin`, `/opt/omni/lbin` et `/opt/omni/sbin` à la variable `PATH`

`/opt/omni/lib/man` à la variable `MANPATH`

`/opt/omni/lib` et `/opt/omni/lib/arm` à la variable `LD_LIBRARY_PATH`

Avant de tenter d'utiliser l'interface graphique utilisateur, assurez-vous que la variable `DISPLAY` et les paramètres régionaux sont correctement définis.

REMARQUE :

Si vous avez l'intention d'utiliser l'interface utilisateur Data Protector pour effectuer des sauvegardes ou des restaurations sur plusieurs plates-formes, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector* pour connaître les limites en vigueur et à l'index de l'aide en ligne (rubrique "personnalisation des paramètres de langue") pour plus d'informations sur la personnalisation des paramètres de langue dans l'interface graphique de Data Protector.

Allocation d'espace disque supplémentaire pour l'installation du Gestionnaire de cellule

Vous devez disposer d'une grande quantité d'espace disque pour installer le Gestionnaire de cellule UNIX, en particulier pour le répertoire `/opt` et, par la suite, pour le répertoire `/var` où est stockée la base de données (environ 2 % des données de sauvegarde prévues). Pour plus d'informations sur l'espace disque requis, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*. Si l'espace disque est insuffisant, vous pouvez utiliser des répertoires liés, mais vous devez alors créer les liens avant l'installation et vous assurer que les répertoires cible existent.

Etape suivante

A ce stade, tout le Gestionnaire de cellule est installé et, en cas de sélection, le Serveur d'installation pour UNIX également. Tâches suivantes :

1. Si vous n'avez pas installé un Serveur d'installation pour UNIX sur le même système, reportez-vous à la section "Installation des Serveurs d'installation pour UNIX" à la page 62.
2. Installez un Serveur d'installation pour Windows, si vous souhaitez effectuer une installation à distance sur des clients Windows. Reportez-vous à la section "Installation d'un Serveur d'installation pour Windows" à la page 65.
3. Distribuez le logiciel aux clients. Reportez-vous à la section "Installation des clients Data Protector" à la page 70.

Installation d'un Gestionnaire de cellule Windows

Configuration système requise

Pour installer un Gestionnaire de cellule Windows, vous devez avoir les droits de l'`Administrateur`. Le système Windows qui deviendra votre Gestionnaire de cellule doit répondre aux critères suivants :

- Etre doté d'une version du système d'exploitation Windows prise en charge. Reportez-vous au site http://www.hp.com/support/manuals pour connaître les systèmes d'exploitation pris en charge pour le Gestionnaire de cellule.
- Disposer de Microsoft Internet Explorer 5.0 ou supérieur.
- Disposer d'un espace disque suffisant pour le logiciel Gestionnaire de cellule de Data Protector. Pour plus d'informations à ce sujet, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- Disposer d'un espace disque suffisant (équivalent à environ 2 % des données sauvegardées) pour la base de données IDB. Pour plus d'informations, consultez les *Références, notes de publication et annonces produits HP Data Protector*.
- Disposer du port numéro 5555 (par défaut). Si ce n'est pas le cas, reportez-vous à la section "Modification du numéro de port par défaut de Data Protector" à la page 398.
- Disposer d'une adresse IP fixe pour le système sur lequel le Gestionnaire de cellule doit être installé. Si le système est configuré en tant que client DHCP, son adresse IP change ; il est donc nécessaire soit d'attribuer une entrée DNS permanente au système (et de le reconfigurer), soit de configurer un serveur DHCP afin de réserver une adresse IP fixe pour le système (l'adresse IP est liée à l'adresse MAC du système).
- Disposer de l'implémentation Microsoft du protocole TCP/IP, lequel doit être installé et en cours d'exécution. Ce protocole doit pouvoir résoudre les noms d'hôte. Les noms de l'ordinateur et de l'hôte doivent être identiques. Reportez-vous à la section "Paramétrage du protocole TCP/IP sur les systèmes Windows" à la page 391 pour obtenir des informations sur l'installation et la configuration du protocole TCP/IP.
- Avoir accès à un lecteur de DVD-ROM.
- Pour installer le serveur d'interface utilisateur graphique Java, veillez à ce que le numéro de port 5556 soit libre.
- Pour le client d'interface utilisateur graphique Java, vous devez installer Java Runtime Environment (JRE) 1.5.0_06 ou toute version supérieure (version 1.5.0_07), par exemple.
- Vérifiez que les droits d'accès au réseau sont définis sous la règle de sécurité locale Windows pour le compte qui procède à l'installation.

Client Microsoft Terminal Services

- Si vous souhaitez installer Data Protector sous Windows via Microsoft Terminal Services Client, le Mode Terminal Server du système où vous installez Data Protector doit être défini sur Administration distante :
  1. Dans le Panneau de configuration de Windows, cliquez sur Outils d'administration, puis sur Configuration des services Terminal Server.
  2. Dans la boîte de dialogue Configuration Terminal Server, cliquez sur Paramètres du serveur. Vérifiez que le serveur Terminal Services s'exécute dans le mode Administration distante.

Recommandation

- Vérifiez si vous avez Microsoft Installer (MSI) 2.0 avant d'installer Data Protector A.06.10. Si vous possédez une version plus ancienne de MSI, le programme d'installation de Data Protector va automatiquement le mettre à niveau avec la version 2.0. Dans ce cas, Data Protector affichera une remarque à la fin de l'installation, indiquant que MSI a été mis à niveau. Si MSI a été mis à niveau, il est vivement recommandé de redémarrer le système.
  Il est recommandé de mettre MSI à niveau vers la version 2.0 avant d'installer Data Protector A.06.10.
- Si vous pensez que des fichiers binaires DC vont occuper un volume supérieur à 2 Go (leur taille limite est définie uniquement par les paramètres des systèmes de fichiers), il est recommandé d'utiliser le système de fichiers NTFS.

Gestionnaire de cellule compatible cluster

D'autres conditions et étapes sont requises pour l'installation d'un Gestionnaire de cellule compatible cluster. Reportez-vous à la section "Installation d'un Gestionnaire de cellule compatible cluster" à la page 188.

Procédure d'installation

Procédez comme suit pour effectuer une nouvelle installation sur un système Windows :

1. Insérez le DVD-ROM d'installation Windows.

   Sous Windows Server 2008, la fenêtre Contrôle du compte utilisateur s'affiche. Cliquez sur Continuer pour poursuivre l'installation.

2. Dans la fenêtre HP Data Protector, cliquez sur Installer Data Protector pour lancer l'assistant d'installation Data Protector.

3. Suivez les instructions de l'assistant et lisez attentivement le contrat de licence. Si vous en acceptez les termes, cliquez sur Suivant pour continuer.

4. Dans la page Type d'installation, sélectionnez Gestionnaire de cellule, puis cliquez sur Suivant pour installer le Gestionnaire de cellule Data Protector.

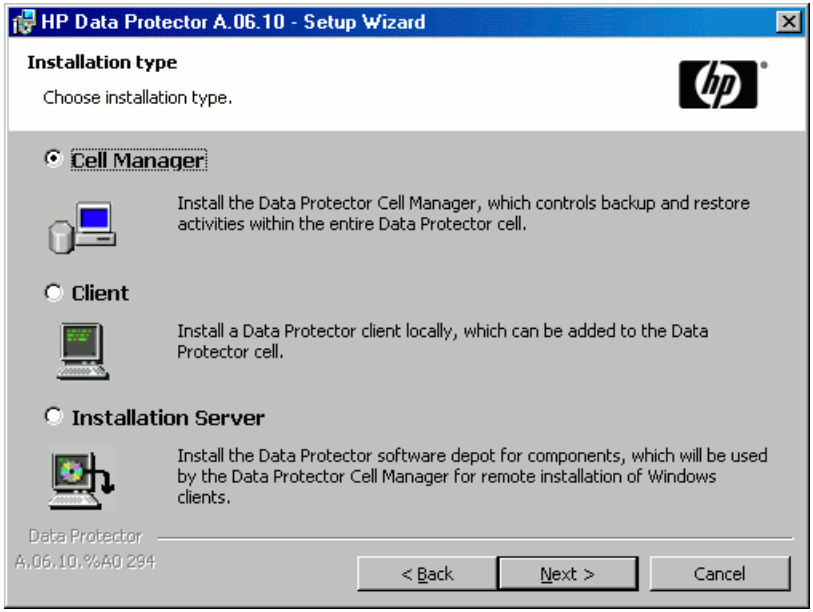

Figure 6 - Sélection du type d'installation

5. Indiquez le nom de l'utilisateur et le mot de passe du compte sur lequel les services Data Protector s'exécuteront. Cliquez sur Suivant pour continuer.

6. Cliquez sur Suivant pour installer Data Protector dans le répertoire par défaut.

   Sinon, cliquez sur Modifier pour ouvrir la fenêtre Modifier le dossier de destination actuel et entrez un autre chemin.

7. Dans la page Sélection des composants, sélectionnez les composants à installer. Pour obtenir la liste et les descriptions des composants Data Protector, reportez-vous à la section "Composants Data Protector" à la page 73.

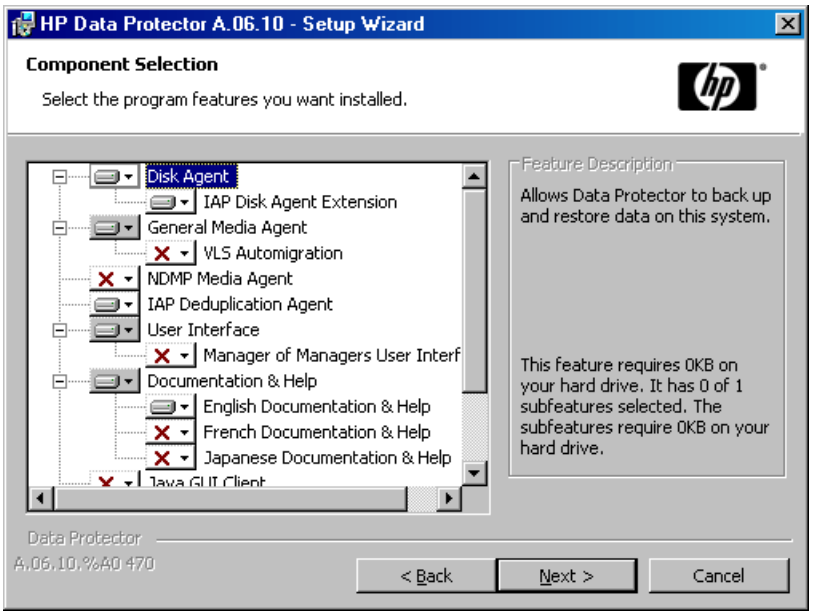

Figure 7 - Sélection des composants logiciels

Les composants Agent de disque, Agent général de support, Interface utilisateur et Serveur d'installation sont sélectionnés par défaut. Cliquez sur Suivant.

8. *Windows XP SP1, Windows Server 2003 SP1 et Windows Server 2008 :* si Data Protector détecte le pare-feu Windows sur votre système, la page Configuration du pare-feu Windows est affichée. Data Protector enregistrera tous les exécutables Data Protector nécessaires. Par défaut, l'option Permettre initialement aux nouveaux fichiers binaires Data Protector enregistrés d'ouvrir des ports le cas échéant est sélectionnée. Si vous ne souhaitez pas activer Data Protector pour les ports ouverts, désélectionnez l'option. Toutefois, notez que les exécutables doivent être activés pour que Data Protector fonctionne correctement.

   Cliquez sur Suivant.

9. La liste des composants sélectionnés s'affiche. Cliquez sur Installer pour démarrer l'installation des composants sélectionnés. L'installation peut durer plusieurs minutes.

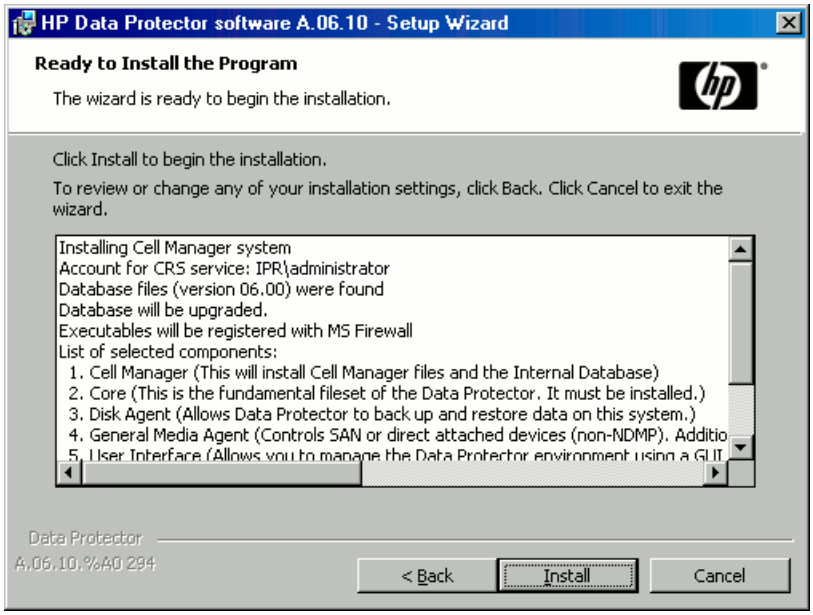

Figure 8 - Liste des composants sélectionnés

10. La page d'état de l'installation s'affiche. Cliquez sur Suivant.

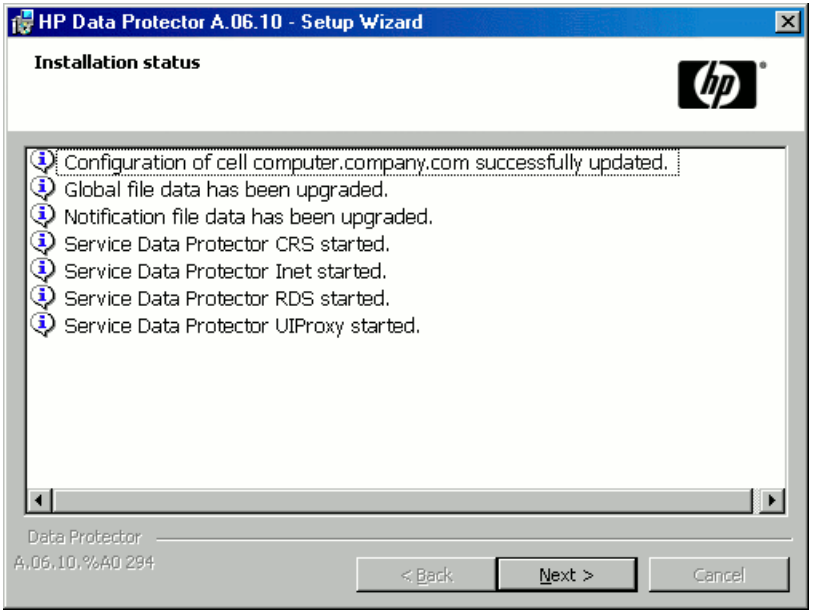

Figure 9 - Page d'état de l'installation

11. L'assistant d'installation vous permet d'installer ou de mettre à niveau l'utilitaire HP AutoPass si vous souhaitez télécharger et installer les mots de passe correspondant aux licences achetées directement via Internet à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus d'informations sur l'utilitaire AutoPass, reportez-vous à la section "Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP AutoPass" à la page 322 et à l'aide en ligne HP AutoPass.

Par défaut, l'option Start AutoPass installation (Démarrer l'installation d'AutoPass) ou Upgrade AutoPass installation (Mettre à niveau l'installation d'AutoPass) est sélectionnée. L'installation de l'utilitaire HP AutoPass est recommandée. Si vous ne souhaitez pas installer ou mettre à niveau AutoPass, désélectionnez cette option.

AutoPass n'est pas installé *sur les systèmes d'exploitation Windows 2000 et 2003 x64, Windows Vista x64 et Windows Server 2008 x64*.

Pour commencer à utiliser Data Protector immédiatement après son installation, sélectionnez Start the Data Protector Manager (Lancer l'interface graphique du gestionnaire Data Protector).

Pour consulter les *Références, notes de publication et annonces produits HP Data Protector*, sélectionnez Ouvrir les annonces sur les produits.

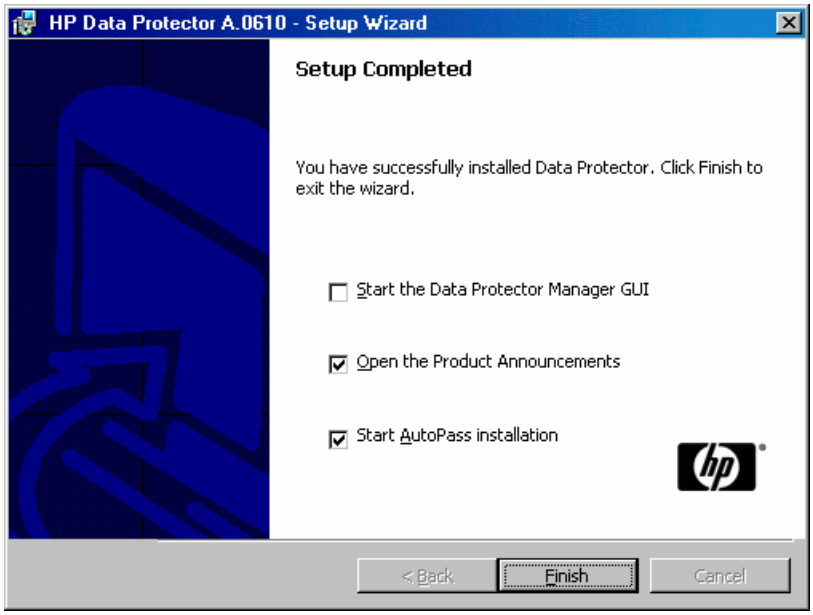

Figure 10 - Sélection d'AutoPass pour l'installation

Cliquez sur Terminer.

Après l'installation

Windows Server 2008 : dès la fin de l'installation, les fichiers de programme et de données du Gestionnaire de cellule se trouvent respectivement dans les répertoires *répertoire_Data_Protector* et *donnes_programme_Data_Protector*, et le dépôt de logiciel se trouve dans le répertoire *donnes_programme_Data_Protector*\Depot.

Autres systèmes Windows : dès la fin de l'installation, les fichiers du Gestionnaire de cellule se trouvent dans le répertoire *répertoire_Data_Protector* et le dépôt de logiciel se trouve dans le répertoire *répertoire_Data_Protector*\Depot.

Une fois l'installation terminée, les processus suivants sont exécutés sur le Gestionnaire de cellule :

crs.exe	Le service Cell Request Server (CRS) Data Protector s'exécute sur le système du Gestionnaire de cellule et est lancé lorsque le logiciel du Gestionnaire de cellule est installé sur le système. Il lance et contrôle les sessions de sauvegarde et de restauration dans la cellule. Il s'exécute dans le répertoire *répertoire_Data_Protector*\bin.

`rds.exe`	Le service Raima Database Server (RDS) Data Protector s'exécute sur le système du Gestionnaire de cellule et est lancé lorsque le logiciel du Gestionnaire de cellule est installé sur le système. Le RDS gère la base de données IDB. Il s'exécute dans le répertoire *`répertoire_Data_Protector`*`\bin`.
`mmd.exe`	Le service Media Management Daemon (MMD) de Data Protector s'exécute sur le système du Gestionnaire de cellule et est lancé lorsque le logiciel du Gestionnaire de cellule est installé sur le système. Il gère les opérations de gestion des périphériques et des supports. Il s'exécute dans le répertoire *`répertoire_Data_Protector`*`\bin`.
`omniinet.exe`	Le service du client Data Protector qui permet au Gestionnaire de cellule de démarrer des agents sur d'autres systèmes. Le service `Inet Data Protector` doit s'exécuter sur tous les systèmes de la cellule Data Protector. Il s'exécute dans le répertoire *`répertoire_Data_Protector`*`\bin`.
`kms.exe`	Le service du serveur gestionnaire de clés (KMS) de Data Protector s'exécute sur le système du Gestionnaire de cellule et est lancé lorsque le logiciel du Gestionnaire de cellule est installé sur le système. Ce service gère les clés pour la fonction de cryptage de Data Protector. Il s'exécute dans le répertoire *`répertoire_Data_Protector`*`\bin`.
`uiproxy.exe`	Le serveur d'interface utilisateur graphique Java de Data Protector (service `UIProxy`) s'exécute sur le système du Gestionnaire de cellule dans le répertoire *`répertoire_Data_Protector`*`\java\server\bin`. Le service `UIProxy` est chargé de la communication entre le client de l'interface Java et le Gestionnaire de cellule.

REMARQUE :

Si vous avez l'intention d'utiliser l'interface utilisateur Data Protector pour effectuer des sauvegardes ou des restaurations sur plusieurs plates-formes, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector* pour connaître les limites en vigueur.

CONSEIL :

Vous pouvez ajouter des tableaux de conversion de pages de codes supplémentaires pour pouvoir afficher correctement les noms de fichier, si l'encodage adéquat n'est pas disponible dans l'interface graphique Data Protector. Pour les instructions détaillées, reportez-vous à la documentation du système d'exploitation.

Dépannage

Si l'installation a échoué, contrôlez la configuration vérifiée par le `processus d'installation` lui-même, et essayez de déterminer les causes de l'échec si la configuration n'a pas été respectée. Reportez-vous à la section Configuration système requise à la page 52.

Les éléments vérifiés par le `processus d'installation` sont les suivants :

- Version du Service Pack
- NSLookup, qui permet à Data Protector de développer les noms d'hôte
- Espace disque
- Droits d'administration

Etape suivante

A ce stade, tout le Gestionnaire de cellule est installé et, en cas de sélection, le Serveur d'installation pour Windows également. Tâches suivantes :

1. Installez le Serveur d'installation pour UNIX, si votre environnement de sauvegarde est mixte. Reportez-vous à la section "Installation des Serveurs d'installation" à la page 61. Ne tenez pas compte de cette étape si vous n'avez pas besoin du Serveur d'installation pour UNIX.
2. Distribuez le logiciel aux clients. Reportez-vous à la section "Installation des clients Data Protector" à la page 70.

Installation des Serveurs d'installation

Les Serveurs d'installation peuvent être installés sur le système du Gestionnaire de cellule ou sur tout système pris en charge et connecté au Gestionnaire de cellule par un réseau

local. Reportez-vous au site http://www.hp.com/support/manuals pour connaître les systèmes d'exploitation pris en charge pour le Serveur d'installation.

Pour garder les Serveurs d'installation sur des systèmes séparés du Gestionnaire de cellule, installez en local le dépôt de logiciel correspondant. La procédure est décrite en détail dans cette section.

Installation des Serveurs d'installation pour UNIX

Configuration système requise

Le système qui deviendra votre Serveur d'installation doit répondre aux critères suivants :

- Disposer du système d'exploitation HP-UX, Solaris ou Linux. Pour obtenir des informations sur les systèmes d'exploitation pris en charge pour le Serveur d'installation, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- Disposer du démon `inetd`, lequel doit être opérationnel.
- Disposer du port numéro 5555 (par défaut). Si ce n'est pas le cas, reportez-vous à la section "Modification du numéro de port par défaut de Data Protector" à la page 398.
- Disposer du protocole TCP/IP, lequel doit être en cours d'exécution. Ce protocole doit pouvoir résoudre les noms d'hôte.
- Disposer d'un espace disque suffisant pour l'intégralité du dépôt de logiciel de Data Protector. Pour plus de détails à ce sujet, reportez-vous au document *Références, notes de publication et annonces produits HP Data Protector*.
- Etre équipé d'un lecteur de DVD-ROM.
- Le Gestionnaire de cellule de la cellule Data Protector doit être mis à niveau vers la version A.06.10.

IMPORTANT :

Pour installer Data Protector dans des répertoires liés, par exemple :

`/opt/omni/ -> /`*`préfixe`*`/opt/omni/`

`/etc/opt/omni/ -> /`*`préfixe`*`/etc/opt/omni/`

`/var/opt/omni/ -> /`*`préfixe`*`/var/opt/omni/`

Créez les liens avant l'installation et vous assurer que les répertoires cible existent.

REMARQUE :

Pour installer des logiciels à partir d'un périphérique via le réseau, vous devez d'abord monter le répertoire source sur votre ordinateur.

Procédure d'installation

Pour installer le Serveur d'installation pour UNIX sur un système HP-UX, Solaris ou Linux, procédez comme suit :

1. Insérez et montez le DVD-ROM d'installation UNIX sur un point de montage.

   Par exemple :

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

   Vous pouvez installer Data Protector depuis un dépôt sur le disque :

   - Pour copier les répertoires `DP_DEPOT`, `AUTOPASS` et `LOCAL_INSTALL` où se trouvent les fichiers d'installation) sur votre disque local, exécutez la commande suivante :
     `mkdir répertoire`
     `cp -r /dvdrom/rép_plateforme/DP_DEPOT répertoire`
     `cp -r /dvdrom/rép_plateforme/AUTOPASS répertoire`
     `cp -r /dvdrom/rép_plateforme/LOCAL_INSTALL répertoire`
     Où *rép_plateforme* est :

`hpux_ia`	HP-UX sur systèmes IA-64
`hpux_pa`	HP-UX sur systèmes PA-RISC
`linux_x86_64`	Systèmes Linux avec AMD64/Intel EM64T
`solaris`	Systèmes Solaris

   - Pour copier l'ensemble du DVD-ROM sur votre disque local, exécutez la commande :
     `cp -r /dvdrom rép_imagedvd`

2. Exécutez la commande `omnisetup.sh`.

   Pour lancer cette commande à partir du DVD-ROM, entrez :

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

   Pour lancer l'installation à partir du disque :

   - Si vous avez copié les répertoires `DP_DEPOT`, `AUTOPASS` et `LOCAL_INSTALL` sur votre disque local dans le *répertoire*, exécutez :
     ```
     cd répertoire/LOCAL_INSTALL
     ./omnisetup.sh -source répertoire -IS
     ```
   - Si vous avez copié l'ensemble du DVD-ROM dans *rép_image_dvd*, exécutez la commande `omnisetup.sh` avec le paramètre `-IS` :
     ```
     cd rép_image_ dvd/LOCAL_INSTALL
     ./omnisetup.sh -IS
     ```

   Pour obtenir une description de la commande `omnisetup.sh`, consultez le fichier `LISEZMOI` se trouvant dans le répertoire *point_de_montage/* sur le DVD-ROM ou le *Guide de rfrence de l'interface de ligne de commande HP Data Protector* se trouvant dans le répertoire *point_de_montage*/`DOCS/C/MAN` sur le DVD-ROM.

Au terme de l'installation, le dépôt de logiciel pour UNIX réside dans le répertoire `/opt/omni/databases/vendor`.

La commande `omnisetup.sh` installe le Serveur d'installation avec tous les packages. Pour installer certains packages uniquement, utilisez la commande `swinstall` (HP-UX), `pkgadd` (Solaris) ou `rpm` (Linux). Reportez-vous à la section "Installation sur des systèmes HP-UX, Solaris et Linux à l'aide d'outils natifs" à la page 373.

IMPORTANT :

Si vous n'installez pas le Serveur d'installation pour UNIX sur votre réseau, vous devrez installer chaque client UNIX en local à partir du DVD-ROM d'installation UNIX.

REMARQUE :

Si vous installez le composant Interface utilisateur (interface graphique utilisateur ou interface de ligne de commande), mettez à jour au préalable les variables d'environnement. Pour plus d'informations, reportez-vous à la section "Configuration des variables d'environnement" à la page 51.

Si vous avez l'intention d'utiliser l'interface utilisateur Data Protector pour effectuer des sauvegardes ou des restaurations sur plusieurs plates-formes, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector* pour connaître les limites en vigueur.

Etape suivante

A ce stade de la procédure, les serveurs d'installation pour UNIX doivent être installés sur votre réseau. Tâches suivantes :

1. Si vous avez installé le Serveur d'installation sur un système autre que celui du Gestionnaire de cellule, il faut ajouter (importer) manuellement le système dans la cellule Data Protector. Reportez-vous à la section "Importation d'un serveur d'installation dans une cellule" à la page 207.

   REMARQUE :

   Lorsqu'un Serveur d'installation est importé, le fichier `/etc/opt/omni/server/cell/installation_servers` sur le Gestionnaire de cellule est mis à jour avec les paquets push installés. Ce fichier peut être utilisé à partir de l'interface de ligne de commande pour vérifier les paquets push disponibles. Pour maintenir ce fichier à jour, vous devrez exporter, puis réimporter un Serveur d'installation à chaque installation ou suppression d'un paquet push. Cette procédure est valable même dans le cas où un Serveur d'installation est installé sur le même système que le Gestionnaire de cellule.

2. Installez le Serveur d'installation pour Windows si vous disposez de systèmes Windows dans votre cellule Data Protector. Reportez-vous à la section "Installation d'un Serveur d'installation pour Windows" à la page 65.
3. Distribuez le logiciel aux clients. Reportez-vous à la section "Installation des clients Data Protector" à la page 70.

Installation d'un Serveur d'installation pour Windows

Configuration système requise

Le système Windows qui deviendra votre Serveur d'installation doit répondre aux critères suivants :

- Disposer de l'une des versions du système d'exploitation Windows prises en charge. Reportez-vous au site http://www.hp.com/support/manuals pour connaître les systèmes d'exploitation pris en charge pour le Serveur d'installation.
- Disposer de Microsoft Internet Explorer 5.0 ou supérieur.
- Disposer d'un espace disque suffisant pour l'intégralité du dépôt de logiciel de Data Protector. Pour plus d'informations à ce sujet, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- Avoir accès à un lecteur de DVD-ROM.
- Disposer de l'implémentation Microsoft du protocole TCP/IP, lequel doit être en cours d'exécution. Ce protocole doit pouvoir résoudre les noms d'hôte. Les noms de l'ordinateur et de l'hôte doivent être identiques. Reportez-vous à

la section “Paramétrage du protocole TCP/IP sur les systèmes Windows” à la page 391 pour obtenir des informations sur l’installation et la configuration du protocole TCP/IP.

Limites

En raison des restrictions de sécurité imposées par le système d’exploitation Windows, le Serveur d’installation peut être utilisé pour installer des clients à distance uniquement dans le même domaine.

Recommandation

Avant de procéder à l’installation de Data Protector A.06.10, assurez-vous que vous disposez de Microsoft Installer (MSI) 2.0. Si vous possédez une version plus ancienne de MSI, le programme d’installation de Data Protector va automatiquement le mettre à niveau avec la version 2.0. Dans ce cas, Data Protector affichera une remarque à la fin de l’installation, indiquant que MSI a été mis à niveau. Si MSI a été mis à niveau, il est vivement recommandé de redémarrer le système. Consultez le support de Microsoft pour en savoir plus sur les prérequis de MSI 2.0 en fonction des différents systèmes d’exploitation Windows.

Il est recommandé de mettre MSI à niveau vers la version 2.0 avant d’installer Data Protector A.06.10.

IMPORTANT :

Si vous n’installez pas le Serveur d’installation pour Windows sur votre réseau, vous devrez installer chaque client Windows en local à partir du DVD-ROM.

REMARQUE :

Il est impossible d’installer à distance un client Data Protector sur le système Windows si un Serveur d’installation est déjà installé sur ce système. Pour installer un Serveur d’installation et un (des) composant(s) client sur le même système, vous devez procéder à une installation locale du client. Au cours de la procédure d’installation, sélectionnez tous les composants client de votre choix ainsi que le composant Serveur d’installation. Reportez-vous à la section “Installation de clients Windows” à la page 87.

Procédure d’installation

Procédez comme suit pour installer le Serveur d’installation pour Windows :

1. Insérez le DVD-ROM d’installation Windows.

   Sous Windows Server 2008, la fenêtre Contrôle du compte utilisateur s’affiche. Cliquez sur Continuer pour poursuivre l’installation.

2. Dans la fenêtre HP Data Protector, cliquez sur Installer Data Protector pour lancer l'assistant d'installation Data Protector.
3. Suivez les instructions de l'assistant et lisez attentivement le contrat de licence. Si vous en acceptez les termes, cliquez sur Suivant pour continuer.
4. Dans la page Type d'installation, sélectionnez Serveur d'installation, puis cliquez sur Suivant pour installer le dépôt de logiciel Data Protector.

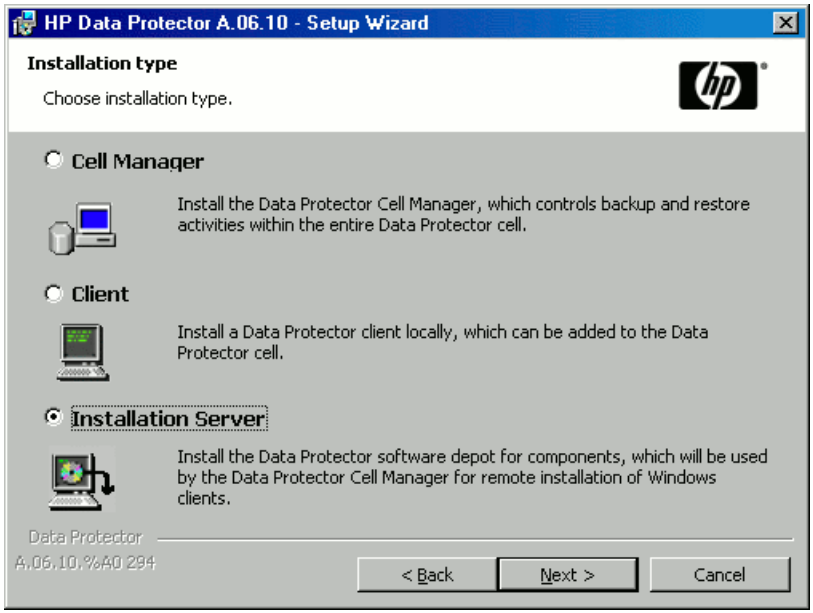

Figure 11 - Sélection du type d'installation

5. Cliquez sur Suivant pour installer Data Protector dans le répertoire par défaut.

   Sinon, cliquez sur Modifier pour ouvrir la fenêtre Modifier le dossier de destination actuel et entrez un autre chemin.
6. *Windows XP SP2, Windows Server 2003 SP1 et Windows Server 2008 :* si Data Protector détecte le pare-feu Windows sur votre système, la page Configuration du pare-feu Windows est affichée. Data Protector enregistrera tous les exécutables Data Protector nécessaires. Par défaut, l'option *Permettre initialement aux nouveaux fichiers binaires Data Protector enregistrés d'ouvrir des ports le cas échéant* est sélectionnée. Si vous ne souhaitez pas activer Data Protector pour les ports ouverts, désélectionnez l'option. Toutefois, notez que les exécutables doivent être activés pour que Data Protector fonctionne correctement.

   Cliquez sur Suivant.

7. La liste des composants sélectionnés s'affiche. Cliquez sur Installer pour démarrer l'installation des composants sélectionnés. L'installation peut durer plusieurs minutes.

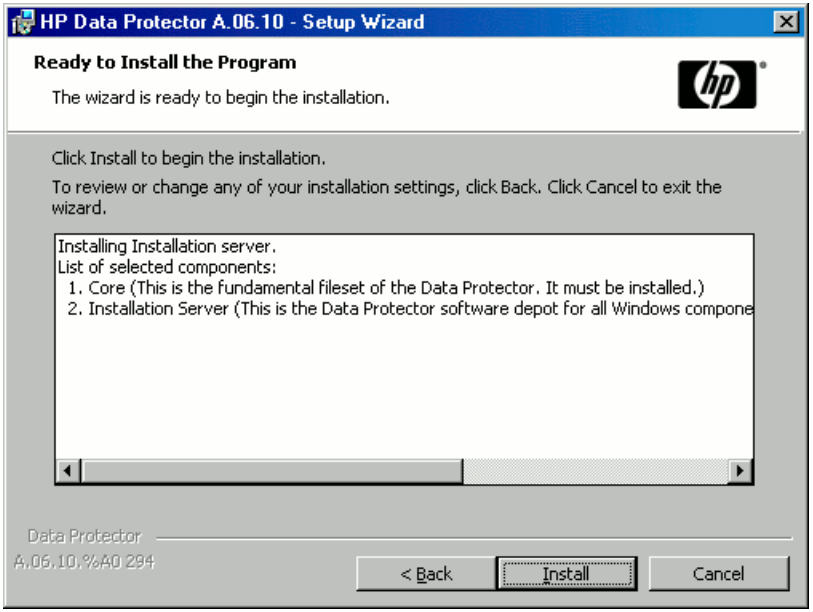

Figure 12 - Page de résumé des composants sélectionnés

8. La page d'état de l'installation s'affiche. Cliquez sur Suivant.

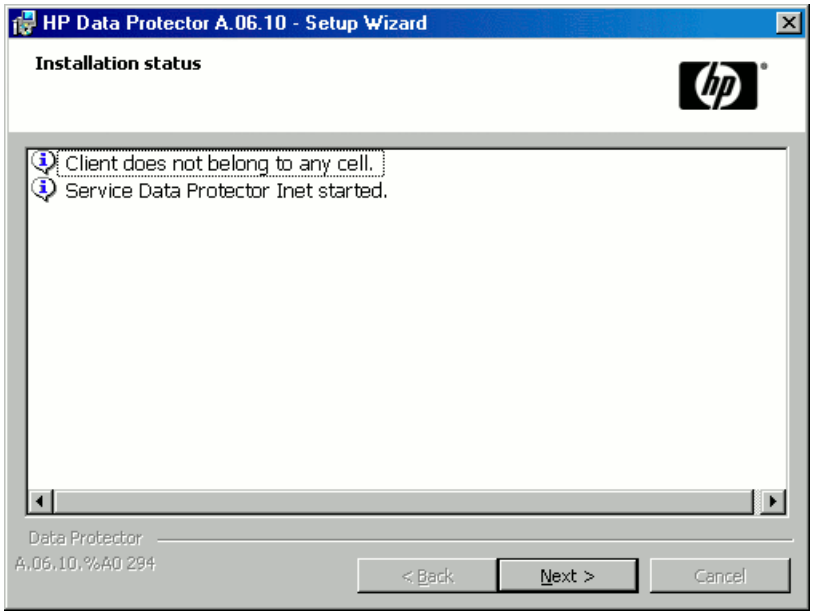

Figure 13 - Page d'état de l'installation

9. Pour consulter les *Références, notes de publication et annonces produits HP Data Protector*, sélectionnez Ouvrir les annonces sur les produits.

   Cliquez sur Terminer.

Dès que l'installation est terminée, le logiciel est placé par défaut dans le répertoire `donnes_programme_Data_Protector\Depot` (Windows Server 2008) ou dans le répertoire `répertoire_Data_Protector\Depot` (autres systèmes Windows). Le logiciel est partagé afin d'être accessible depuis le réseau.

Etape suivante

A ce stade de la procédure, le Serveur d'installation pour Windows doit être installé sur votre réseau. Vous devez maintenant effectuer les tâches suivantes :

1. Si vous avez configuré un Serveur d'installation indépendant (c'est-à-dire ne figurant pas dans le Gestionnaire de cellule), il faut ajouter (importer) manuellement le système dans la cellule Data Protector. Reportez-vous à la section "Importation d'un serveur d'installation dans une cellule" à la page 207.
2. Installez un Serveur d'installation pour UNIX sous HP-UX, Solaris ou Linux si votre environnement de sauvegarde est mixte. Reportez-vous à la section "Installation des Serveurs d'installation pour UNIX" à la page 62.
3. Distribuez le logiciel aux clients. Reportez-vous à la section "Installation des clients Data Protector" à la page 70.

Installation des clients Data Protector

Vous pouvez installer les clients Data Protector *à distance*, en les distribuant à l'aide du Serveur d'installation ou *localement*, à partir du DVD-ROM d'installation approprié.

Pour obtenir la liste des DVD-ROM d'installation Data Protector, reportez-vous à la section "DVD-ROM d'installation de Data Protector" à la page 34.

Une fois que vous avez installé les clients Data Protector et, le cas échéant, les avez importés dans la cellule Data Protector, il est fortement recommandé de vérifier l'installation et de protéger les clients contre tout accès non autorisé. Pour connaître la procédure de vérification de l'installation du client, reportez-vous à la section "Vérification de l'installation du client Data Protector" à la page 342. Pour plus d'informations sur la sécurité, reportez-vous à la section "Considérations sur la sécurité" à la page 214.

La section "Installation des clients Data Protector" à la page 70 répertorie les systèmes client Data Protector et contient des références permettant d'accéder à des descriptions détaillées.

Tableau 4 - Installation des systèmes client Data Protector

Système client	Type d'installation et référence
Windows	Installation à distance et en local ; voir la section "Installation de clients Windows" à la page 87.
HP-UX	Installation à distance et en local ; voir la section "Installation de clients HP-UX" à la page 94.
Solaris	Installation à distance et en local ; voir la section "Installation de clients Solaris" à la page 97.
Linux	Installation à distance et en local ; voir la section "Installation de clients Linux" à la page 103.
ESX Server	Installation à distance et en local ; voir la section "Installation des clients ESX Server" à la page 109.
AIX	Installation à distance et en local ; voir la section "Installation de clients AIX" à la page 110.
Tru64	Installation à distance et en local ; voir la section "Installation de clients Tru64" à la page 114.
Siemens Sinix	Installation à distance et en local ; voir la section "Installation de clients Siemens Sinix" à la page 112.
SCO	Installation à distance et en local ; voir la section "Installation de clients SCO" à la page 116.
Client DAS	Installation à distance et en local ; voir la section "Installation d'un Agent de support pour l'utilisation de la bibliothèque ADIC/GRAU ou de la bibliothèque StorageTek" à la page 118.
Client ACS	Installation à distance et en local ; voir la section "Installation d'un Agent de support pour l'utilisation de la bibliothèque ADIC/GRAU ou de la bibliothèque StorageTek" à la page 118.
Novell NetWare	Installation en local ; voir la section "Installation locale de clients Novell NetWare" à la page 126.
HP OpenVMS	Installation en local ; voir la section "Installation locale de clients HP OpenVMS" à la page 132.
MPE/iX	Installation en local ; voir la section "Installation de clients MPE/iX" à la page 139.
Autres clients UNIX	Installation en local ; voir la section "Installation locale de clients UNIX" à la page 142.

Intégrations ZDB

Data Protector Les intégrations ZDB sont des composants logiciels vous permettant de sauvegarder des applications de base de données avec Data Protector. Les systèmes

exécutant ces applications s'installent de la même manière que tout système client Windows ou UNIX, à condition d'avoir sélectionné le composant logiciel approprié (par exemple, le composant `Intégration MS Exchange` pour la sauvegarde de la base de données Microsoft Exchange Server, le composant `Intégration Oracle` pour la sauvegarde de la base de données Oracle, etc.). Pour connaître les références, reportez-vous au Tableau 5 à la page 72.

Tableau 5 - Installation d'intégrations

Application	Référence
Microsoft Exchange Server	Voir "Clients Microsoft Exchange Server" à la page 149.
Microsoft SQL Server	Voir "Clients Microsoft SQL Server" à la page 149.
Microsoft SharePoint Portal Server	Voir "Clients Microsoft SharePoint Portal Server" à la page 150.
Sybase	Voir "Clients Sybase" à la page 150.
Informix Server	Voir "Clients Informix Server" à la page 150.
SAP R/3	Voir "Clients SAP R/3" à la page 151.
SAP DB/MaxDB	Voir "Clients SAP DB/MaxDB" à la page 151.
Oracle	Voir "Clients Oracle" à la page 152.
VMware Virtual Infrastructure	Voir "Clients VMware Virtual Infrastructure" à la page 152.
IBM DB2 UDB	Voir "Clients DB2" à la page 153.
NNM	Voir "Clients NNM" à la page 153.
NDMP	Voir "Clients NDMP" à la page 153.
Microsoft Volume Shadow Copy Service	Voir "Clients Microsoft Volume Shadow Copy Service" à la page 153.
Lotus Domino Server	Voir "Clients Lotus Notes/Domino Server" à la page 154.
EMC Symmetrix	Voir "Intégration EMC Symmetrix" à la page 154.
HP StorageWorks Disk Array XP	Voir "Intégration HP StorageWorks Disk Array XP" à la page 159.
HP StorageWorks Virtual Array	Voir "Intégration HP StorageWorks Virtual Array" à la page 165.
HP StorageWorks Enterprise Virtual Array	Voir "Intégration HP StorageWorks Enterprise Virtual Array" à la page 171.

Tableau 6 - Autres installations

Installation	Référence
Integrated Archive Platform (IAP)	Voir "Clients IAP" à la page 178.
Auto-migration avec Virtual Library System (VLS)	Voir "Clients d'auto-migration VLS" à la page 179.
Interface utilisateur localisée	Voir "Installation de l'interface utilisateur localisée de Data Protector" à la page 180.
Rapports Web	Voir "Installation des Rapports Web de Data Protector" à la page 185.
MC/ServiceGuard	Voir "Installation de Data Protector sur MC/ServiceGuard" à la page 186.
Microsoft Cluster Server	Voir "Installation de Data Protector sur Microsoft Cluster Server" à la page 187.
Veritas Cluster Server	Voir "Installation de clients Data Protector sur un cluster Veritas" à la page 200.
Novell NetWare Cluster	Voir "Installation de clients Data Protector sur un cluster Novell NetWare" à la page 201.
IBM HACMP Cluster	Reportez-vous à la section "Installation de Data Protector sur un cluster IBM HACMP" à la page 203.

Composants Data Protector

Pour obtenir les toutes dernières informations sur les plates-formes prises en charge, consultez la page d'accueil du site Web de HP Data Protector à l'adresse http://www.hp.com/support/manuals.

Voici une description de chacun des composants Data Protector que vous pouvez sélectionner :

Interface utilisateur

Le composant Interface utilisateur comprend l'interface graphique utilisateur Data Protector sur les systèmes Windows et l'interface de ligne de commande sur les systèmes Windows et UNIX. Ce logiciel est nécessaire pour accéder au Gestionnaire de cellule Data Protector et doit être installé au moins sur le système utilisé pour gérer la cellule.

REMARQUE :

Si vous avez l'intention d'utiliser l'interface utilisateur Data Protector pour effectuer des sauvegardes ou des restaurations sur plusieurs plates-formes, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector* pour connaître les limites en vigueur.

Interface graphique utilisateur Java	L'interface graphique Java de Data Protector est une interface utilisateur Java à architecture client-serveur. Le client de l'interface graphique utilisateur Java ne sera pas sélectionné pour l'installation par défaut. Vous devez le sélectionner manuellement. Pour installer l'interface de ligne de commande sur un client disposant de l'interface graphique utilisateur Java, vous devez installer le package Interface utilisateur sur ce système.
Documentation et aide en anglais	Il s'agit de la documentation et de l'aide en ligne en anglais de Data Protector.
Documentation et aide en français	Il s'agit de la documentation et de l'aide en ligne en français de Data Protector.
Documentation et aide en japonais	Il s'agit de la documentation et de l'aide en ligne en japonais de Data Protector.
Interface utilisateur Manager-of-Managers (MoM)	L'interface utilisateur Manager-of-Managers (MoM) comprend l'interface graphique utilisateur Data Protector. Ce logiciel est nécessaire pour accéder aux fonctionnalités Manager-of-Managers de Data Protector et pour contrôler l'environnement multicellules. L'interface utilisateur Manager-of-Managers (MoM) et l'interface graphique utilisateur Manager sont disponibles en tant qu'application commune.
Agent de disque	Le composant Agent de disque doit être installé sur les systèmes disposant de disques qui doivent être sauvegardés avec Data Protector.

Extension de l'agent de disque IAP	L'extension d'agent de disque IAP doit être installé sur des systèmes qui effectuent des sauvegardes directement vers le système IAP en utilisant Data Protector.
Agent général de support	Le composant Agent général de support doit être installé sur les systèmes auxquels sont reliés des périphériques de sauvegarde ou qui disposent d'un accès au robot de bibliothèque et qui seront gérés avec Data Protector.
Auto-migration VLS	Le composant d'auto-migration de VLS doit être installé sur des clients qui réalisent des copies de supports intelligentes dans le système de bibliothèques virtuelles (VLS) en utilisant Data Protector.
Récupération après sinistre automatique	Le composant Récupération après sinistre automatique doit être installé sur les systèmes pour lesquels vous souhaitez activer la récupération à l'aide d'une méthode automatique de récupération après sinistre et sur le système sur lequel l'image CD ISO DR pour la récupération après sinistre avancée sera préparée, afin de fournir une préparation automatique en vue de la récupération après sinistre avancée.
Intégration SAP R/3	Le composant Intégration SAP R/3 doit être installé sur les systems that have an SAP R/3 database that will be backed up with Data Protector.
Intégration SAP DB	Le composant Intégration SAP DB doit être installé sur les systèmes disposant d'une base de données SAP DB/MaxDB qui sera sauvegardée avec Data Protector.
Intégration Oracle	Le composant Intégration Oracle doit être installé sur les systèmes disposant d'une base de données Oracle qui sera sauvegardée avec Data Protector.
Intégration VMware	Le composant Intégration VMware doit être installé sur les systèmes VirtualCenter (s'ils existent) et sur tous les systèmes ESX Server que vous envisagez de sauvegarder avec

	Data Protector. Si vous envisagez d'utiliser la méthode de sauvegarde VCBfile ou VCBimage, le composant d'intégration doit également être installé sur les systèmes de sauvegarde proxy.
Intégration DB2	Le composant Intégration DB2 doit être installé sur tous les systèmes disposant d'un serveur DB2 qui sera sauvegardé avec Data Protector.
Intégration Sybase	Le composant Intégration Sybase doit être installé sur les systèmes disposant d'une base de données Sybase qui sera sauvegardée avec Data Protector.
Intégration Informix	Le composant Intégration Informix doit être installé sur les systèmes disposant d'une base de données Informix Server qui sera sauvegardée avec Data Protector.
Intégration MS Exchange	Le composant Intégration MS Exchange doit être installé sur les systèmes disposant d'une base de données Microsoft Exchange Server qui sera sauvegardée avec Data Protector.
Intégration MS SQL	Le composant Intégration SQL doit être installé sur les systèmes où une base de données Microsoft SQL sera sauvegardée avec Data Protector.
Intégration MS SharePoint Portal Server	Le composant Intégration MS SharePoint Portal Server doit être installé sur les systèmes Microsoft SharePoint Portal Server qui seront sauvegardés avec Data Protector.
Intégration du service MS Volume Shadow Copy	Le composant Intégration du service MS Volume Shadow Copy doit être installé sur les systèmes Windows Server 2003 sur lesquels vous souhaitez exécuter des sauvegardes coordonnées par le service Volume Shadow Copy.
Agent EMC Symmetrix	Le composant Agent EMC Symmetrix doit être installé sur le système d'application et de sauvegarde pour intégrer EMC Symmetrix dans Data Protector.

Agent HP StorageWorks XP	Le composant Agent HP StorageWorks XP doit être installé sur le système d'application et de sauvegarde pour intégrer HP StorageWorks Disk Array XP dans Data Protector.
Agent HP StorageWorks VA	Le composant Agent HP StorageWorks VA doit être installé sur le système d'application et de sauvegarde pour intégrer HP StorageWorks Virtual Array XP dans Data Protector.
Agent HP StorageWorks EVA SMI-S	Le composant Agent HP StorageWorks EVA SMI-S doit être installé sur le système d'application et de sauvegarde pour intégrer HP StorageWorks Enterprise Virtual Array dans Data Protector.
Intégration de sauvegarde HP NNM	Le composant Intégration NNM doit être installé sur tous les systèmes de la cellule où réside la base de données NNM devant être sauvegardée avec Data Protector.
Agent de support NDMP	L'Agent de support NDMP doit être installé sur tous les systèmes qui sauvegardent des données vers des lecteurs dédiés NDMP via un serveur NDMP.
Agent de déduplication IAP	L'agent de déduplication IAP doit être installé sur des systèmes qui effectuent des sauvegardes directement vers le système IAP en utilisant Data Protector.
Intégration Lotus	Le composant Intégration Lotus doit être installé sur tous les systèmes de la cellule Data Protector où réside une base de données Lotus Notes/Domino Server qui sera sauvegardée avec Data Protector.

REMARQUE :

Vous ne pouvez pas installer l'Agent général de support et l'Agent de support NDMP sur le même système.

Installation distante de clients Data Protector

Cette section décrit la procédure à suivre pour distribuer le logiciel Data Protector aux clients à l'aide du Serveur d'installation (installation ou mise à niveau distante).

Configuration système requise

- Pour connaître les conditions préalables et les recommandations d'installation, reportez-vous à la section décrivant la procédure d'installation pour ce client particulier. Les références sont énumérées dans le Tableau 4 à la page 71 et le Tableau 5 à la page 72.
- Accédez au site http://www.hp.com/support/manuals et reportez-vous au document *Références, notes de publication et annonces produits HP Data Protector* pour plus d'informations sur les plates-formes et les composants Data Protector pris en charge, ainsi que sur l'espace disque nécessaire.
- A ce stade de la procédure, le Gestionnaire de cellule et le(s) Serveur(s) d'installation doivent être installés sur votre réseau.

REMARQUE :

Le Serveur d'installation pour Windows doit résider dans un répertoire partagé, de sorte qu'il soit visible sur l'ensemble du réseau.

Vous devez distribuer le logiciel aux clients à l'aide de l'interface utilisateur de Data Protector. L'installation de clients sur plusieurs plates-formes est prise en charge.

- Pour utiliser une installation via un shell sécurisé, installez et configurez OpenSSH sur le client et le Serveur d'installation. Si votre clé privée est cryptée, installez et configurez Keychain sur le Serveur d'installation. Reportez-vous à la section "Installation à distance via un shell sécurisé" à la page 84 pour de plus amples informations.

REMARQUE :

Vous ne pouvez pas distribuer le logiciel aux clients situés dans une autre cellule Data Protector. Toutefois, si vous disposez d'un Serveur d'installation indépendant, vous pouvez l'importer dans plusieurs cellules. Vous pouvez ensuite distribuer le logiciel au sein de différentes cellules à l'aide de l'interface graphique utilisateur connectée à chaque Gestionnaire de cellule à tour de rôle.

Ajout de clients à la cellule

Pour distribuer le logiciel Data Protector aux clients qui n'appartiennent pas encore à la cellule Data Protector, procédez comme suit :

1. Démarrez l'interface graphique utilisateur de Data Protector :
   - Interface graphique d'origine de Data Protector (sous Windows uniquement) :
     - Démarrer > Programmes > HP Data Protector > Gestionnaire Data Protector.
   - Interface graphique utilisateur Java de Data Protector :
     - Sous Windows : sélectionnez Démarrer > Programmes > HP Data Protector > Gestionnaire de l'interface Java Data Protector.
       Dans la boîte de dialogue Se connecter à un Gestionnaire de cellule, sélectionnez ou entrer le nom d'un Gestionnaire de cellule et cliquez sur `Connexion`.
     - Sous UNIX, exécutez :
       `/opt/omni/java/client/bin/javadpgui.sh`

   Reportez-vous à la section "Interface graphique utilisateur de Data Protector" à la page 38 et à l'aide en ligne pour plus de détails sur l'interface graphique utilisateur de Data Protector.
2. Dans le Gestionnaire Data Protector, affichez le contexte Clients.
3. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur Clients, puis cliquez sur Ajouter clients.
4. Si plusieurs Serveurs d'installation sont configurés, sélectionnez la plate-forme des clients à installer (UNIX ou Windows) et le Serveur d'installation à utiliser pour la procédure. Cliquez sur Suivant.
5. Entrez les noms des clients ou recherchez les clients (interface Windows uniquement) à installer comme l'illustrent la Figure 14 à la page 80 et la . Cliquez sur Suivant.

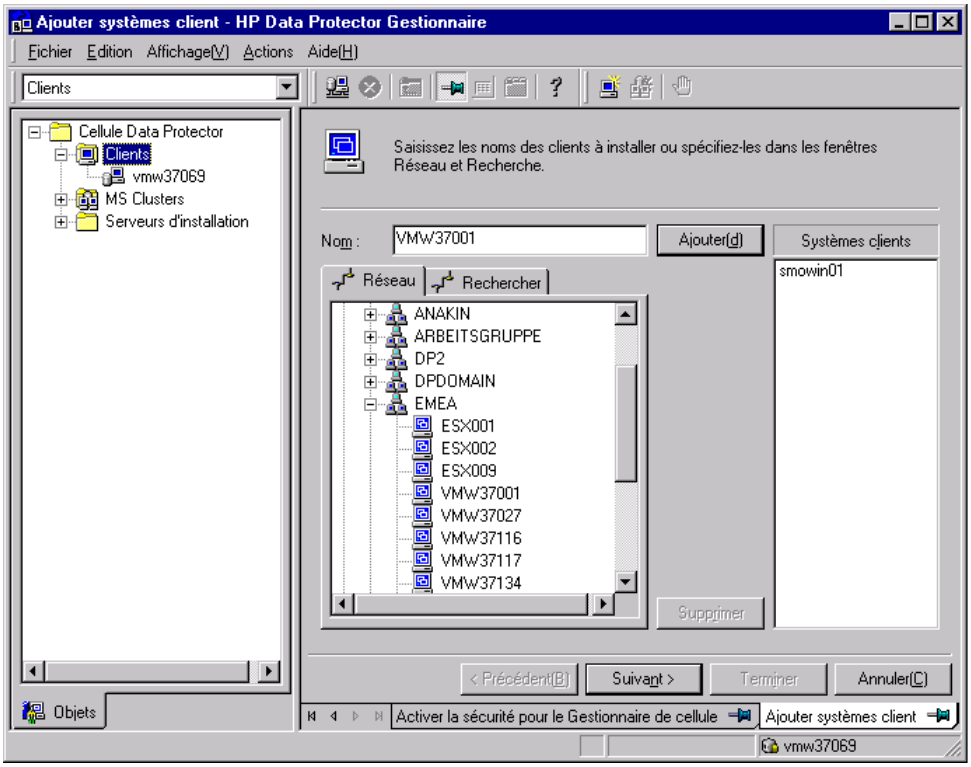

Figure 14 - Sélection de clients

6. Sélectionnez les composants Data Protector à installer comme l'illustre la Figure 15 à la page 81 et la . Notez que vous ne pouvez sélectionner qu'un type d'Agent de support. Reportez-vous à la section "Composants Data Protector" à la page 73.

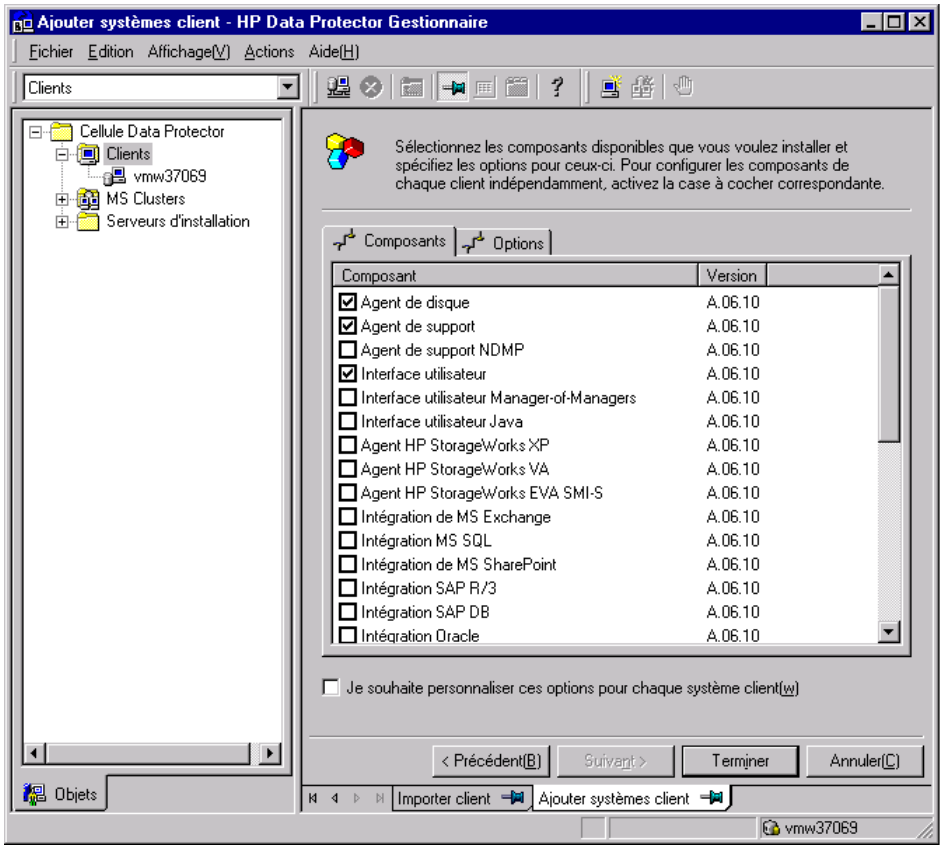

Figure 15 - Sélection de composants

Pour modifier le compte utilisateur et le répertoire cible par défaut (sous Windows uniquement) de l'installation, cliquez sur Options.

Si vous avez sélectionné plusieurs clients et que vous souhaitez installer des composants différents sur chacun d'eux, choisissez Je souhaite personnaliser cette option pour chaque système client séparément, puis cliquez sur Suivant. Sélectionnez les composants à installer pour chaque client séparément.

Cliquez sur Terminer pour démarrer l'installation.

7. Lors de l'installation, vous devez fournir les informations demandées (nom d'utilisateur, mot de passe, ainsi que le domaine sous Windows) afin d'accéder au système client spécifique ; cliquez ensuite sur OK.

Dès que le logiciel Data Protector est installé sur un système et que ce dernier est ajouté à la cellule Data Protector, il devient un client Data Protector.

REMARQUE :

Afin d'utiliser l'interface Data Protector sur le système client, ajoutez un utilisateur de ce système à un groupe d'utilisateurs Data Protector adéquat. Pour connaître la procédure à suivre et les droits utilisateur disponibles, reportez-vous à l'aide en ligne.

Dépannage

Dès que l'installation à distance est terminée, vous pouvez relancer les procédures d'installation qui ont échoué via l'interface en cliquant sur Actions et Redémarrer clients ayant échoué. Si l'installation échoue de nouveau, reportez-vous au Chapitre 6 à la page 333.

Ajout de composants aux clients

Vous pouvez installer d'autres composants logiciels de Data Protector sur les clients existants et le Gestionnaire de cellule. L'ajout des composants peut s'effectuer à distance ou en local. Pour une installation en local, reportez-vous à la section "Changement de composants logiciels Data Protector" à la page 242.

Clients MC/ServiceGuard

Dans l'environnement de cluster MC/ServiceGuard, vérifiez que le nœud auquel vous ajoutez les composants est actif.

Condition préalable

Le Serveur d'installation correspondant doit être disponible.

Pour distribuer le logiciel Data Protector aux clients de la cellule Data Protector, procédez comme suit :

1. Dans le `Gestionnaire` Data Protector, affichez le contexte Clients.
2. Dans la fenêtre de navigation, développez Clients, cliquez avec le bouton droit de la souris sur un client, puis cliquez sur Ajouter composants.
3. Si plusieurs Serveurs d'installation sont configurés, sélectionnez la plate-forme des clients sur lesquels installer les composants (UNIX ou Windows) et le Serveur d'installation à utiliser pour la procédure. Cliquez sur Suivant.
4. Sélectionnez les clients sur lesquels vous souhaitez installer les composants comme illustré sur la Figure 16 à la page 83 et la . Cliquez sur Suivant.

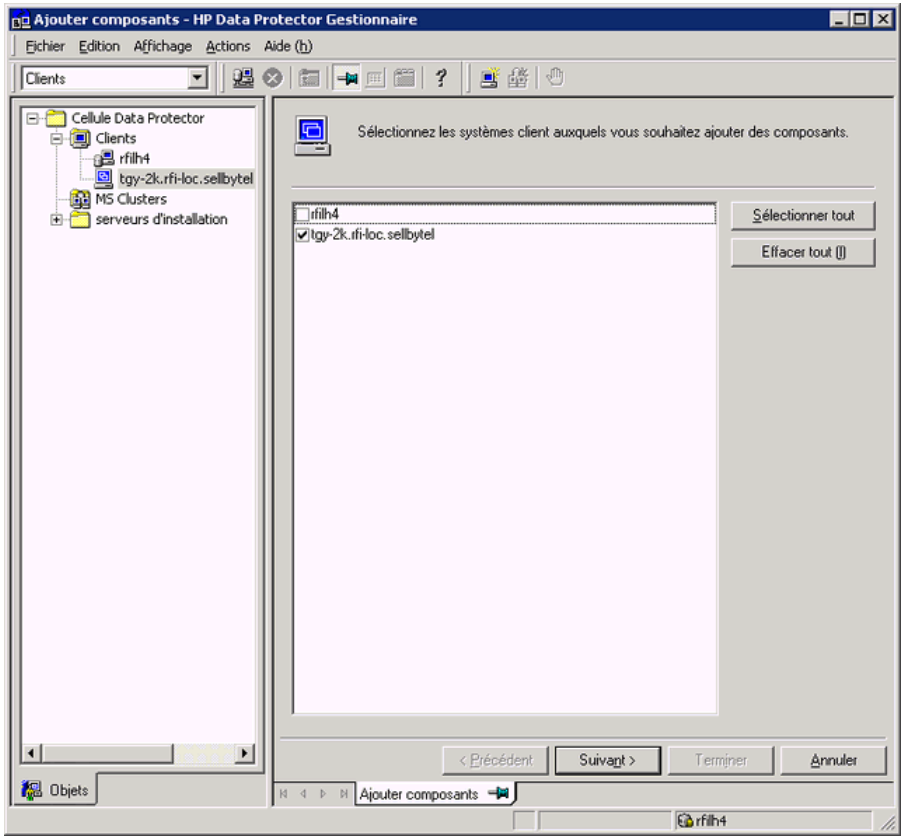

Figure 16 - Sélection de clients

5. Sélectionnez les composants Data Protector à installer comme l'illustre la Figure 17 à la page 84. Notez que vous ne pouvez sélectionner qu'un type d'Agent de support. Reportez-vous à la section "Composants Data Protector" à la page 73.

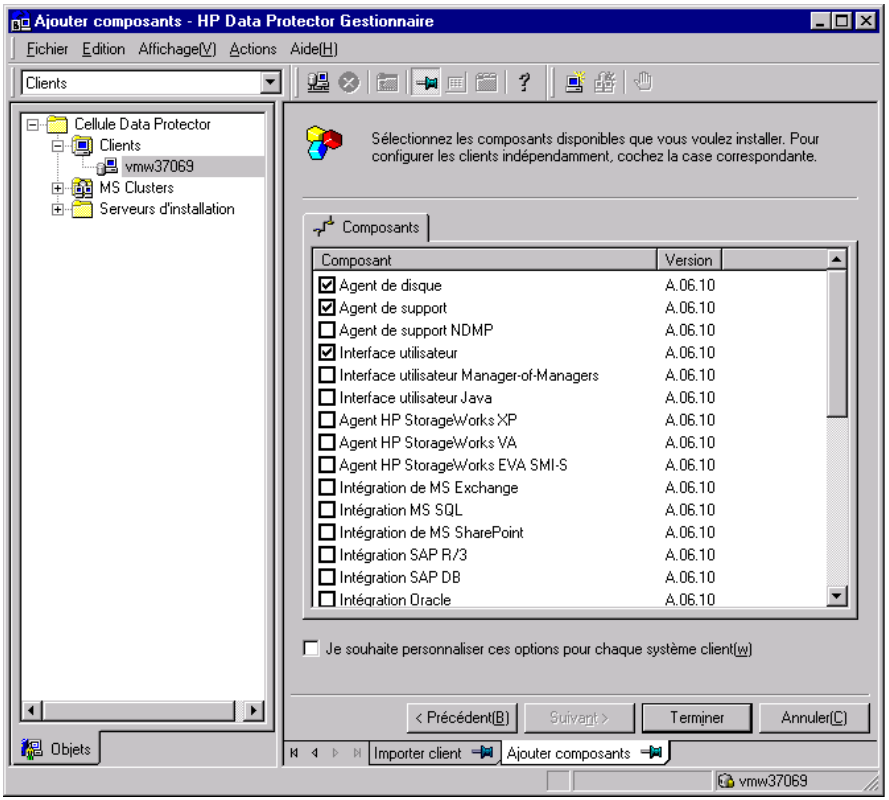

Figure 17 - Sélection de composants

Si vous avez sélectionné plusieurs clients et que vous souhaitez installer des composants différents sur chacun d'eux, choisissez Je souhaite personnaliser cette option pour chaque système client séparément, puis cliquez sur Suivant. Sélectionnez les composants pour chaque client individuellement.

Cliquez sur Terminer pour démarrer l'installation.

Installation à distance via un shell sécurisé

L'installation via un shell sécurisé permet de protéger le client et le Serveur d'installation en installant les composants Data Protector en toute sécurité. Un haut niveau de protection est obtenu comme suit :

- Authentification sécurisée de l'utilisateur Serveur d'installation sur le client grâce au mécanisme de paires de clés publiques-privées.
- Envoi de packages d'installation cryptés sur le réseau.

REMARQUE :

L'installation via un shell sécurisé est prise en charge sur les plates-formes UNIX seulement.

Pour utiliser une installation via un shell sécurisé, installez et configurez OpenSSH sur le client et le Serveur d'installation comme décrit ci-dessous.

Configuration de OpenSSH

OpenSSH est une mise en oeuvre libre du protocole de shell sécurisé. Pour configurer OpenSSH :

1. Si n'est pas déjà installé sur votre système, téléchargez-le à partir du site http://www.openssh.org, puis installez-le sur le client Data Protector et le Serveur d'installation. Sinon, sous HP-UX, vous pouvez utiliser le shell sécurisé HP-UX.

   REMARQUE :

   L'emplacement par défaut pour l'installation via un shell sécurisé est `/opt/ssh`.

2. Sur le Serveur d'installation, exécutez `ssh-keygen` pour générer une paire de clés publique-privée. Conservez la clé privée sur le Serveur d'installation et transférez la clé publique sur le client. Notez que si vous utilisez une clé privée cryptée (c'est-à-dire, protégée par une phrase passe), vous devez configurer Keychain sur le Serveur d'installation (voir la section Configuration de Keychain à la page 86 pour plus de détails).

   Pour des informations sur `ssh-keygen`, consultez le site http://www.openbsd.org/cgi-bin/man.cgi?query=ssh-keygen&sektion=1.

3. Stockez la clé publique dans le répertoire `$HOME/.ssh` du client sous le nom `authorized_keys`.

   REMARQUE :

   `$HOME/.ssh` est en général le répertoire de base de l'utilisateur `root`.

   Pour définir une version de protocole SSH (SSH1 ou SSH2), modifiez le paramètre `protocol` dans les fichiers suivants :

   1. *Sur le Serveur d'installation :*

      répertoire_installation_ssh`/ssh/etc/ssh_config`

      Ce fichier va être utilisé par la commande `ssh`.

   2. *Sur le client :*

répertoire_installation_ssh/ssh/etc/sshd_config

Ce fichier va être utilisé par le démon ssh (sshd).

Notez que ces deux fichiers doivent être synchronisés.

REMARQUE :

La version de protocole SSH par défaut est SSH2.

4. Sur le client, démarrez le démon ssh :

   répertoire_installation_ssh/ssh/sbin/sshd

5. Ajoutez le client à une liste des hôtes connus (elle se trouve dans $HOME/.ssh/known_hosts sur le Serveur d'installation) en exécutant la commande :

   ssh root@*hôte_client*

   Notez que *hôte_client* doit être le nom DNS complet, par exemple :

   ssh root@client1.société.com

6. Sur le Serveur d'installation, donnez à la variable omnirc OB2_SSH_ENABLED la valeur 1. Pour plus d'informations sur les variables omnirc, reportez-vous au *Guide de dépannage HP Data Protector*.

Configuration de Keychain

Keychain est un outil évitant d'avoir à fournir manuellement une phrase passe pour décrypter la clé privée. Il n'est nécessaire que si la clé privée est cryptée. Pour configurer Keychain :

1. Téléchargez Keychain à l'adresse http://www.gentoo.org/proj/en/keychain/index.xml vers le Serveur d'installation.

2. Ajoutez au fichier $HOME/.profile les deux lignes suivantes :

   HP-UX, Solaris :

   répertoire_installation_keychain/keychain-*version_keychain*/keychain $HOME/.ssh/*clé_privée*

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

   Linux :

   /usr/bin/keychain $HOME/.ssh/*clé_privée*

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

3. Sur le Serveur d'installation, donnez à la variable omnirc OB2_ENCRYPT_PVT_KEY la valeur 1. Pour plus d'informations sur les variables omnirc, reportez-vous au *Guide de dépannage HP Data Protector*.

Etape suivante

Après avoir configuré OpenSSH et Keychain, ajoutez des clients à la cellule à l'aide de l'interface graphique, comme décrit à la section Ajout de clients à la cellule à la page 78, ou à l'aide de l'interface de ligne de commande en exécutant la commande `ob2install`. Pour plus d'informations sur les commandes de l'interface de ligne de commande et leurs paramètres, reportez-vous au *Guide de rfrence de l'interface de ligne de commande HP Data Protector*.

REMARQUE :

S'il est impossible d'effectuer une installation via un shell sécurisé en raison de l'échec de l'exécution de sa commande, un message d'avertissement est émis. Toutefois, l'installation continue à l'aide de la méthode d'installation à distance standard de Data Protector.

Installation de clients Windows

Pour connaître les plates-formes et les composants pris en charge pour un système d'exploitation Windows donné, reportez-vous au site http://www.hp.com/support/manuals.

Configuration système requise

Pour installer un client Windows, vous devez avoir les droits de l'Administrateur. Le système Windows qui deviendra votre système client Data Protector doit répondre aux critères suivants :

- Disposer de Microsoft Internet Explorer 5.0 ou supérieur.
- Disposer d'un espace disque suffisant pour le logiciel client Data Protector. Pour plus d'informations à ce sujet, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- Disposer du port numéro 5555 (par défaut).
- Disposer de l'implémentation Microsoft du protocole TCP/IP, lequel doit être installé et en cours d'exécution. Ce protocole doit pouvoir résoudre les noms d'hôte. Les noms de l'ordinateur et de l'hôte doivent être identiques. Reportez-vous à la section "Paramétrage du protocole TCP/IP sur les systèmes Windows" à la page 391 pour obtenir des informations sur l'installation et la configuration du protocole TCP/IP.
- Pour le client d'interface utilisateur graphique Java, vous devez installer Java Runtime Environment (JRE) 1.5.0_06 ou toute version supérieure (version 1.5.0_07), par exemple.
- Vérifiez que les droits d'accès au réseau sont définis sous la règle de sécurité locale Windows pour le compte qui procède à l'installation.

Limites

- En raison des restrictions de sécurité imposées par le système d'exploitation Windows, le Serveur d'installation peut être utilisé pour installer des clients à distance uniquement dans le même domaine.
- Sous Windows Me/XP, les clients Data Protector peuvent uniquement être installés en local.
- Lors de l'installation à distance de clients sur des systèmes Windows Vista et Windows Server 2008, vous devez utiliser l'un des comptes suivants :
  - Un compte administrateur intégré sur l'hôte distant. Le compte doit être activé et le *mode approbation d'administrateur* désactivé.
  - Un compte d'utilisateur du domaine, qui est membre d'un groupe Administrateurs local sur l'hôte distant.

Recommandation

Sur chaque client Windows, assurez-vous que vous disposez de Microsoft Installer (MSI) 2.0 avant d'installer Data Protector A.06.10. Si vous possédez une version plus ancienne de MSI, le programme d'installation de Data Protector va automatiquement le mettre à niveau avec la version 2.0. Dans ce cas, Data Protector affichera une remarque à la fin de l'installation, indiquant que MSI a été mis à niveau. Si MSI a été mis à niveau, il est vivement recommandé de redémarrer le système client. Consultez le support technique Microsoft pour connaître la configuration requise pour Microsoft Installer 2.0 sur les différents systèmes d'exploitation Windows.

Si vous lancez l'installation de Data Protector avec une version antérieure de MSI, le programme d'installation de Data Protector procédera à sa mise à jour vers la version 2.0. Toutefois, ces changements ne prennent effet qu'après le redémarrage du système. Une fois l'ordinateur redémarré, reprenez l'installation.

Récupération après sinistre automatique

Le composant `Récupération après sinistre automatique` doit être installé sur les clients pour lesquels vous souhaitez activer la récupération à l'aide d'une méthode de récupération après sinistre automatique, ainsi que sur le système sur lequel l'image CD ISO DR pour la récupération après sinistre avancée sera préparée.

Clients compatibles cluster

D'autres conditions sont requises pour l'installation de clients compatibles cluster. Pour plus de détails, reportez-vous à la section "Installation de clients compatibles cluster" à la page 197.

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section "Composants Data Protector" à la page 73.

Limite du fournisseur matériel HP StorageWorks Disk Array XP

Data Protector et FRS requièrent différentes versions du fournisseur matériel HP StorageWorks Disk Array XP. Toutefois, une seule version du fournisseur matériel peut être installée sur le même système. Si vous installez Data Protector et FRS sur le même système connecté au HP StorageWorks Disk Array XP, vous ne pouvez utiliser que l'un de ces produits.

Installation locale

Il est possible d'installer les clients Windows en local à partir du DVD-ROM d'installation :

1. Insérez le DVD-ROM.

   Sur les systèmes Windows Vista et Windows Server 2008, la fenêtre Contrôle du compte utilisateur s'affiche. Cliquez sur Continuer pour poursuivre l'installation.

2. Dans la fenêtre HP Data Protector, cliquez sur Installer Data Protector pour lancer l'assistant d'installation Data Protector.

3. Suivez les instructions de l'assistant et lisez attentivement le contrat de licence. Si vous en acceptez les termes, cliquez sur Suivant pour continuer.

4. Dans la page Type d'installation, sélectionnez Client. Pour les clients Itanium, le type est sélectionné automatiquement.

5. Saisissez le nom du Gestionnaire de cellule. Reportez-vous à la Figure 18 à la page 90.

   Si le Gestionnaire de cellule utilise un autre port que le port 5555 (par défaut), modifiez le numéro du port. Vous pouvez tester si le Gestionnaire de cellule est actif et utilise le port sélectionné en cliquant sur Check response... (Tester réponse).

   Cliquez sur Suivant.

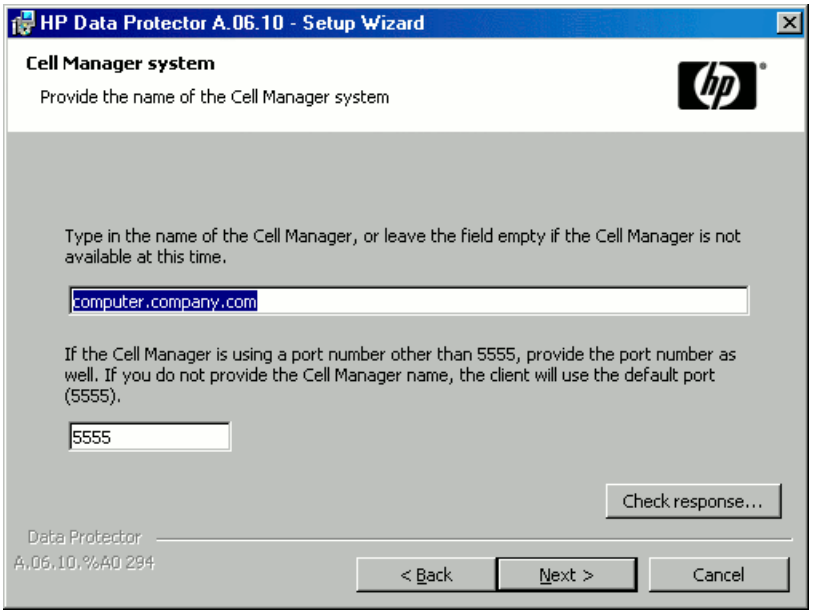

Figure 18 - Choix du Gestionnaire de cellule

6. Cliquez sur Suivant pour installer Data Protector dans le répertoire par défaut.

   Sinon, cliquez sur Modifier pour ouvrir la page Modifier le dossier de destination actuel et entrez le chemin souhaité.

7. Sélectionnez les composants de Data Protector à installer.

   Pour obtenir des informations sur les composants Data Protector, reportez-vous à la section "Composants Data Protector" à la page 73.

   Cliquez sur Suivant.

8. *Windows XP SP2, Windows Server 2003 SP1, Windows Vista et Windows Server 2008 :* si Data Protector détecte le pare-feu Windows sur votre système, la page Configuration du pare-feu Windows est affichée. Le programme d'installation de Data Protector enregistrera tous les exécutables Data Protector nécessaires. Par défaut, l'option Permettre initialement aux nouveaux fichiers binaires Data Protector enregistrés d'ouvrir des ports le cas échéant est sélectionnée. Si vous ne souhaitez pas activer Data Protector pour les ports ouverts, désélectionnez l'option. Toutefois, notez que les exécutables doivent être activés pour que Data Protector fonctionne correctement.

   Cliquez sur Suivant.

9. La liste des composants sélectionnés s'affiche. Cliquez sur Installer pour installer les composants sélectionnés.

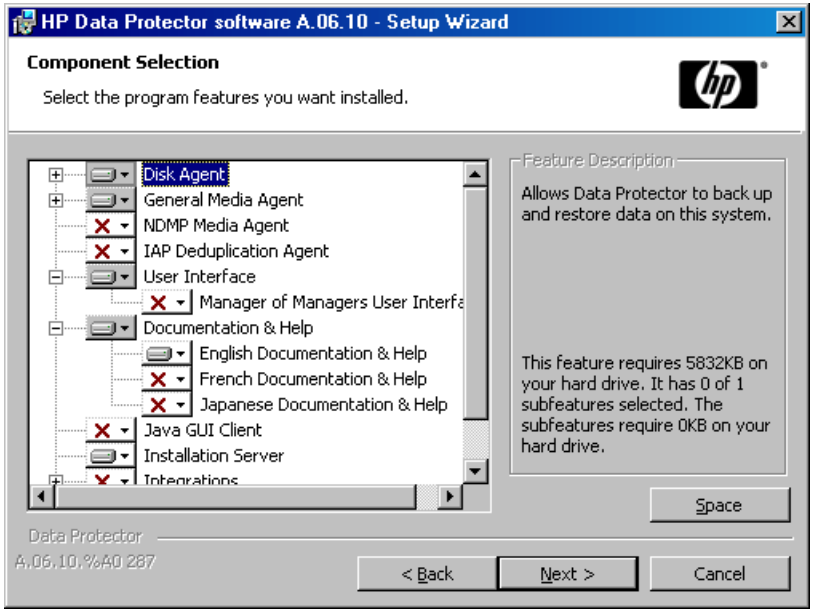

Figure 19 - Page de résumé des composants sélectionnés

10. La page d'état de l'installation s'affiche. Cliquez sur Suivant.

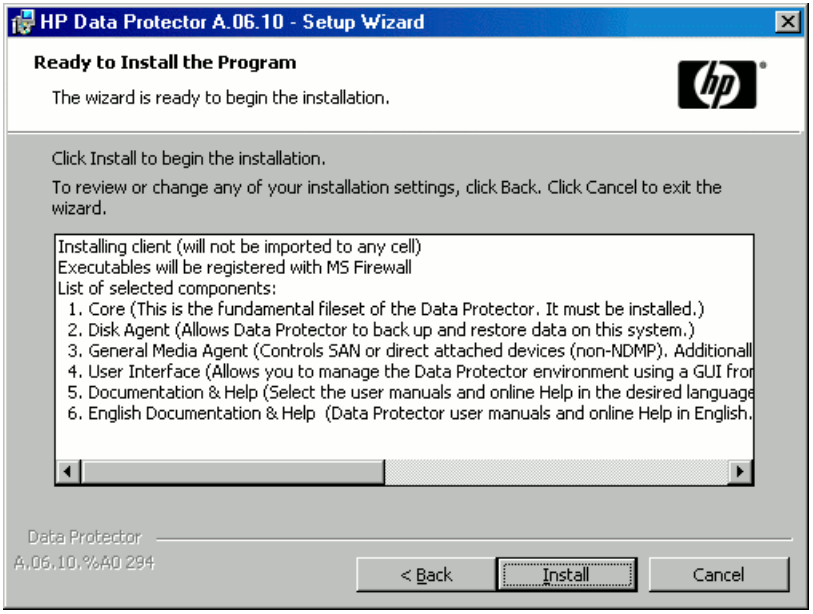

Figure 20 - Page de résumé de l'installation

11. Pour commencer à utiliser Data Protector immédiatement après son installation, sélectionnez Lancer Gestionnaire Data Protector .

Pour consulter les *Références, notes de publication et annonces produits HP Data Protector*, sélectionnez Ouvrir les annonces sur les produits.

Cliquez sur Terminer.

Connexion d'un périphérique de sauvegarde aux systèmes Windows

Une fois que vous avez installé un composant Agent de support, vous pouvez relier un périphérique de sauvegarde au système Windows en procédant comme suit :

1. Recherchez les adresses SCSI disponibles (désignées sous le nom de *ID SCSI cibles* sous Windows) pour les lecteurs et le périphérique de contrôle (robot) du périphérique de sauvegarde à connecter. Reportez-vous à la section "Recherche des ID SCSI cibles inutilisés sur un système Windows" à la page 421.

2. Définissez les `ID SCSI cibles` inutilisés pour les lecteurs et le périphérique de contrôle (robot). En fonction du type de périphérique, vous pouvez généralement effectuer cette opération avec les commutateurs du périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.

Pour plus d'information sur les périphériques pris en charge, reportez-vous au site http://www.hp.com/support/manuals.

3. Eteignez votre ordinateur et connectez le périphérique de sauvegarde au système.

4. Allumez le périphérique, puis l'ordinateur, et attendez que le processus d'amorçage soit terminé.

5. Pour vérifier que le système reconnaît correctement votre nouveau périphérique de sauvegarde, dans le répertoire *répertoire_Data_Protector*\bin, exécutez la commande `devbra -dev`.

   Un périphérique supplémentaire doit alors être répertorié dans le résultat de la commande. Par exemple, la commande `devbra -dev` peut produire le résultat suivant :

   - Si le pilote de bandes de votre périphérique est chargé :
     ```
     HP:C1533A
     tape3:0:4:0
     DDS
     ...
     ```
     La première ligne représente la spécification du périphérique, la seconde indique le nom du fichier du périphérique.
     Le format du chemin d'accès indique qu'un périphérique à bande HP DDS est doté du numéro d'instance de lecteur 3 et est connecté au bus SCSI 0, à l'ID SCSI cible 4 et au LUN numéro 0.
   - Si le pilote de bandes de votre périphérique n'est pas chargé :
     ```
     HP:C1533A
     scsi1:0:4:0
     DDS
     ...
     ```
     La première ligne représente la spécification du périphérique, la seconde indique le nom du fichier du périphérique.
     Le format du chemin d'accès indique qu'un périphérique à bande HP DDS est relié au port SCSI 1 et au bus SCSI 0, et que le lecteur de bande possède l'ID SCSI cible 4 et le numéro de LUN 0.

Pour charger ou décharger le pilote de bandes d'origine de votre périphérique, reportez-vous à la section "Utilisation de pilotes de bandes et de pilotes de robots sous Windows" à la page 402. Pour plus d'informations sur la création d'un fichier de périphérique, reportez-vous à la section "Création de fichiers de périphérique (adresses SCSI) sous Windows" à la page 406.

Etape suivante

A ce stade de la procédure, les composants clients doivent être installés et les périphériques de sauvegarde doivent être connectés pour que vous puissiez configurer des périphériques de sauvegarde et des pools de supports. Reportez-vous à l'index de l'aide en ligne : (rubrique "configuration, périphériques de sauvegarde") pour plus d'informations sur les tâches de configuration.

Installation de clients HP-UX

Les clients HP-UX peuvent être installés en local à partir du DVD-ROM d'installation UNIX ou à distance à l'aide du Serveur d'installation pour UNIX.

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section "Composants Data Protector" à la page 73.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes, processeurs et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Le cas échéant, reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 42 pour obtenir des instructions.
- Vous devez disposer soit d'un accès *root*, soit d'un compte doté des droits *root*.
- Pour le client d'interface utilisateur graphique Java, vous devez installer Java Runtime Environment (JRE) 1.5.0_06 ou toute version supérieure (version 1.5.0_07), par exemple.

Installation en local

Si aucun Serveur d'installation pour UNIX n'est installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation pour UNIX. Reportez-vous à la section "Installation locale de clients UNIX" à la page 142 pour de plus amples informations.

Après l'installation en local, le système client doit être importé manuellement dans la cellule. Reportez-vous également à la section "Importation de clients dans une cellule" à la page 205.

Installation distante

Vous devez installer le logiciel client à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface graphique utilisateur Data Protector. Pour connaître la procédure détaillée pour installer le logiciel à distance, reportez-vous à la section "Installation distante de clients Data Protector" à la page 78.

Une fois l'installation à distance terminée, le système client devient automatiquement membre de la cellule Data Protector.

Si vous avez installé un Agent de support sur le système client, vous devez connecter physiquement le périphérique de sauvegarde au système. Pour savoir si les pilotes de

périphériques correspondant au type de votre périphérique sont déjà intégrés dans le noyau, vérifiez la configuration du noyau avant d'exécuter une sauvegarde.

Clients compatibles cluster

D'autres conditions et étapes sont requises pour l'installation de clients compatibles cluster. Pour plus de détails, reportez-vous à la section "Installation d'un client compatible cluster" à la page 187.

Vérification de la configuration du noyau sous HP-UX

La procédure suivante explique comment vérifier et déterminer la configuration de votre noyau sur le système HP-UX 11.x à l'aide de l'utilitaire *HP System Administration Manager (SAM)*. Pour connaître la procédure manuelle de création du noyau, reportez-vous à la section "Configuration de robot SCSI sous HP-UX" à la page 407.

Procédez comme suit pour configurer le noyau à l'aide de l'utilitaire *HP System Administration Manager (SAM)* :

1. Connectez-vous comme utilisateur `root`, ouvrez le terminal puis tapez `sam`.
2. Dans la fenêtre System Administration Manager, cliquez deux fois sur Configuration du kernel, puis cliquez sur Pilotes.
3. Dans la fenêtre Configuration du kernel, vérifiez les éléments suivants :
   - Les pilotes des périphériques que vous allez utiliser doivent apparaître dans la liste des pilotes installés. Reportez-vous à la Figure 21 à la page 96. Si le pilote que vous recherchez n'est pas mentionné, vous devez l'installer à l'aide de l'utilitaire `/usr/sbin/swinstall`. Par exemple :
     - Un pilote de périphériques à bandes est requis pour les périphériques à bande et doit être installé si vous souhaitez connecter ce type de périphérique au système. Par exemple, le pilote `stape` est utilisé pour les lecteurs de bande SCSI génériques de type DLT ou LTO, alors que le pilote `tape2` est réservé aux périphériques DDS.
     - Un pilote de passage SCSI nommé `sctl` ou `spt`, ou un pilote de robot de changeur automatique nommé `schgr` (selon le matériel) est requis pour contrôler le robot des périphériques de bibliothèque de bande. Pour plus de détails, reportez-vous à la section "Configuration de robot SCSI sous HP-UX" à la page 407.

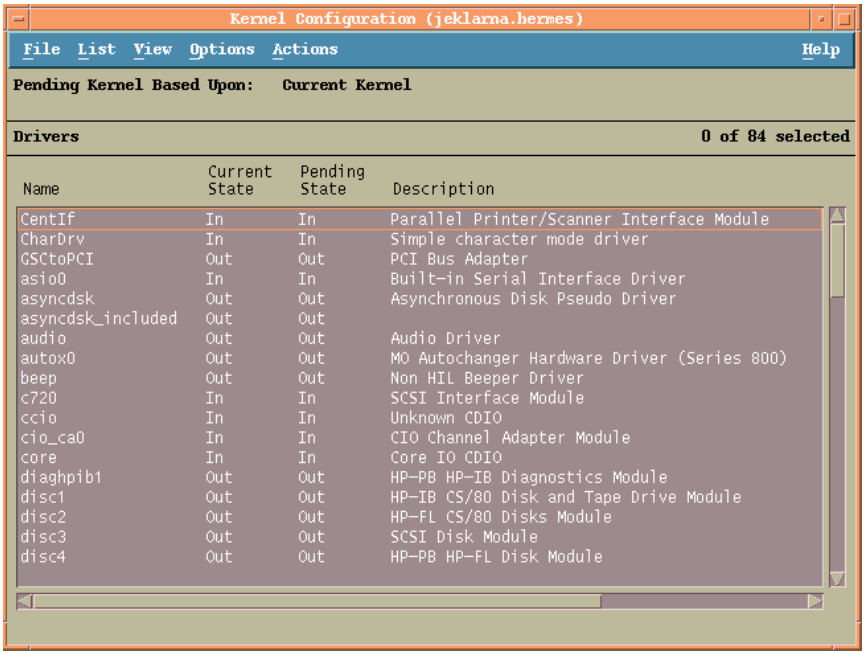

Figure 21 - Fenêtre de configuration du kernel

- L'état d'un pilote affiché dans la colonne Etat actuel doit être défini à Dedans. Si la valeur de l'état est Dehors, procédez comme suit :
  1. sélectionnez le pilote dans la liste. Cliquez sur Actions et sélectionnez Ajouter pilote au kernel. L'état est alors réglé sur Dedans dans la colonne `Etat en attente`.

     Répétez cette étape pour chaque pilote dont l'Etat actuel est défini sur Dedans.
  2. Cliquez sur Actions et sélectionnez Créer kernel pour appliquer les modifications, c'est-à-dire créer un kernel en attente dans le kernel en cours. Cette opération nécessite un redémarrage du système.

Une fois que tous les pilotes requis sont créés dans le noyau, vous pouvez continuer en reliant un périphérique de sauvegarde à votre système.

Connexion d'un périphérique de sauvegarde aux systèmes HP-UX

1. Déterminez les adresses SCSI disponibles pour les lecteurs et le périphérique de contrôle (robot). Utilisez la commande système `/usr/sbin/ioscan -f`.

   Pour plus d'informations, reportez-vous à la section "Recherche des adresses SCSI non utilisées sous HP-UX" à la page 414.

2. Définissez l'adresse SCSI sur le périphérique. En fonction du type de périphérique, vous pouvez généralement effectuer cette opération avec les commutateurs du périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.

   Pour plus d'information sur les périphériques pris en charge, reportez-vous au site http://www.hp.com/support/manuals.

3. Connectez le périphérique au système, allumez le périphérique, puis l'ordinateur et attendez que le processus d'amorçage soit terminé. Les fichiers du périphérique sont généralement créés au cours de ce processus.

4. Vérifiez que le système reconnaît bien le nouveau périphérique de sauvegarde. Servez-vous de l'utilitaire `ioscan` :

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

   de manière à pouvoir visualiser la liste des fichiers de chaque périphérique de sauvegarde connecté. Si un fichier de périphérique n'a pas été créé automatiquement durant le processus d'amorçage, vous devez le créer manuellement. Reportez-vous à la section "Création de fichiers de périphérique sous HP-UX" à la page 412.

Lorsque vous avez terminé l'installation et connecté correctement les périphériques de sauvegarde au système, reportez-vous à l'index de l'aide en ligne (rubrique "configuration, périphériques de sauvegarde") pour obtenir des informations détaillées sur la configuration des périphériques et des pools de supports, ou sur d'autres tâches de configuration de Data Protector.

Installation de clients Solaris

Les clients Solaris peuvent être installés en local à partir du DVD-ROM d'installation UNIX ou à distance à l'aide du Serveur d'installation pour UNIX.

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section "Composants Data Protector" à la page 73.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 42 pour obtenir des instructions.
- Pour installer un client Solaris, vous devez disposer soit d'un accès *root*, soit d'un compte doté des droits *root*.

- Pour le client d'interface utilisateur graphique Java, vous devez installer Java Runtime Environment (JRE) 1.5.0_06 ou toute version supérieure (version 1.5.0_07), par exemple.

Installation en local

Si aucun Serveur d'installation pour UNIX n'est installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation pour UNIX. Reportez-vous à la section "Installation locale de clients UNIX" à la page 142 pour obtenir des instructions.

Installation distante

Vous devez installer le logiciel client à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface graphique utilisateur Data Protector. Pour connaître la procédure détaillée pour installer le logiciel à distance, reportez-vous à la section "Installation distante de clients Data Protector" à la page 78.

REMARQUE :

Si vous installez le composant `Interface utilisateur` (comprenant l'interface graphique utilisateur et l'interface de ligne de commande), il faut au préalable mettre à jour les variables de votre environnement. Pour plus d'informations, reportez-vous à la section "Configuration des variables d'environnement" à la page 51.

Si vous installez l'interface utilisateur sur un client Solaris 2.6, seule l'interface de ligne de commande sera disponible.

Dès que les composants client sont installés, le système cible devient automatiquement un élément de la cellule Data Protector.

IMPORTANT :

Si vous souhaitez installer Data Protector sur des répertoires liés, par exemple :

`/opt/omni/ -> /`*`préfixe`*`/opt/omni/`

`/etc/opt/omni/ -> /`*`préfixe`*`/etc/opt/omni/`

`/var/opt/omni/ -> /`*`préfixe`*`/var/opt/omni/`

Vous devez créer les liens avant l'installation et vous assurer que les répertoires cible existent.

Clients compatibles cluster

D'autres conditions sont requises pour l'installation de clients compatibles cluster. Pour plus de détails, reportez-vous à la section "Installation d'un client" à la page 200.

Configuration post-installation

Fichiers de configuration

Une fois qu'un composant Agent de support est installé sur le système client, vous devez vérifier les fichiers de configuration (`/kernel/drv/st.conf`) selon le type de périphérique que vous allez utiliser.

- Pour un périphérique Exabyte (8 mm), aucune modification du fichier `/kernel/drv/st.conf` n'est requise.
- Pour un périphérique HP DAT (4 mm), ajoutez les lignes suivantes au fichier `/kernel/drv/st.conf` :
  `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 ;
```

IMPORTANT :

Ces entrées HP data sont différentes des entrées par défaut généralement proposées par l'assistance HP. Saisissez ces caractères avec précision ; dans le cas contraire, Data Protector ne pourra pas utiliser votre lecteur.

- Pour les périphériques DLT, DLT1, SuperDLT, LTO1, LTO2 et STK9840, ajoutez les lignes suivantes au fichier `/kernel/drv/st.conf` :
  `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;
```

- Pour un système de chargement automatique HP StorageWorks 12000e (48AL) (HP C1553A), ajoutez les entrées suivantes en plus des entrées HP dans le fichier `/kernel/drv/st.conf` :

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

  Remplacez l'*ID* par l'adresse SCSI du chargeur automatique et définissez le numéro de l'option sur `5` (le commutateur se trouve au niveau du panneau arrière du périphérique) et le paramètre du commutateur DIP du lecteur sur `11111001` (les commutateurs sont accessibles par le dessous du chargeur automatique).

REMARQUE :

La bibliothèque HP StorageWorks 12000e ne possède pas d'ID SCSI dédié pour le périphérique sélectionneur, mais les commandes d'accès au lecteur de données et les commandes sélectionneur sont acceptées pour le même ID SCSI. Les commandes d'accès au lecteur de données doivent toutefois être dirigées vers SCSI lun=0 et les commandes sélectionneur doivent être définies sur SCSI lun=1.

Pour tous les autres périphériques, consultez le modèle `st.conf.templ` (situé dans le répertoire `/opt/omni/spt`) pour connaître les entrées requises dans le fichier `st.conf`. Il ne s'agit que d'un fichier modèle, qui n'est pas conçu pour remplacer le fichier `st.conf`.

- Pour les périphériques échangeurs SCSI sous Solaris utilisant le pilote de passage SCSI, vous devez installer ce pilote en premier, puis le périphérique SCSI.
  Pour installer le pilote de passage SCSI, procédez comme suit :

  1. Copiez le module `sst` dans le répertoire `/usr/kernel/drv/sparcv9` et le fichier de configuration `sst.conf` dans le répertoire `/usr/kernel/drv` :

     Systèmes Solaris 32 bits :

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

     Systèmes Solaris 64 bits :

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

2. Ajoutez la ligne suivante au fichier `/etc/devlink.tab` :

IMPORTANT :

N'insérez pas de caractère [espace] lorsque vous modifiez le fichier `/etc/devlink.tab`. Utilisez uniquement des tabulations.

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

Des devlinks (1M) créent alors un/des lien(s) vers les périphériques dont le nom est de type `/dev/rsstX`, où X représente le numéro de cible SCSI.

3. Installez le pilote sur le système en entrant la commande suivante :

```
add_drv sst
```

4. A ce niveau de la procédure, vous êtes prêt à installer le périphérique SCSI. Mais avant l'installation, vous devez attribuer l'adresse SCSI appropriée à chaque lecteur et au robot (sélectionneur) du périphérique échangeur. Les adresses choisies ne doivent être utilisées par aucun autre périphérique du système.

   Pour vérifier la configuration SCSI, arrêtez le système en tapant la commande suivante :

```
shutdown -i0
```

   Exécutez ensuite la commande `probe-scsi-all` à l'invite `ok` pour vérifier les adresses attribuées :

```
ok probe-scsi-all
```

   Lorsque vous avez terminé, relancez le système avec :

```
ok boot -r
```

   Pour installer le périphérique SCSI, procédez comme suit :

   a. Editez le fichier `/kernel/drv/st.conf` pour configurer les paramètres de lecteur du périphérique afin d'utiliser les ports SCSI attribués (reportez-vous à la documentation du périphérique approprié).

      L'exemple suivant présente l'installation du périphérique ADIC-VLS DLT, le port SCSI 5 étant attribué au lecteur de bande SCSI et le port SCSI 4 étant attribué au périphérique de contrôle (sélectionneur) ADIC SCSI :

Exemple

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

```
target=4 lun=0;
```

Les données de l'exemple ci-dessus doivent se trouver dans le fichier

`/kernel/drv/st.conf`.

b. Editez le fichier `/usr/kernel/drv/sst.conf` pour configurer le périphérique de contrôle ADIC SCSI afin d'utiliser le port SCSI 4 qui lui est attribué. Ajoutez les données suivantes pour le lecteur ADIC au fichier `/usr/kernel/drv/sst.conf` :

```
name="sst" class= "scsi" target=4 lun=0;
```

Une fois que vous avez modifié les fichiers `/kernel/drv/st.conf` et `/usr/kernel/drv/sst.conf`, vous pouvez relier physiquement le périphérique de sauvegarde au système.

Connexion d'un périphérique de sauvegarde à un système Solaris

Procédez comme suit pour connecter un périphérique de sauvegarde à un système Solaris :

1. Créez un fichier `reconfigure` :

   ```
   touch /reconfigure
   ```

2. Arrêtez le système en entrant la commande `$shutdown -i0` et éteignez l'ordinateur, puis connectez physiquement le périphérique au bus SCSI. Vérifiez qu'aucun autre périphérique n'utilise l'adresse SCSI que vous avez sélectionnée.

   Pour plus d'information sur les périphériques pris en charge, reportez-vous au site http://www.hp.com/support/manuals.

   REMARQUE :

   Data Protector ne reconnaît pas automatiquement les bandes nettoyantes sur un système Solaris. Si Data Protector détecte et insère la bande nettoyante utilisée dans le périphérique StorageWorks 12000e (48AL), le pilote de bandes prend un état non défini et peut vous demander de réamorcer le système. Chargez manuellement une bande nettoyante lorsque Data Protector en fait la demande.

3. Rallumez l'ordinateur et suspendez le processus d'amorçage en appuyant sur la touche `Stop-A`. Vérifiez que le nouveau périphérique est bien reconnu en entrant la commande `probe-scsi-all` à l'invite `ok` :

   ```
   ok > probe-scsi-all
   ```

   puis entrez :

   ```
   ok > go
   ```

   pour continuer.

4. A ce niveau de la procédure, le périphérique doit fonctionner correctement. Les fichiers de périphérique doivent se trouver dans le répertoire `/dev/rmt` pour les lecteurs, et dans le répertoire `/dev` pour le périphérique de contrôle (sélectionneur) SCSI.

REMARQUE :

Sur les systèmes Solaris (en particulier dans le cas de Solaris 64 bits), les liens vers le périphérique de contrôle SCSI (sélectionneur) ne sont pas toujours créés automatiquement. Dans ce cas, créez des liens symboliques. Par exemple : `ln -s /devices/pci@1f,4000/scsi@3,1/sst@4,1:character /dev/rsst4`

Vous pouvez vérifier le périphérique à l'aide de l'utilitaire `uma` de Data Protector. Pour vérifier le sélectionneur du périphérique échangeur SCSI à partir de l'exemple précédent (avec le port SCSI 4), entrez :

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

Ce dernier doit s'identifier comme une bibliothèque de périphérique SCSI-2. Vous pouvez vérifier la bibliothèque en la forçant à s'initialiser. La commande est la suivante :

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

Vérifiez que vous utilisez bien des fichiers de périphérique de style Berkeley, dans ce cas `/dev/rmt/ohb` (et non `/dev/rmt/0h`) pour le lecteur échangeur, et `/dev/rsst4` pour le périphérique de contrôle (sélectionneur) SCSI.

Etape suivante

Lorsque vous avez terminé l'installation et connecté correctement les périphériques de sauvegarde au client Solaris, reportez-vous à l'index de l'aide en ligne (rubrique "configuration, périphériques de sauvegarde") pour obtenir plus d'informations sur la configuration des périphériques de sauvegarde et des pools de supports, ou sur d'autres tâches de configuration.

Installation de clients Linux

Les clients Linux peuvent être installés en local à partir du DVD-ROM d'installation UNIX ou à distance à l'aide du Serveur d'installation pour UNIX.

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section "Composants Data Protector" à la page 73.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 42 pour de plus amples informations.
- L'utilitaire `rpm` doit être installé et configuré. Les autres systèmes de gestion de packages (tels que `deb`) ne sont pas pris en charge.
- Pour le client d'interface utilisateur graphique Java, vous devez installer Java Runtime Environment (JRE) 1.5.0_06 ou toute version supérieure (version 1.5.0_07), par exemple.

REMARQUE :

Sur les plates-formes Gestionnaire de cellule qui ne prennent pas en charge l'interface utilisateur graphique d'origine de Data Protector, vous pouvez utiliser l'interface utilisateur graphique Java de Data Protector ou installer l'interface utilisateur graphique d'origine de Data Protector sur un système qui la prend en charge. Utilisez la commande `omniusers` pour créer un compte utilisateur distant sur le nouveau Gestionnaire de cellule. Vous pouvez alors utiliser ce compte utilisateur avec l'interface graphique utilisateur de Data Protector installée pour lancer l'interface et vous connecter au nouveau Gestionnaire de cellule. Reportez-vous à la page `omniusers` du manuel.

REMARQUE :

Data Protector utilise le numéro de port par défaut 5555. Ce numéro de port particulier ne doit donc pas être utilisé par un autre programme. Certaines versions de Linux utilisent ce numéro à d'autres fins.

Si ce numéro de port est déjà utilisé, vous devez le rendre disponible pour Data Protector ou remplacer cette valeur par défaut par le numéro d'un port non utilisé. Reportez-vous à la section "Modification du numéro de port par défaut de Data Protector" à la page 398.

Cluster MC/ServiceGuard

Pour les clusters MC/ServiceGuard, il faut installer séparément les agents Data Protector (de disque ou de support) *sur chaque nœud de cluster* (disque local) et pas sur le disque partagé.

Une fois l'installation terminée, vous devez importer l'*hôte virtuel* (package d'application) dans la cellule sous forme de client. Le package d'application (par exemple Oracle)

doit donc fonctionner sur le cluster avec son *adresse IP de serveur virtuel*. Utilisez la commande `cmviewcl -v` pour le vérifier avant d'importer le client.

Novell Open Enterprise Server (OES)

Sur les systèmes Novell OES, Data Protector installe automatiquement l'agent de disque compatible OES. Les systèmes Novell OES présentent cependant des spécificités :

- Si vous installez Novell OES sur un serveur SUSE Linux Enterprise Server 9.0 (SLES) 32 bits après avoir installé un client Linux Data Protector sur un système, vous devez également mettre à niveau le client Data Protector.
  Notez que le nouvel agent de disque compatible Novell OES sera chargé sur le système client au cours de cette mise à niveau.
- Si vous supprimez le composant Novell OES du SLES, vous devez réinstaller le client Data Protector.

Installation en local

Si aucun Serveur d'installation pour UNIX n'est installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation pour UNIX. Reportez-vous à la section "Installation locale de clients UNIX" à la page 142 pour de plus amples informations.

Installation distante

Vous pouvez installer à distance un système client Linux en distribuant les composants Data Protector à partir du Serveur d'installation pour UNIX sur le système Linux, à l'aide de l'interface graphique utilisateur de Data Protector. Pour connaître la procédure détaillée de cette opération, reportez-vous à la section "Installation distante de clients Data Protector" à la page 78.

Dès que les composants client sont installés, le système cible devient automatiquement un élément de la cellule Data Protector.

Dépannage

Si un problème survient lors de l'installation à distance sur un système client Linux, vérifiez que le compte `root` dispose de droits d'accès au système, en utilisant soit le service `exec`, soit le service `shell`. Pour effectuer cette opération, procédez comme suit :

1. Editez le fichier `/etc/xinetd.conf`. Recherchez les définitions des services `exec` et `shell` et ajoutez-leur la ligne suivante :

   ```
   server_args = -h
   ```

   Par exemple :

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

REMARQUE :

Dans certaines distributions Linux, ces services sont configurés dans des fichiers distincts situés dans le répertoire `/etc/xinetd.d`. Dans ce cas, localisez le fichier approprié (`/etc/xinetd.d/rexec` et `/etc/xinetd.d/rsh`) et modifiez-le comme décrit ci-dessus.

2. Arrêtez le processus `inetd` avec le signal `HUP` :

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

3. Créez un fichier `~root/.rhosts` avec l'entrée : *`mon_serveur_installation`* `root` Cette opération permettra l'accès d'administration à partir du Serveur d'installation.

Après avoir installé Data Protector, vous pouvez supprimer l'entrée du fichier `-root/.rhosts`, l'indicateur `-h` du fichier `/etc/xinetd.conf` (`/etc/inetd.conf` pour Red Hat Enterprise Linux). Répétez ensuite la commande `kill` décrite à l'Étape 2 à la page 106.

Pour obtenir plus d'informations, reportez-vous à la page du manuel `rexecd`(8), `rexec`(3), `rshd`(8), `rsh`(1) ou `pam`(8). En cas d'échec, reportez-vous à la section "Installation locale de clients UNIX" à la page 142.

Configuration du noyau

Vous trouverez ci-après la procédure à suivre pour vérifier et créer la configuration de votre noyau :

1. Connectez-vous en tant qu'utilisateur root, puis, dans le répertoire `/usr/src/linux`, exécutez la commande `make menuconfig`.
2. Sélectionnez `Prise en charge SCSI` et appuyez sur `Entrée`. Sélectionnez ensuite les options suivantes : `Prise en charge SCSI`, `Prise en charge de bandes SCSI`, `Prise en charge générique SCSI` et éventuellement `Explorer tous les LUNS de chaque périphérique SCSI`.

   Si ces éléments sont déjà inclus dans le noyau, quittez le programme sans enregistrer les modifications. Vous pouvez poursuivre en connectant un périphérique de sauvegarde à votre système. Reportez-vous à la section "Connexion d'un périphérique de sauvegarde à un système Linux" à la page 108.
3. Si vous avez effectué des modifications, enregistrez la configuration et procédez comme suit :

   a. Exécutez la commande `make dep`.

   Cette commande génère l'arborescence des dépendances dans les sources du noyau. Ces dépendances peuvent être affectées par les options que vous avez choisies lors de la configuration du noyau.

   b. Exécutez la commande `make clean` pour purger les fichiers restants des créations antérieures du noyau.

   c. Exécutez la commande `make bzImage`. Une fois qu'elle est terminée, exécutez la commande `make modules`.

4. Pour installer le noyau dans le répertoire `/boot` sur un système Intel, copiez le nouveau fichier `bzImage` dans le répertoire `/boot` en procédant comme suit :

   a. Exécutez la commande suivante : `cp /usr/src/linux/arch/i386/boot/bzImage /boot/newkernel`

   b. Exécutez la commande `make modules_install` pour installer les modules dans le répertoire `/lib/modules`.

   c. Modifiez `/etc/lilo.conf` et ajoutez les informations suivantes :

   ```
   image = /boot/newkernel
   label = new
   read-only
   ```

   d. Exécutez la commande `/sbin/lilo` pour mettre à jour LILO.

   Au redémarrage suivant, sélectionnez le noyau (kernel) 'new' dans LILO : cette opération chargera le nouveau noyau. Si tout fonctionne correctement, placez-le en première position dans le fichier `lilo.conf` afin qu'il s'amorce systématiquement par défaut.

   Pour plus d'informations sur le noyau et la configuration SCSI, reportez-vous au répertoire source du noyau, `/usr/src/linux/Documentation/`.

Connexion d'un périphérique de sauvegarde à un système Linux

Lorsqu'un composant Agent de support est installé sur le client Linux, procédez comme suit pour relier un périphérique de sauvegarde au système :

1. Exécutez la commande `cat /proc/scsi/scsi` pour déterminer les adresses SCSI disponibles pour les lecteurs et le périphérique de contrôle (robot).

2. Définissez l'adresse SCSI sur le périphérique. En fonction du type de périphérique, vous pouvez effectuer cette opération à l'aide des commutateurs du périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.

   Pour plus d'information sur les périphériques pris en charge, reportez-vous au site http://www.hp.com/support/manuals.

3. Connectez le périphérique au système, allumez le périphérique, puis l'ordinateur et attendez que le processus d'amorçage soit terminé. Les fichiers du périphérique sont créés au cours de ce processus. (sur RedHat Linux, une application, Kudzu, est lancée lors du processus d'amorçage lorsqu'un nouveau périphérique est connecté au système. Appuyez sur n'importe quelle touche pour lancer l'application, puis cliquez sur le bouton `Configurer`).

4. Pour vous assurer que le système reconnaît votre nouveau périphérique de sauvegarde, exécutez la commande `cat /proc/scsi/scsi`, puis la commande `dmesg |grep scsi`. Les fichiers du périphérique sont répertoriés pour chaque périphérique de sauvegarde connecté.

Exemples

En ce qui concerne le robot, la commande `dmesg |grep scsi` produit le résultat suivant :

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

En ce qui concerne les lecteurs, cette commande produit le résultat suivant :

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

5. Les fichiers du périphérique sont créés dans le répertoire `/dev`. Pour vous assurer que les liens vers les fichiers du périphérique ont été créés, exécutez la commande :

   ```
   ll /dev | grep fichier_périphérique
   ```

   Par exemple :

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

   Le résultat de cette commande est le suivant :

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

   où `/dev/sg2` est un lien vers le fichier de périphérique `/dev/sgc`. Cela signifie que les fichiers de périphérique à utiliser par Data Protector sont `/dev/sgc` pour le robot et `/dev/st0` pour le lecteur. Les fichiers de périphérique destinés au robot sont `sga`, `sgb`, `sgc`,... `sgh` ; ceux qui sont destinés aux lecteurs sont `st0`, `st1`, ... `st7`.

Etape suivante

Lorsque vous avez terminé l'installation et connecté correctement les périphériques de sauvegarde au système client Linux, reportez-vous à l'index de l'aide en ligne (rubrique "configuration, périphériques de sauvegarde") pour obtenir plus d'informations sur la configuration des périphériques et des pools de supports, ou sur d'autres tâches de configuration.

Installation des clients ESX Server

ESX Server est un système d'exploitation Linux modifié. Pour plus d'informations sur l'installation des composants Data Protector sur des systèmes ESX Server, reportez-vous à la section "Installation de clients Linux" à la page 103.

Installation de clients AIX

Les clients AIX peuvent être installés en local à partir du DVD-ROM d'installation UNIX ou à distance à l'aide du Serveur d'installation pour UNIX.

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section "Composants Data Protector" à la page 73.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 42 pour obtenir des instructions.

IMPORTANT :

Avant d'installer le composant `Agent de disque` sur un système AIX, vérifiez que le portmapper est en cours d'exécution. La ligne permettant de lancer le portmapper doit se trouver dans le fichier `/etc/rc.tcpip` :

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

L'indicateur `src_running` est défini sur 1 si le démon `srcmstr` est en cours d'exécution. Ce dernier est le Contrôleur des ressources système (SRC). Il génère et contrôle les sous-systèmes, gère les demandes courtes d'état de sous-système, transfère des demandes à un sous-système et gère des notifications d'erreur.

Cluster IBM HACMP

Dans l'environnement IBM HACMP (High Availability Cluster Multi-Processing) pour AIX, installez le composant `Agent de disque`Data Protector sur tous les noeuds du cluster. Pour plus d'informations sur l'installation de Data Protector dans un environnement de cluster comprenant une application de base de données compatible cluster, reportez-vous à la section "Installation des clients d'intégration Data Protector" à la page 145.

Après l'installation, importez les nœuds du cluster et le *serveur virtuel* (adresse IP du package de l'environnement virtuel) dans la cellule Data Protector.

Installation en local

Si aucun Serveur d'installation pour UNIX n'est installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation pour

UNIX. Reportez-vous à la section “Installation locale de clients UNIX” à la page 142 pour obtenir des instructions.

Installation distante

Vous devez installer le logiciel client AIX à partir du Serveur d’installation pour UNIX sur les systèmes clients utilisant l’interface graphique utilisateur Data Protector. Pour connaître la procédure détaillée pour installer le logiciel à distance, reportez-vous à la section “Installation distante de clients Data Protector” à la page 78.

Dès que les composants client sont installés, le système cible devient automatiquement un élément de la cellule Data Protector.

Connexion d’un périphérique de sauvegarde à un client AIX

Lorsqu’un composant Agent de support est installé sur un système client AIX, procédez comme suit:

1. Eteignez l’ordinateur et reliez le périphérique de sauvegarde au bus SCSI. Vérifiez qu’aucun autre périphérique n’utilise la même adresse SCSI que celle qui a été sélectionnée pour le périphérique de sauvegarde à relier.

   Pour plus d’information sur les périphériques pris en charge, reportez-vous au site http://www.hp.com/support/manuals.

2. Allumez l’ordinateur et attendez que le processus d’amorçage soit terminé. Lancez l’outil de gestion `smit` du système AIX et vérifiez que ce dernier reconnaît bien le nouveau périphérique de sauvegarde.

   IMPORTANT :

   Utilisez l’outil `smit` pour donner à la taille de bloc du périphérique la valeur par défaut `0` (taille de bloc variable).

3. Sélectionnez les fichiers de périphérique appropriés dans le répertoire `/dev` et configurez le périphérique de sauvegarde Data Protector.

IMPORTANT :

Utilisez uniquement des fichiers de périphérique du type sans rembobinage. Par exemple, sélectionnez `/dev/rmt0.1` au lieu de `/dev/rmt0`.

Etape suivante

Lorsque vous avez terminé l’installation et connecté correctement les périphériques de sauvegarde au système, reportez-vous à l’index de l’aide en ligne (rubrique "configuration, périphériques de sauvegarde") pour obtenir plus d’informations sur la

configuration des périphériques et des pools de supports, ou sur d'autres tâches de configuration de Data Protector.

Installation de clients Siemens Sinix

Les clients Siemens Sinix peuvent être installés en local à partir du DVD-ROM d'installation UNIX ou à distance à l'aide du Serveur d'installation pour UNIX.

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section "Composants Data Protector" à la page 73.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 42 pour de plus amples informations.

Installation en local

Si aucun Serveur d'installation pour UNIX n'est installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation pour UNIX. Reportez-vous à la section "Installation locale de clients UNIX" à la page 142 pour de plus amples informations.

Installation distante

Vous devez installer le logiciel client Sinix à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface graphique utilisateur Data Protector. Pour connaître la procédure détaillée pour installer le logiciel à distance, reportez-vous à la section "Installation distante de clients Data Protector" à la page 78.

Dès que les composants client sont installés, le système cible devient automatiquement un élément de la cellule Data Protector.

Connexion d'un périphérique de sauvegarde à un système Siemens Sinix

Lorsqu'un composant Agent de support est installé sur un système client Siemens Sinix, procédez comme suit pour connecter un périphérique de sauvegarde au système:

1. Eteignez votre ordinateur et connectez le périphérique de sauvegarde au bus SCSI.

   Pour plus d'information sur les périphériques pris en charge, reportez-vous au site http://www.hp.com/support/manuals et à la documentation fournie avec chaque périphérique.

   Vérifiez qu'aucun autre périphérique n'utilise la même adresse SCSI que celle que vous avez sélectionnée pour le périphérique de sauvegarde à relier.

2. Rallumez l'ordinateur et attendez que le processus d'amorçage soit terminé.

3. Sélectionnez le fichier de périphérique approprié dans le répertoire `/dev`.

   Vous pouvez obtenir la liste des périphériques avec la commande `autoconf -l`. Utilisez le périphérique à bande (`ios0/stape006` par exemple) indiqué dans le résultat de cette commande pour connaître le nom du fichier du périphérique spécial qui peut être utilisé par Data Protector (par exemple, `/dev/ios0/rstape006nv`).

REMARQUE :

Les fichiers de périphérique spéciaux se trouvent dans le répertoire `/dev`. Vous devez donc ajouter le chemin d'accès `/dev` devant le nom du périphérique.

Data Protector ne pouvant utiliser qu'un périphérique type caractère, la lettre `r` est ajoutée devant `stape006`.

Data Protector peut gérer un périphérique à bandes s'il est ouvert comme un périphérique non rembobinable et avec une taille de bloc variable ; vous devez donc ajouter les lettres `n` et `v` comme suffixes.

Le nom de fichier de périphérique `/dev/ios0/rstape006nv` est expliqué à la Figure 22 à la page 114.

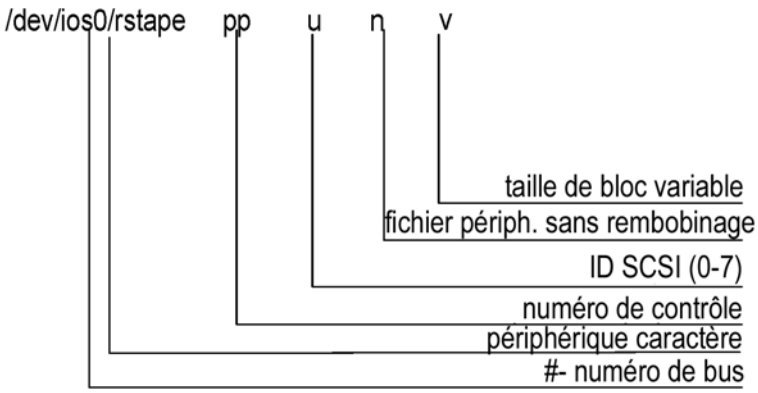

Figure 22 - Format de nom de fichier de périphérique

Etape suivante

Lorsque vous avez terminé l'installation et connecté correctement les périphériques de sauvegarde au système client Siemens Sinix, reportez-vous à l'index de l'aide en ligne (rubrique "configuration, périphériques de sauvegarde") pour obtenir plus d'informations sur la configuration des périphériques et des pools de supports, ou sur d'autres tâches de configuration.

Installation de clients Tru64

Les clients Tru64 peuvent être installés en local à partir du DVD-ROM d'installation UNIX ou à distance à l'aide du Serveur d'installation pour UNIX.

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section "Composants Data Protector" à la page 73.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 42 pour de plus amples informations.

Installation en local

Si aucun Serveur d'installation pour UNIX n'est installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation pour UNIX. Reportez-vous à la section "Installation locale de clients UNIX" à la page 142 pour de plus amples informations.

Installation distante

Vous devez installer le logiciel client Tru64 à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface graphique utilisateur Data Protector. Pour connaître la procédure détaillée pour installer le logiciel à distance, reportez-vous à la section "Installation distante de clients Data Protector" à la page 78.

Dès que les composants client sont installés, le système cible devient automatiquement un élément de la cellule Data Protector.

Cluster Tru64

Vous devez disposer d'autorisations de `root` sur chaque système cible.

Data Protector doit être installé en local ou à distance sur le disque partagé du cluster Tru64. Utilisez l'un des nœuds du cluster pour effectuer une installation.

Après l'installation, il faut importer le nom d'hôte virtuel du cluster et les différents nœuds dans la cellule Data Protector. Pour connaître la procédure, reportez-vous à la section "Importation d'un client compatible cluster dans une cellule" à la page 208

Connexion d'un périphérique de sauvegarde à un client Tru64

Lorsqu'un composant Agent de support est installé sur un système client Tru64, procédez comme suit:

1. Eteignez votre ordinateur et connectez le périphérique de sauvegarde au bus SCSI.

   REMARQUE :

   Il est déconseillé de connecter le périphérique de sauvegarde sur le même bus SCSI que le disque dur.

   Vérifiez qu'aucun autre périphérique n'utilise la même adresse SCSI que celle que vous avez sélectionnée pour le périphérique de sauvegarde.

   Pour plus d'information sur les périphériques pris en charge, reportez-vous au site http://www.hp.com/support/manuals.

2. Allumez l'ordinateur et attendez que le processus d'amorçage soit terminé. Vérifiez que le système reconnaît bien le nouveau périphérique de sauvegarde.

Etape suivante

Lorsque vous avez terminé l'installation et connecté correctement les périphériques de sauvegarde au système Tru64, reportez-vous à l'index de l'aide en ligne (rubrique "configuration, périphériques de sauvegarde") pour obtenir plus d'informations sur la configuration des périphériques et des pools de supports, ou sur d'autres tâches de configuration de Data Protector.

Installation de clients SCO

Les clients SCO peuvent être installés en local à partir du DVD-ROM d'installation UNIX ou à distance à l'aide du Serveur d'installation pour UNIX.

Notez que l'installation à distance du système UnixWare n'est pas disponible.

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section "Composants Data Protector" à la page 73.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 42 pour de plus amples informations.

Installation en local

Si aucun Serveur d'installation pour UNIX n'est installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation pour UNIX. Reportez-vous à la section "Installation locale de clients UNIX" à la page 142 pour de plus amples informations.

Installation distante

Vous devez installer le logiciel client SCO à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface graphique utilisateur Data Protector. Pour connaître la procédure détaillée pour installer le logiciel à distance, reportez-vous à la section "Installation distante de clients Data Protector" à la page 78.

Dès que les composants client sont installés, le système cible devient automatiquement un élément de la cellule Data Protector.

Connexion d'un périphérique de sauvegarde à un système SCO

Lorsqu'un composant Agent de support est installé sur le système client SCO, procédez comme suit pour relier un périphérique de sauvegarde au système :

1. Recherchez les adresses SCSI encore disponibles en consultant le fichier `/etc/conf/cf.d/mscsi`. Les périphériques SCSI actuellement reliés y sont indiqués.

   Pour plus d'information sur les périphériques pris en charge, reportez-vous au site http://www.hp.com/support/manuals et à la documentation fournie avec chaque périphérique.

2. Eteignez votre ordinateur et connectez le périphérique de sauvegarde au bus SCSI.
3. Redémarrez votre ordinateur.
4. Configurez le périphérique à l'aide de la commande `mkdev tape`. Dans la liste des types de lecteurs de bande, sélectionnez le `lecteur de bande SCSI-1 / SCSI-2 générique`.

   REMARQUE :

   Notez l'ID d'unité, qui s'affiche lorsque vous exécutez la commande `mkdev tape`. Vous en aurez besoin pour reconnaître le nom de fichier du périphérique.

5. Après avoir configuré le périphérique et relancé le système, vous pouvez vérifier, dans le fichier `/etc/conf/cf.d/mscsi`, si le périphérique a été connecté correctement.
6. Sélectionnez le nom de fichier du périphérique approprié dans le répertoire `/dev`.

   Utilisez le nom `nrStp#`, dans lequel # représente l'ID D'UNITE du périphérique. L'ID D'UNITE du périphérique est définie à l'Étape 4 à la page 117. Le nom de fichier de périphérique `/dev/nrStp#` est expliqué à la Figure 23 à la page 118.

ATTENTION :

Utilisez uniquement des fichiers de périphérique du type sans rembobinage avec une taille de bloc variable. Vérifiez si cette taille est variable à l'aide de la commande `tape -s getblk /dev/nrStp#`. La valeur de la taille de bloc variable doit être 0. Si ce n'est pas le cas, utilisez la commande `tape -a 0 setblk /dev/nrStp#` pour définir cette valeur à 0.

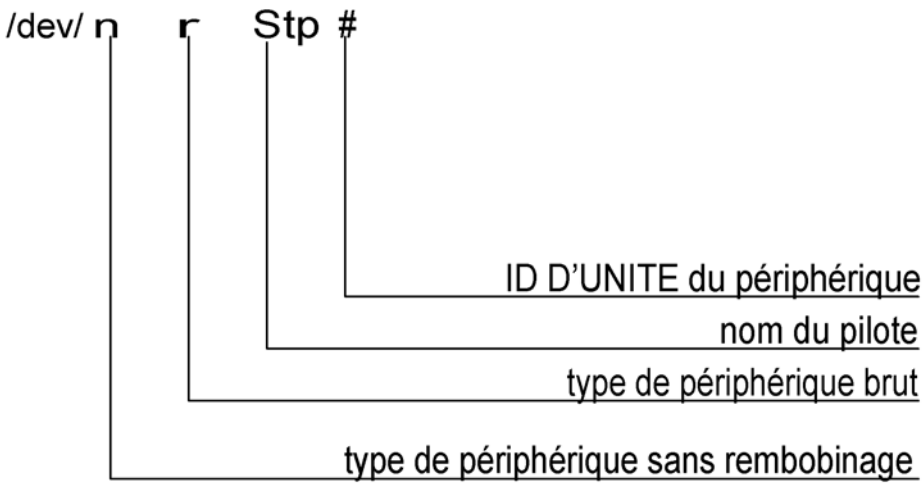

Figure 23 - Format de nom de fichier de périphérique

Etape suivante

Lorsque vous avez terminé l'installation et connecté correctement les périphériques de sauvegarde au système client SCO, reportez-vous à l'index de l'aide en ligne (rubrique "configuration, périphériques de sauvegarde") pour obtenir plus d'informations sur la configuration des périphériques et des pools de supports, ou sur d'autres tâches de configuration.

Installation d'un Agent de support pour l'utilisation de la bibliothèque ADIC/GRAU ou de la bibliothèque StorageTek

Data Protector fournit des stratégies dédiées une bibliothèque ADIC/GRAU ou ACS StorageTek pour configurer une bibliothèque ADIC/GRAU ou une bibliothèque ACS StorageTrek en tant que support de sauvegarde Data Protector. Vous devez installer un Agent de support Data Protector (l'Agent général de support ou l'Agent de support NDMP) sur chaque système qui sera connecté physiquement à un lecteur dans la bibliothèque ADIC/GRAU ou StorageTek. De même, dans le cas de configurations multihôtes, vous devez installer un Agent de support Data Protector sur les systèmes qui commandent le robot de bibliothèque ADIC/GRAU ou StorageTek. Notez que la configuration multihôte est une configuration où bibliothèque et lecteur ne sont pas reliés au même ordinateur.

Pour la bibliothèque ADIC/GRAU, chaque système sur lequel vous installez un Agent de support et qui accède au robot de bibliothèque via le serveur DAS GRAU/ADIC est appelé client DASPour l'intégration STK ACS, chaque système sur lequel vous installez un Agent de support et qui accède au robot de bibliothèque via le serveur STK ACS est appelé client ACS.

REMARQUE :

Vous devez disposer de licences spéciales, qui sont fonction du nombre de lecteurs et d'emplacements utilisés dans la bibliothèque StorageTek. Pour plus d'informations, reportez-vous au Chapitre 5 à la page 307.

Connexion de lecteurs de bibliothèque

Reliez physiquement les lecteurs de bibliothèque aux systèmes sur lesquels vous allez installer un logiciel Agent de support.

Pour plus d'information sur les bibliothèques ADIC/GRAU ou STK prises en charge, reportez-vous au site http://www.hp.com/support/manuals.

Reportez-vous à la section "Installation de clients HP-UX" à la page 94 pour savoir comment connecter physiquement un périphérique de sauvegarde au système. Consultez également la documentation fournie avec la bibliothèque ADIC/GRAU ou StorageTek.

Reportez-vous à la section "Installation de clients Windows" à la page 87 pour savoir comment connecter physiquement un périphérique de sauvegarde à un système Windows pris en charge. Consultez également la documentation fournie avec la bibliothèque ADIC/GRAU ou StorageTek.

Préparation des clients Data Protector à l'utilisation des bibliothèques ADIC/GRAU

La procédure suivante concerne la configuration d'une bibliothèque ADIC/GRAU. Vous devez suivre cette procédure avant d'installer le logiciel Agent de support :

1. Si un serveur DAS est basé sur OS/2, avant de configurer un périphérique de sauvegarde Data Protector ADIC/GRAU, vous devez créer/mettre à jour le fichier `C:\DAS\ETC\CONFIG` sur l'ordinateur serveur DAS. Une liste de tous les clients DAS doit être définie dans ce fichier. Pour Data Protector, cela signifie que chaque client Data Protector autorisé à contrôler le robot doit être défini dans le fichier.

   Chaque client DAS est identifié avec un nom de client unique (sans espace), par exemple `DP_C1`. Dans cet exemple, le contenu du fichier `C:\DAS\ETC\CONFIG` doit ressembler à ceci :

```
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. Sur chaque client Data Protector doté d'un Agent de support Data Protector installé devant accéder aux robots de bibliothèque DAS ADIC/GRAU, modifiez le fichier `omnirc` (fichiers *`répertoire_Data_Protector`*`\omnirc` sous Windows, `/opt/omni/.omnirc` sous HP-UX et Solaris ou `/usr/omni/omnirc` sur AIX) et définissez les variables suivantes :

`DAS_CLIENT`	Un nom unique de client GRAU défini sur le serveur DAS. Par exemple, si le nom du client est "DP_C1", la ligne correspondante dans le fichier `omnirc` est `DAS_CLIENT=DP_C1`.
`DAS_SERVER`	Le nom du serveur DAS.

3. Vous devez savoir comment votre stratégie d'allocation d'emplacement de bibliothèque ADIC/GRAU a été configurée : de manière statique ou dynamique. Reportez-vous au document *AMU Reference Manual* pour savoir comment vérifier le type de stratégie d'allocation que vous utilisez.

   Dans le cadre de la stratégie statique, un emplacement est déterminé pour chaque volser, alors que dans le cadre de la stratégie dynamique, les emplacements sont attribués de manière aléatoire. Vous devez configurer Data Protector en fonction de la stratégie qui a été définie.

   S'il s'agit d'une stratégie d'allocation statique, vous devez ajouter la variable `omnirc` suivante au système contrôlant le robot de la bibliothèque :

   ```
   OB2_ACIEJECTTOTAL = 0
   ```

   REMARQUE :

   Cette opération s'applique aux systèmes HP-UX et Windows.

   Si vous avez d'autres questions sur la configuration de votre bibliothèque ADIC/GRAU, contactez votre support ADIC/GRAU local ou consultez la documentation ADIC/GRAU.

Installation d'un Agent de support pour l'utilisation de la bibliothèque ADIC/GRAU

Configuration système requise

Les conditions préalables à l'installation de l'Agent de support sur un système sont les suivantes :

- La bibliothèque ADIC/GRAU doit être configurée et fonctionner. Consultez la documentation fournie avec la bibliothèque ADIC/GRAU pour en savoir plus à ce sujet.

- Data Protector doit être installé et configuré. Pour connaître la procédure à suivre, reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 42 de ce chapitre.
- Le serveur DAS doit être en cours d'exécution.
  Le logiciel DAS est requis pour contrôler la bibliothèque ADIC/GRAU. Chaque client DAS doit être doté d'un logiciel client DAS installé. Chaque action relative aux supports et aux périphériques lancée par Data Protector est d'abord transférée du client DAS au serveur DAS. Elle est ensuite transmise au module interne (AMU - Unité de gestion de l'AML) de la bibliothèque ADIC/GRAU qui contrôle le robot et déplace ou charge les supports. Lorsqu'une action est terminée, le serveur DAS répond au client DAS. Consultez la documentation fournie avec la bibliothèque ADIC/GRAU pour en savoir plus à ce sujet.
- Vous devez obtenir les informations suivantes avant d'installer l'Agent de support :
  - Le nom d'hôte du serveur DAS (application exécutée sur l'hôte OS/2).
  - La liste des lecteurs disponibles et de leurs noms DAS correspondants. Les noms des lecteurs obtenus doivent être utilisés dans la configuration des lecteurs ADIC/GRAU dans Data Protector.
    Si vous avez défini les clients DAS pour votre système ADIC/GRAU, vous pouvez obtenir cette liste avec les commandes `dasadmin` suivantes :
    `dasadmin listd2` *`client`*
    `dasadmin listd` *`client`*
    où *`client`* représente le client DAS pour lequel les lecteurs réservés doivent être affichés.
    Vous pouvez appeler la commande `dasadmin` depuis le répertoire `C:\DAS\BIN` sur l'hôte OS/2 ou, dans le cas d'une installation sur d'autres systèmes, depuis le répertoire dans lequel le logiciel client DAS a été installé. Sur un système client UNIX, ce répertoire est généralement le répertoire système `/usr/local/aci/bin`.
  - La liste des zones d'insertion/éjection disponibles avec les spécifications de format correspondantes.
    Vous pouvez obtenir la liste de ces zones dans la configuration graphique de l'AMS (Logiciel de gestion de l'AML) d'un hôte OS/2 :
    1. Lancez cette configuration à partir du menu `Admin > Configuration`.

2. Ouvrez la fenêtre Configuration-EIF en cliquant deux fois sur l'icône de l'unité d'E/S, puis cliquez sur le champ Plages logiques. Les zones d'insertion/éjection disponibles sont énumérées dans la zone de texte.

REMARQUE :

Un périphérique de bibliothèque Data Protector ne peut gérer qu'un seul type de support. Il est important de se rappeler quel type de support appartient à chacune des zones d'insertion et d'éjection spécifiées, car vous aurez par la suite besoin de ces données pour configurer les zones d'insertion/éjection de la bibliothèque Data Protector.

- Une liste de fichiers de périphérique UNIX pour les lecteurs, si vous souhaitez installer l'Agent de support sur un système UNIX.
  Exécutez la commande système `ioscan -fn` sur votre système pour afficher les informations requises.
  Pour obtenir plus d'informations sur les fichiers de périphérique UNIX, reportez-vous à la section "Connexion d'un périphérique de sauvegarde aux systèmes HP-UX" à la page 96.
- Une liste d'adresses SCSI pour les lecteurs, si vous souhaitez installer l'Agent de support sur un système Windows. Par exemple, `scsi4:0:1:0`.
  Pour obtenir plus d'informations sur les adresses SCSI, reportez-vous à la section "Connexion d'un périphérique de sauvegarde aux systèmes Windows" à la page 92.

Installation

La procédure d'installation est la suivante :

1. Distribuez le composant Agent de support aux clients à l'aide de l'interface graphique utilisateur Data Protector et du Serveur d'installation. Pour connaître la procédure à suivre, reportez-vous à la section "Installation distante de clients Data Protector" à la page 78 de ce chapitre.
2. Installez la bibliothèque ADIC/GRAU :
   - Avec un système Windows, procédez comme suit :
     a. Copiez les bibliothèques `aci.dll`, `winrpc32.dll` et `ezrpc32.dll` dans le répertoire *`répertoire_Data_Protector`*`\bin`. (Ces trois bibliothèques font partie du logiciel client DAS livré avec la bibliothèque ADIC/GRAU ; vous pouvez les trouver sur le support d'installation ou dans le répertoire `C:\DAS\AMU\` de l'AMU-PC).
     b. Copiez également ces trois fichiers dans le répertoire *`%SystemRoot%`*`\system32`.

c. Copiez `Portinst` et le `service Portmapper` dans le client DAS (ces éléments font partie du logiciel client DAS livré avec la bibliothèque ADIC/GRAU ; vous les trouverez sur le support d'installation).

d. Dans le Panneau de configuration, ouvrez `Outils d'administration, Services` et lancez `portinst` pour installer `portmapper`. Vous devez relancer le client DAS pour exécuter le service `portmapper`.

e. Après avoir réamorcé le système, vérifiez que `portmapper` et les deux `services rpc` sont exécutés (dans le Panneau de configuration, ouvrez Outils d'administration, Services et vérifiez l'état des services).

- Sur un système HP-UX, copiez la bibliothèque partagée `libaci.sl` dans le répertoire `/opt/omni/lib`. Vous devez avoir les autorisations nécessaires pour accéder à ce répertoire. Vérifiez que la bibliothèque partagée dispose bien des autorisations de lecture et d'exécution pour tout le monde (root, groupe et autre). La bibliothèque partagée `libaci.sl` fait partie du logiciel client DAS livré avec la bibliothèque ADIC/GRAU ; vous la trouverez sur le support d'installation.
- Sur un système AIX, copiez la bibliothèque partagée `libaci.sl` dans le répertoire `/usr/omni/lib`. Vous devez avoir les autorisations nécessaires pour accéder à ce répertoire. Vérifiez que la bibliothèque partagée dispose bien des autorisations de lecture et d'exécution pour tout le monde (root, groupe et autre). La bibliothèque partagée `libaci.o` fait partie du logiciel client DAS livré avec la bibliothèque ADIC/GRAU ; vous la trouverez sur le support d'installation.

A ce stade de la procédure, votre matériel doit être relié et le logiciel DAS doit être installé correctement.

Exécutez la commande suivante pour savoir si les lecteurs de bibliothèque sont reliés correctement à votre ordinateur :

- *Sous Windows* : *`répertoire_Data_Protector`*`\bin\devbra -dev`
- *Sous HP-UX* : `/opt/omni/lbin/devbra -dev`
- *Sous AIX* : `/opt/omni/lbin/devbra -dev`

Vous devez voir dans la liste les lecteurs de bibliothèque et leurs fichiers de périphérique correspondants.

Etape suivante

Une fois un Agent de support installé et la bibliothèque ADIC/GRAU connectée physiquement au système, reportez-vous à l'index de l'aide en ligne (rubrique "configuration, périphériques de sauvegarde") pour obtenir des informations sur d'autres tâches de configuration, telles que la configuration des périphériques de sauvegarde et des pools de supports.

Préparation des clients Data Protector à l'utilisation des bibliothèques StorageTek

Les conditions préalables requises pour l'installation d'un Agent de support sont les suivantes :

- La bibliothèque StorageTek doit être configurée et en cours d'exécution. Consultez la documentation fournie avec cette bibliothèque.
- Data Protector doit être installé et configuré. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 42.
- Vous devez obtenir les informations suivantes avant de commencer à installer un logiciel Agent de support :
  - Le *nom de l'hôte* sur lequel ACSLS est en cours d'exécution.
  - Une liste d'ID de lecteurs ACS que vous souhaitez utiliser avec Data Protector. Les ID des lecteurs obtenus doivent être utilisés dans la configuration des lecteurs StorageTek dans Data Protector. Pour afficher cette liste, connectez-vous à l'hôte où ACSLS est en cours d'exécution, puis exécutez la commande suivante :
    `rlogin "ACSLS hostname" -l acssa`
    Vous devrez entrer le type du terminal et attendre l'invite de commande. A l'invite ACSSA, entrez la commande suivante :
    `ACSSA> query drive all`
    La spécification de format d'un lecteur ACS doit être la suivante :
    `ACS DRIVE: ID:#,#,#,# - (ACS num, LSM num, PANEL, DRIVE)`
  - Une liste d'ID DE CAP ACS disponibles avec leur spécification de format. Pour afficher cette liste, connectez-vous à l'hôte où ACSLS est en cours d'exécution, puis exécutez la commande suivante :
    `rlogin "ACSLS hostname" -l acssa`
    Vous devrez entrer le type du terminal et attendre l'invite de commande. A l'invite ACSSA, entrez la commande suivante :
    `ACSSA> query cap all`
    La spécification de format de CAP ACS doit être la suivante :
    `ACS CAP: ID:#,#,# - (ACS num, LSM num, CAP num)`
  - Une liste de fichiers de périphérique UNIX pour les lecteurs, si vous souhaitez installer l'Agent de support sur un système UNIX.
    Exécutez la commande système `ioscan -fn` sur votre système pour afficher les informations requises.
    Pour obtenir plus d'informations sur les fichiers de périphérique UNIX, reportez-vous à la section "Connexion d'un périphérique de sauvegarde aux systèmes HP-UX" à la page 96.
  - Une liste d'adresses SCSI pour les lecteurs, si vous souhaitez installer l'Agent de support sur un système Windows. Par exemple, `scsi4:0:1:0`.

Pour obtenir plus d'informations sur les adresses SCSI, reportez-vous à la section "Connexion d'un périphérique de sauvegarde aux systèmes Windows" à la page 92.

- Vérifiez que les lecteurs qui vont être utilisés pour Data Protector sont bien à l'état `en ligne`. Si un lecteur n'est pas `en ligne`, changez l'état à l'aide de la commande suivante sur l'hôte ACSLS : `vary drive` *`id_lecteur`* `online`
- Vérifiez que les CAP qui seront utilisés pour Data Protector sont à l'état `en ligne` et en mode de fonctionnement `manuel`.
  Si un CAP n'est pas dans l'état `en ligne`, changez l'état avec la commande suivante : `vary cap` *`id_cap`* `online`
  Si un CAP n'est pas en mode de fonctionnement `manuel`, changez le mode avec la commande suivante : `set cap manual` *`id_cap`*

Installation d'un Agent de support pour l'utilisation de la bibliothèque StorageTek

La procédure d'installation est la suivante :

1. Distribuez le composant Agent de support aux clients à l'aide de l'interface graphique utilisateur Data Protector et du Serveur d'installation pour UNIX. Pour connaître la procédure à suivre, reportez-vous à la section "Installation distante de clients Data Protector" à la page 78 de ce chapitre.
2. Exécutez le démon ACS `ssi` pour chaque client ACS :
   - Sur des clients HP-UX, Solaris et Linux, exécutez la commande suivante : `/opt/omni/acs/ssi.sh start` *`nom_hôte_LS_ACS`*
   - Sur des clients ACS Windows, installez le service `LibAttach`. Pour plus de détails à ce sujet, reportez-vous à la documentation ACS. Vérifiez que le nom d'hôte d'ACSLS approprié est entré pendant la configuration du service `LibAttach`. Au terme d'une configuration réussie, les services `LibAttach` sont lancés automatiquement. Ils seront également lancés automatiquement après chaque réamorçage.
   - Sur des clients ACS AIX, exécutez la commande suivante : `/usr/omni/acs/ssi.sh start` *`nom_hôte_LS_ACS`*

REMARQUE :

Après avoir installé le service `LibAttach`, vérifiez si le répertoire `libattach\bin` a été ajouté automatiquement au chemin d'accès du système. Si ce n'est pas le cas, ajoutez-le manuellement.

Pour plus d'informations sur le service `LibAttach`, consultez la documentation fournie avec la bibliothèque StorageTek.

3. Exécutez la commande suivante pour vérifier si les lecteurs de bibliothèque sont reliés correctement à votre ordinateur :
   - Sur un client HP-UX, Solaris et Linux : `/opt/omni/lbin/devbra -dev`
   - Sur un client ACS Windows : `répertoire_Data_Protector\bin\devbra -dev`
   - Sur un client ACS AIX : `/opt/omni/lbin/devbra -dev`

   Vous devez voir apparaître dans la liste les lecteurs de bibliothèque et leurs fichiers de périphérique/adresses SCSI correspondant(e)s.

Etape suivante

Une fois un Agent de support installé et la bibliothèque StorageTek connectée physiquement au système, reportez-vous à l'index de l'aide en ligne (rubrique "configuration, périphériques de sauvegarde") pour obtenir des informations sur d'autres tâches de configuration, telles que la configuration des périphériques de sauvegarde et des pools de supports.

Installation locale de clients Novell NetWare

Vous devez effectuer l'installation du système client Novell NetWare à partir d'un système Windows pris en charge et connecté au réseau Novell.

Vous pouvez installer l'Agent de disque et l'Agent général de support Data Protector sur les systèmes exécutant Novell NetWare. Pour obtenir des informations sur les composants Data Protector, reportez-vous à la section "Composants Data Protector" à la page 73.

Pour des détails sur les périphériques pris en charge et les versions de plate-forme Novell NetWare, ainsi que sur les problèmes connus et leurs solutions, consultez les *Références, notes de publication et annonces produits HP Data Protector*.

Configuration système requise

Avant d'installer Data Protector sur la plate-forme Novell NetWare, vérifiez les éléments suivants :

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- Le protocole de transport TCP/IP doit être installé et en état de fonctionnement.
- Assurez-vous que l'un des services suivants est en cours d'exécution sur le système Windows :
  - Service passerelle pour Novell NetWare.
    Ce service doit s'exécuter sur Windows lorsqu'une installation est exécutée à partir du serveur Windows.
  - Client Novell pour Windows ou service client Microsoft pour NetWare.

Ce service doit s'exécuter sur Windows lorsqu'une installation est exécutée à partir de la station de travail Windows.

- Connectez-vous au serveur NetWare cible (ou à l'arborescence NDS/eDirectory appropriée) à partir du système Windows.
- Vérifiez que vous disposez bien des droits de superviseur pour le volume SYS : sur le serveur NetWare cible.
- Assurez-vous qu'au moins un nom de périphérique local est libre sur le système Windows.

Clients compatibles cluster

D'autres conditions sont requises pour l'installation de clients compatibles cluster. Pour plus de détails, reportez-vous à la section "Installation d'un client" à la page 201.

Installation

La procédure d'installation peut s'effectuer à partir du DVD-ROM Windows de Data Protector. Notez que l'installation de Novell NetWare ne fait pas partie des fonctionnalités du Serveur d'installation.

Procédez comme suit pour installer Data Protector sur le serveur Novell NetWare :

1. Exécutez une invite de commande sur votre système Windows et indiquez comme chemin d'accès le répertoire racine du DVD-ROM.
2. Exécutez le script d'installation.

   Pour installer le client Novell NetWare Data Protector, modifiez le chemin d'accès au répertoire `NetWare` et tapez :

   `NWInstall` *`nom du serveur cible`* `ALL|DA|MA` *`numéro_port`*

   Le deuxième paramètre permet de déterminer la partie du client Novell de Data Protector qui va être installée :

   - Tapez `ALL` pour installer l'intégralité des fonctionnalités du client Novell NetWare Data Protector.
   - Tapez `DA` pour installer l'Agent de disque Data Protector pour Novell NetWare uniquement.
   - Tapez `MA` pour installer l'Agent général de support Data Protector pour Novell NetWare uniquement.

REMARQUE :

Pour l'installation de Data Protector sur chaque version de Novell NetWare, le numéro de port est facultatif. Si vous ne le spécifiez pas, le numéro de port par défaut qui sera utilisé est 5555.

Si la version de votre système d'exploitation Novell NetWare n'est pas prise en charge par Data Protector, l'installation est toujours possible mais vous recevez un avertissement en conséquence.

Une vérification est maintenant effectuée pour déterminer si les fichiers Data Protector sont déjà sur le serveur cible. Si c'est le cas, l'installation précédente de Data Protector sera déplacée vers le répertoire `SYS:\usr\Omni.old`.

En fonction de la version de client NetWare installée, vérifiez si `OMNIINET.NLM`, `HPINET.NLM` ou `HPBRAND.NLM` est en cours d'exécution sur le serveur. Si l'un de ces programmes est en cours d'exécution, déchargez-le en tapant la commande suivante au niveau de la console Novell NetWare :

`UNLOAD HPINET` (`UNLOAD OMNIINET` / `UNLOAD HPBRAND`)

L'installation crée automatiquement une structure de répertoires Data Protector et copie tous les fichiers Data Protector sur le serveur cible.

3. Avant de continuer, assurez-vous que les modules suivants sont chargés sur votre système :
   - `NETDB.NLM`
   - `TSAFS.NLM`
   - `TSANDS.NLM`

   Vous permettez ainsi au chargeur de résoudre les symboles publics tout en essayant de charger `HPINET.NLM`.

   Si vous avez configuré Novell NetWare Cluster Services sur votre système Novell NetWare 6.x, vérifiez que vous avez chargé le module `NCSSDK.NLM`.

4. Pour charger `HPINET.NLM`, tapez la commande suivante sur la console Novell NetWare :

   ```
   SEARCH ADD SYS:USR\OMNI\BIN
   ```

   ```
   LOAD HPINET.NLM
   ```

REMARQUE :

Si vous n'utilisez pas le port par défaut 5555, spécifiez le numéro de port en ajoutant l'option `-port` *`numéro_port`* à la commande `LOAD`. Par exemple :

`LOAD HPINET.NLM -port` *`numéro_port`*

Pour activer la reconnaissance automatique du Gestionnaire de cellule Data Protector par le serveur Novell NetWare, l'installation ajoutera automatiquement les commandes de la console au fichier `AUTOEXEC.NCF`, afin que le fichier `HPINET.NLM` soit toujours chargé et prêt à se connecter au Gestionnaire de cellule Data Protector.

REMARQUE :

Vérifiez le fichier `AUTOEXEC.NCF` une fois l'installation terminée. Si les commandes console nécessaires n'ont pas été ajoutées à ce fichier durant l'installation, vous devez les ajouter manuellement.

Pour permettre la sauvegarde et la restauration de la base de données `NDS/eDirectory`, suivez les étapes ci-dessous :

1. Définissez le compte d'utilisateur à utiliser lors de la sauvegarde ou de la restauration de NDS/eDirectory.
2. A partir de la console Novell NetWare, chargez le module `HPLOGIN.NLM` :

   ```
   LOAD HPLOGIN.NLM
   ```

3. Fournissez les informations utilisateur suivantes au fichier `HPLOGIN.NLM` pour réussir la connexion à la base de données `NDS/eDirectory` :
   - Contexte NDS/eDirectory :
     Ce contexte décrit le conteneur où résident les objets utilisateur. La syntaxe du nom de ce conteneur doit être une syntaxe de nom unique. Par exemple :
     `OU=SDM.O=HSL`
   - Nom d'objet NDS/eDirectory :
     Il s'agit du nom commun de l'objet utilisateur qui sera utilisé comme utilisateur NDS/eDirectory valide pour la connexion à la base de données NDS/eDirectory lorsque l'Agent de disque Data Protector effectue une sauvegarde ou une restauration des NDS/eDirectory. L'utilisateur sélectionné doit se trouver dans le contexte appliqué précédemment. Par exemple :
     `CN=MarcJ`
     si le nom unique de l'utilisateur sélectionné a pour syntaxe
     `.CN=MarcJ.OU=SDM.O=HSL`.
   - Mot de passe d'objet NDS/eDirectory :
     Il s'agit d'un mot de passe utilisateur valide utilisé avec le nom d'utilisateur pour la connexion à la base de données NDS/eDirectory lorsqu'une sauvegarde ou une restauration de cette dernière est lancée.
     Les informations utilisateur saisies dans le module `HPLOGIN` sont encodées et stockées dans le répertoire `SYS:SYSTEM`. Il est également utilisé en association avec les modules Novell NetWare SMS qui doivent être chargés et qui doivent fonctionner.

REMARQUE :

Le compte utilisateur sélectionné dans le module `HPLOGIN` doit disposer des droits d'exécution de sauvegarde et de restauration de la base de données NDS/eDirectory.

Si certaines modifications sont apportées à l'objet NDS/eDirectory utilisé (déplacement vers un autre conteneur, suppression, attribution

d'un nouveau nom, changement de mot de passe), les informations encodées dans le répertoire `SYS:SYSTEM` doivent être mises à jour dans le module `HPLOGIN`.

4. Pour sauvegarder et restaurer NDS/eDirectory auprès des services Novell NetWare de gestion du stockage `(SMS)`, les modules `SMDR.NLM` et `TSANDS.NLM` doivent être chargés sur au moins un serveur de l'arborescence `NDS/eDirectory`. Vous pouvez télécharger les dernières versions de `TSANDS.NLM` et `SMDR.NLM` à partir du Web à l'adresse http://support.novell.com/filefinder/.

   La ligne `LOAD TSANDS.NLM` est ajoutée automatiquement au fichier `AUTOEXEC.NCF` , ce qui permet au serveur Novell NetWare de reconnaître immédiatement `TSANDS.NLM`. Le module Novell NetWare `SMS SMDR.NLM` est chargé dès que `TSANDS.NLM` est chargé.

REMARQUE :

Si, au cours de l'installation, les commandes console n'ont pas été ajoutées au fichier `AUTOEXEC.NCF`, vous devez les ajouter manuellement.

CONSEIL :

Pour réduire au minimum le trafic réseau pendant le processus de sauvegarde, chargez les modules sur le serveur contenant une réplique de la plus grande partition `NDS/eDirectory`.

Vous avez maintenant terminé les opérations nécessaires à la sauvegarde et la restauration des `NDS/eDirectory`. Reportez-vous à l'index de l'aide en ligne (rubrique "configuration") pour obtenir des instructions sur les autres tâches de configuration.

Configuration de l'Agent de support

A ce stade de la procédure, tous les composants Data Protector sont déjà installés. Toutefois, si vous avez sélectionné `ALL` ou le paramètre `MA` au début de la procédure d'installation, vous devez effectuer quelques opérations de configuration supplémentaires pour permettre à l'Agent général de support de Data Protector d'utiliser les périphériques de sauvegarde connectés au serveur Novell NetWare.

Data Protector prend en charge l'adaptateur hôte SCSI `Adaptec` et le pilote `.HAM` correspondant. L'agent de support Data Protector peut communiquer directement avec le pilote `.HAM` afin d'accéder à l'adaptateur hôte SCSI. Par conséquent, vous devez installer le pilote de l'adaptateur hôte SCSI. Vous pouvez télécharger les dernières versions des pilotes `Adaptec` à partir du site Web http://www.adaptec.com.

Le pilote peut être chargé automatiquement lorsque vous redémarrez le serveur si vous ajoutez une commande `LOAD` au fichier `STARTUP.NCF`. La commande doit préciser la situation du pilote, toutes les options disponibles et le numéro d'emplacement.

Reportez-vous au document *Adaptec Driver User's Guide* d'Adaptec pour obtenir la liste des options disponibles et déterminer les numéros d'emplacement.

Exemple

Pour charger automatiquement le pilote `AHA-2940 Adaptec` sur le serveur Novell NetWare 6.x chaque fois que celui-ci est redémarré, ajoutez les lignes suivantes au fichier `STARTUP.NCF` :

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

où `SLOT` représente l'emplacement de l'adaptateur de périphérique sur le système hôte et `lun_enable` est un masque permettant l'analyse de LUN (Numéros d'unité logique) spécifiques sur toutes les cibles.

Pour toutes les adresses SCSI, une analyse de chaque LUN est activée ; le bit à la position correspondante est à 1. Par exemple, `lun_enable=03` permet l'analyse de LUN 0 et 1 sur toutes les cibles.

REMARQUE :

`lun_enable` ne doit être spécifié que si vous utilisez des périphériques ayant des LUN SCSI supérieurs à 0 ; lorsque vous configurez le périphérique de bibliothèque HP StorageWorks Tape 12000e, par exemple.

CONSEIL :

Pour rechercher automatiquement tous les périphériques connectés au serveur Novell NetWare et leurs LUN associés à chaque redémarrage du serveur, ajoutez les lignes suivantes au fichier `AUTOEXEC.NCF` :

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

La configuration de l'Agent général de support est maintenant terminée.

Etape suivante

Une fois que le logiciel Agent général de support Data Protector est installé correctement sur la plate-forme Novell NetWare, il est conseillé de vérifier son installation. Reportez-vous à la section "Vérification de l'installation de l'Agent général de support sous Novell NetWare" à la page 436.

Après avoir vérifié l'installation, vous pouvez importer le client Novell NetWare dans la cellule Data Protector à l'aide de l'interface graphique utilisateur Data Protector.

Reportez-vous à l'index de l'aide en ligne (rubrique "Novell NetWare") pour plus d'informations sur les autres tâches de configuration.

Installation locale de clients HP OpenVMS

La procédure d'installation des clients OpenVMS doit être exécutée en local sur un système OpenVMS pris en charge. L'installation à distance n'est pas prise en charge.

Vous pouvez installer l'Agent de disque, l'Agent général de support et l'interface utilisateur (interface de ligne de commande uniquement) de Data Protector sur des systèmes OpenVMS 7.3-2/IA64 8.2-1. Vous pouvez également installer le composant Intégration Oracle sur des systèmes utilisant OpenVMS I64 version 7.3-1 ou supérieure. Pour obtenir des informations sur les composants Data Protector, reportez-vous à la section "Composants Data Protector" à la page 73.

Pour obtenir des informations sur les périphériques pris en charge et les versions de plate-forme OpenVMS, ainsi que sur les limites, les problèmes connus et leurs solutions, consultez les *Références, notes de publication et annonces produits HP Data Protector* .

Pour des informations plus précises sur OpenVMS, consultez le document *OpenVMS Release Notes* disponible dans le répertoire des documents d'aide par défaut sous OpenVMS, par exemple : `SYS$COMMON:[SYSHLP]DPA0610.RELEASE_NOTES`.

Configuration système requise

Avant d'installer un client Data Protector sur la plate-forme OpenVMS, vérifiez les éléments suivants :

- Le protocole de transport HP TCP/IP doit être installé et actif.
- Définissez les caractéristiques TIMEZONE de votre système en exécutant la commande `SYS$MANAGER:UTC$TIME_SETUP.COM`.
- Connectez-vous au compte `SYSTEM` du système OpenVMS. Notez que vous devez disposer des autorisations appropriées.
- Vérifiez que vous avez accès au DVD-ROM d'installation de Data Protector contenant le package d'installation du client OpenVMS.

Installation

La procédure d'installation peut s'effectuer à partir du DVD-ROM d'installation Windows de Data Protector. Notez que l'installation de OpenVMS ne fait pas partie des fonctionnalités du Serveur d'installation.

Pour installer un client Data Protector sur un système OpenVMS, procédez comme suit :

1. Si vous disposez déjà d'un fichier d'installation PCSI, passez à l'Étape 2 à la page 133. Pour obtenir le fichier d'installation PCSI, montez le DVD-ROM d'installation sur un système OpenVMS Server et copiez le fichier à l'endroit désiré. Vous pouvez également utiliser FTP pour récupérer le fichier PCSI à partir d'un système Windows.

2. Exécutez la commande suivante :

   `$ PRODUCT INSTALL DP /SOURCE=`*`unité`*`:[`*`répertoire`*`]`

   où *`unité`*`:[`*`répertoire`*`]` est l'emplacement du fichier d'installation .PCSI.

3. Vérifiez la version du kit en répondant `YES` à l'invite :

   `The following product has been selected:` HP AXPVMS DP A06.10-xx Layered Product Do you want to continue? [YES]

4. Sélectionnez les composants logiciels à installer. Si vous choisissez l'installation par défaut, l'Agent de disque, l'Agent général de support et l'Interface utilisateur seront installés. Vous pouvez également sélectionner chaque composant séparément.

   Vous devrez choisir les options (le cas échéant) pour chaque produit sélectionné et pour tout produit pouvant être installé afin de satisfaire aux exigences en matière de dépendance des logiciels.

Exemple

```
HP IA64VMS DP A6.10-xx: HP OpenVMS IA64 Data Protector
V6.10

COPYRIGHT HEWLETT-PACKARD COMPANY 2007

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 A6.10-xx: HP OpenVMS IA64 Data Protector
V6.10 [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
```

L'emplacement par défaut des répertoires et fichiers de Data Protector est le suivant :

```
SYS$SYSDEVICE:[VMS$COMMON.OMNI]
```

La structure de répertoires sera créée automatiquement et les fichiers placés dans cette arborescence.

Les procédures liées aux commandes de démarrage et d'arrêt de Data Protector seront placées dans

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

Pour un client OpenVMS, il existe toujours quatre fichiers ; il existera un cinquième fichier uniquement si vous choisissez l'option CLI. Il s'agit des cinq fichiers suivants :

- `SYS$STARTUP:OMNI$STARTUP.COM` Procédure de commande qui démarre Data Protector sur ce nœud.
- `SYS$STARTUP:OMNI$SYSTARTUP.COM` Procédure de commande qui définit le nom logique `OMNI$ROOT`. Les autres noms logiques requis par ce client peuvent être ajoutés à cette procédure de commande.
- `SYS$STARTUP:OMNI$SHUTDOWN.COM` Procédure de commande qui arrête Data Protector sur ce nœud.
- `OMNI$ROOT:[BIN]OMNI$STARTUP_INET.COM` Procédure de commande utilisée pour démarrer le processus `TCP/IP INET`, qui exécute ensuite les commandes envoyées par le Gestionnaire de cellule.
- `OMNI$ROOT:[BIN]OMNI$CLI_SETUP.COM` Procédure de commande qui définit les symboles nécessaires pour appeler l'interface de ligne de commande (CLI) de Data Protector. Elle ne sera disponible sur le système que si vous avez choisi l'option CLI pendant l'installation.
  Exécutez cette procédure de commande à partir des procédures `login.com` pour tous les utilisateurs qui utiliseront l'interface de ligne de commande. Plusieurs noms logiques sont définis dans cette procédure ; ils sont nécessaires pour l'exécution correcte des commandes CLI.

5. Insérez la ligne suivante dans `SYS$MANAGER:SYSTARTUP_VMS.COM` :

   `@sys$startup:omni$startup.com`

6. Insérez la ligne suivante dans `SYS$MANAGER:SYSHUTDWN.COM` :

   `@sys$startup:omni$shutdown.com`

7. Vérifiez que vous pouvez vous connecter depuis le client OpenVMS à tous les alias TCP/IP possibles pour le Gestionnaire de cellule.

8. Importez le client OpenVMS dans la cellule Data Protector en utilisant l'interface graphique utilisateur de Data Protector comme indiqué dans la section "Importation de clients dans une cellule" à la page 205.

Un compte portant le nom OMNIADMIN est créé au cours de l'installation. Le service `OMNI` s'exécute sous ce compte.

Le répertoire de connexion pour ce compte est `OMNI$ROOT:[LOG]` et il contient le fichier journal `OMNI$STARTUP_INET.LOG` pour chaque démarrage d'un composant Data Protector. Ce fichier journal contient le nom du processus exécutant la requête, le nom de l'image de Data Protector utilisée et les options de la requête.

Toutes les erreurs inattendues sont consignées dans le fichier `DEBUG.LOG` de ce répertoire.

REMARQUE :

Sous OpenVMS 8.3 (et versions supérieures), le programme d'installation de Data Protector affiche le message suivant :

```
%PCSI-I-CANNOTVAL, cannot validate [PATH]HP-AXPVMS-DP-A0610-
XXX-1.PCSI;1
-PCSI-I-NOTSIGNED, product kit is not signed and therefore
has no manifest file
```

Pour éviter ce message, exécutez la commande d'installation du produit avec `/OPTION=NOVALIDATE_KIT`.

Installation dans un environnement de cluster

Si vous utilisez un disque système commun, il suffit d'installer une seule fois le logiciel client. Toutefois, la procédure `OMNI$STARTUP.COM` doit être exécutée pour chaque nœud pour être utilisable comme client Data Protector. Si vous n'utilisez pas de disque système commun, le logiciel client doit être installé sur chaque client.

Si vous utilisez un nom d'alias TCP/IP pour le cluster, vous pouvez également définir un client pour le nom d'alias si vous utilisez un disque système commun pour le cluster. Lorsque le client alias est défini, il n'est plus nécessaire de configurer individuellement chaque nœud client. Vous avez alors le choix entre la définition du client et la définition de l'alias pour exécuter les sauvegardes et restaurations dans un cluster. Selon votre

configuration, la sauvegarde ou la restauration peuvent ou non utiliser un chemin d'accès direct vers votre lecteur de bande ou votre bibliothèque de bandes.

Configuration de l'Agent de disque

L'Agent de disque Data Protector pour OpenVMS prend en charge les volumes de disque `FILES-11 ODS-2` et `ODS-5` montés. Il n'est pas nécessaire de configurer l'Agent de disque OpenVMS. Il faut cependant avoir à l'esprit certains points lorsque vous configurez une spécification de sauvegarde qui l'utilisera. Ceux-ci sont décrits ci-dessous :

- Les spécifications de fichier saisies dans l'interface graphique utilisateur ou transmis à l'interface de ligne de commande doivent être énoncées dans une syntaxe de type UNIX, comme par exemple :
  `/disque/répertoire1/répertoire2/.../nomfichier.ext.n`
  - La chaîne doit commencer par une barre de fraction, suivie du lecteur, des noms de répertoire et du nom de fichier, séparés par des barres de fraction.
  - Le nom du lecteur ne doit pas être suivi d'un deux-points.
  - Utilisez un point devant le numéro de version plutôt qu'un point-virgule.
  - Les spécifications de fichier pour les fichiers OpenVMS ne sont pas sensibles à la casse, excepté pour les fichiers résidant sur les disques `ODS-5`.

Exemple

Une spécification de fichier OpenVMS :

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

doit être spécifiée à Data Protector sous la forme :

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

REMARQUE :

Il n'existe pas de numéro de version implicite. Vous devez toujours spécifier un numéro de version et seule la version de fichier spécifiée pour la sauvegarde sera sauvegardée.

Pour certaines options, qui autorisent l'emploi des caractères génériques, le numéro de version peut être remplacé par un astérisque "*".

Si vous souhaitez inclure toutes les versions du fichier dans une sauvegarde, vous devez les sélectionner toutes dans l'interface graphique utilisateur ou dans l'interface de ligne de commande. Ajoutez les spécifications de fichier sous l'option `-only`, en utilisant des caractères génériques pour le numéro de version, comme suit :

```
/DKA1/rep1/nomfichier.txt.*
```

Configuration de l'Agent de support

Vous devez configurer les périphériques sur votre système OpenVMS en prenant pour guide la documentation OpenVMS et celle relative au matériel. Les pseudo-périphériques pour la bibliothèque de bandes doivent être créés en premier à l'aide de SYSMAN, comme suit :

```
$ RUN SYS$SYSTEM:SYSMAN

SYSMAN&gt; IO CONNECT gcan/NOADAPTER/DRIVER=SYS$GcDRIVER
```

où :

- `c` = K pour les bibliothèques de bandes SCSI à connexion directe.
- `a` = A,B,C, …lettre de l'adaptateur pour le contrôleur SCSI.
- `n` = numéro d'unité du robot de la bibliothèque de bandes.

REMARQUE :

Cette séquence de commandes doit être exécutée après le redémarrage du système.

Pour les bibliothèques de bandes reliées à un réseau SAN, les lecteurs de bande et le nom du robot s'affichent automatiquement sous OpenVMS une fois que les périphériques SAN ont été configurés conformément aux instructions SAN.

Si vous installez des bibliothèques de bandes magnéto-optiques pour les utiliser avec Data Protector, vous devez vérifier que ce matériel fonctionne correctement avant de le configurer dans Data Protector. Pour vérifier le matériel, vous pouvez utiliser l'utilitaire MRU (Media Robot Utility), fourni par Hewlett-Packard.

REMARQUE :

Vous pouvez généralement utiliser l'interface graphique utilisateur de Data Protector pour configurer manuellement ou auto-configurer ces périphériques.

Certaines bibliothèques de bandes plus anciennes ainsi que toutes les bibliothèques de bandes connectées aux contrôleurs HSx ne peuvent toutefois pas être auto-configurées. Utilisez les méthodes de configuration manuelle pour ajouter ces périphériques à Data Protector.

Agent de support sur un cluster

Avec les périphériques reliés aux systèmes de cluster :

1. Configurez chaque lecteur et bibliothèque de bande pour qu'il puisse être accessible à partir de tous les nœuds.
2. Ajoutez le nom du nœud à la fin du nom du périphérique pour le différencier.

3. Pour les périphériques à bande, définissez un `nom de verrouillage de périphérique` dans `Devices/Properties/Settings/Advanced/Other`.

Exemple

Dans un cluster comportant les nœuds A et B, un TZ89 est connecté au nœud A et relié comme serveur au nœud B par protocole MSCP. Configurez un périphérique nommé `TZ89_A`, avec le nœud A comme client et configurez un périphérique nommé `TZ89_B`, avec le nœud B comme client. Les deux périphériques obtiennent le nom de verrouillage de périphérique commun `TZ89`. Data Protector peut alors utiliser les périphériques par chacun des chemins d'accès, tout en les reconnaissant comme un périphérique unique. Si vous exécutez une sauvegarde sur le noeud B avec `TZ89_A`, Data Protector transfère les données du noeud B au périphérique sur le noeud A. Si vous exécutez une sauvegarde sur le noeud B avec `TZ89_B`, le serveur MSCP OpenVMS transfère au périphérique sur le noeud A les données du noeud B.

REMARQUE :

Pour les périphériques à bande reliés à un serveur par MSCP ou connectés via un contrôleur HSx ou via Fibre Channel, suivez les instructions relatives aux configurations SAN indiquées dans l'index de l'aide en ligne (rubrique "SAN, configuration de périphériques").

Interface de ligne de commande

Avant de pouvoir utiliser l'interface de ligne de commande de Data Protector sous OpenVMS, vous devez exécuter la procédure d'installation de la commande CLI, comme suit :

`$ @OMNI$ROOT:[BIN]OMNI$CLI_SETUP.COM` Pour une description des commandes CLI disponibles, reportez-vous au *Guide de rfrence de l'interface de ligne de commande HP Data Protector*.

Intégration Oracle

Après avoir installé l'intégration Oracle et l'avoir configurée comme décrit dans le *Guide d'intégration HP Data Protector pour Oracle et SAP*, vérifiez que l'entrée `-key Oracle8` figure dans le fichier `OMNI$ROOT:[CONFIG.CLIENT]omni_info`, par exemple :

```
-key oracle8 -desc "Oracle Integration" -nlsset 159 -nlsId
12172 -flags 0x7 -ntpath "" -uxpath "" -version A.06.10
```

Si l'entrée est absente, copiez-la dans le fichier `OMNI$ROOT:[CONFIG.CLIENT]omni_format`. Sinon, l'installation de l'intégration Oracle ne sera pas indiquée sur le client OpenVMS.

Etape suivante

Reportez-vous à l'index de l'aide en ligne (rubrique "HP OpenVMS") pour plus d'informations sur les autres tâches de configuration.

Installation de clients MPE/iX

Reportez-vous au *Guide de l'utilisateur MPE/iX System HP Data Protector* pour obtenir des informations détaillées. Si la documentation est installée sur votre système (sous HP-UX, Solaris ou Windows), le guide est disponible sous le nom `MPE_user.pdf` dans *`répertoire_Data_Protector`*`\Docs` (sous Windows), `/opt/omni/doc/C/` (sous UNIX) ou sur le DVD-ROM d'installation Windows de Data Protector dans le répertoire `docs`.

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section "Composants Data Protector" à la page 73.

Pour obtenir des informations sur les périphériques, les versions de la plate-forme MPE/iX et les composants Data Protector pris en charge, reportez-vous au document *Références, notes de publication et annonces produits HP Data Protector*.

Configuration système requise

Avant d'installer Data Protector sur la plate-forme MPE/iX, vérifiez les éléments suivants :

- TurboSTORE/iX ou TurboSTORE/iX 7x24 True-Online doit être installé sur votre ordinateur.
- Le protocole TCP/IP doit être installé et configuré.
- Le mécanisme de résolution de nom (DNS de fichiers d'hôtes) doit être activé.
- Pour connaître l'espace disque nécessaire, reportez-vous aux Références, notes de publication et annonces produits HP Data Protector.

Installation

Procédez comme suit pour installer Data Protector sur le serveur MPE/iX :

1. Déplacez le script `installDP6.10_MPE.sh` et le package `DP61_MPE6.5.tar` ou `DP61_MPE7.0.tar` (selon la version du système MPE/iX) vers le répertoire `/tmp` à l'aide de l'utilitaire `ftp`. Reportez-vous à la section Exemple 1 à la page 140.

   Vous devez impérativement déplacer le fichier `installDP6.10_MPE.sh` avec les caractéristiques suivantes :

   - Taille de l'enregistrement : `-150`
   - Facteur de bloc : `-empty`
   - Longueur variable des enregistrements du fichier : `V`
   - Type des enregistrements codés : `ASCII`

   Exemple 1 - Transfert du script d'installation DP6.10_MPE.sh et du package DP61_MPE6.5.tar

```
C:\WINNT\System32\cmd.exe

F:\144>ftp terry.hermes
Connected to terry.hermes
220 HP ARPA FTP Server [A0009C04] (C) Hewlett-Packard Co. 1990
User (terry.hermes:(none)): manager.sys
230 User logged on
ftp> cd /tmp
250 CWD  file action successful.
ftp> put ./installDP6.10_MPE.sh ./installDP6.10_MPE.sh;rec=-150,,v,ascii
200 PORT command ok.
150 File: ./installDP6.10_MPE.sh;rec=-150,,v,ascii opened; data connection will
be opened
226 Transfer complete.
ftp: 9139 bytes sent in 0.00Seconds 9139000.00Kbytes/sec.
ftp> bin
200 Type set to I.
ftp> put ./DP61_MPE6.0.tar ./DP61_MPE6.0.tar
200 PORT command ok.
150 File: ./DP61_MPE6.0.tar opened; data connection will be opened
226 Transfer complete.
ftp: 6182912 bytes sent in 5.70Seconds 1085.10Kbytes/sec.
ftp> quit
221 Server is closing command connection

F:\144>
```

2. Connectez-vous au système cible, puis démarrez le processus de décompactage, comme indiqué dans l'exemple ci-dessous :

Exemple 2 - Processus de décompactage sur le système cible

```
Untitled - Reflection for HP
File  Edit  Connection  Setup  Macro  Window  Help

MPE/iX:hello manager.sys
HP3000  Release: C.60.00   User Version: C.60.00   TUE, FEB  4, 2003,  2:45 PM
MPE/iX  HP31900 C.16.01  Copyright Hewlett-Packard 1987.  All rights reserved.
:sh
##############################################################################

               MPE/iX Shell and Utilities (A.50.02)
    COPYRIGHT (c) Hewlett-Packard Company 1992, All Rights Reserved.

##############################################################################


shell/iX> cd /tmp
shell/iX> . ./installDP6.10_MPE.sh
HP Data Protector 6.10 installation
-> Checking MPE/iX OS version ...
-> Detecting old Data Protector installation ...
-> Unpacking ...
-> Retriving Data Protector version ...
-> Updating Data Protector info using Disk Agent version A.06.10 ...
-> Updating Data Protector info using Media Agent version A.06.10 ...
-> Setting file and directory permissions ...
HP Data Protector 6.10 installed successfully !
shell/iX> _
f1  f2  f3  f4  f5  f6  f7  f8
24, 11   HP70092 -- terry via VT-MGR   Num
```

Après cette opération, tous les fichiers se retrouvent dans le répertoire `/usr/omni`.

REMARQUE :

Utilisez EDIT/3000 (appelé avec la commande `editor`) pour modifier les fichiers ci-dessous. Pour obtenir plus d'informations, reportez-vous au document *EDIT/3000 Reference Manual*.

3. Ajoutez la ligne suivante au fichier `DCNF.NET.SYS` :

   ```
   omni stream tcp nowait MANAGER.SYS /usr/omni/bin/inet inet
   -log /tmp/inet.log
   ```

4. Ajoutez la ligne suivante au fichier `SERVICES.NET.SYS` :

   ```
   omni 5555/tcp #Data Protector inet
   ```

5. Relancez `inetd` pour mettre à jour la configuration avec les nouveaux paramètres.

   Pour en savoir plus, reportez-vous au document *Configuring and Managing MPE/iX Internet Services*.

6. Pour savoir si `Data Protector Inet` est en cours d'exécution, utilisez telnet vers le port 5555 à partir d'un système différent :

   `telnet` *`nom_hôte`* `5555`

   Vous recevrez un message de Data Protector. S'il n'y a aucune réponse après 10 secondes, vérifiez les fichiers `INETDCNF.NET.SYS` et `SERVICES.NET.SYS`.

7. Importez le système dans la cellule Data Protector. Pour connaître la procédure à suivre, reportez-vous à la section "Importation de clients dans une cellule" à la page 205.

8. Une fois le système client importé, ajoutez l'utilisateur `MANAGER.SYS` au groupe d'utilisateurs `Admin` de Data Protector.

Pour plus d'informations sur les clients MPE/iX, reportez-vous au *Guide de l'utilisateur MPE/iX System HP Data Protector*, qui figure sur le DVD-ROM d'installation Windows sous le nom `\Docs\MPE_user.pdf`.

Installation locale de clients UNIX

Si vous ne disposez pas d'un Serveur d'installation pour UNIX sur votre réseau, ou que, pour une raison quelconque, vous ne parvenez pas à installer un système client à distance, il est possible d'installer les clients Data Protector en local à partir du DVD-ROM d'installation UNIX.

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section "Composants Data Protector" à la page 73.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes, processeurs et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- Vous devez disposer d'autorisations de `root` sur chaque système cible.

Le shell POSIX (`sh`) doit être installé.

REMARQUE :

Vous pouvez également utiliser la procédure suivante pour mettre à niveau les clients UNIX localement. Le script détecte une version déjà installée et vous invite à effectuer la mise à niveau.

Procédure

Procédez comme suit pour installer localement les clients UNIX :

1. Insérez et montez le DVD-ROM d'installation UNIX.
2. A partir de *Point_de_montage*/LOCAL_INSTALL, exécutez la commande omnisetup.sh. La syntaxe de la commande est la suivante :

   omnisetup.sh [-source *répertoire*] [-server *nom*] [-install *liste_composants*]

   où :

   - *répertoire* est l'emplacement où le DVD-ROM d'installation est monté. S'il n'est pas spécifié, le répertoire en cours est utilisé.
   - *nom* est un nom d'hôte complet du Gestionnaire de cellule de la cellule sur laquelle vous souhaitez installer le client. S'il n'est pas spécifié, le client ne sera pas automatiquement importé dans la cellule.

   REMARQUE :

   Si vous mettez à niveau le client qui ne réside pas sur le Gestionnaire de cellule, il n'est pas nécessaire de spécifier -install *liste_composants*. Dans ce cas, le programme d'installation sélectionnera sans émettre d'invite les mêmes composants que ceux déjà installés sur le système.

   Toutefois, pour mettre à niveau les composants du client se trouvant dans le Gestionnaire de cellule, exécutez la commande omnisetup.sh avec le paramètre -install *liste_composants* une fois la mise à niveau de Gestionnaire de cellule terminée.

   - *liste_composants* est une liste séparée par des virgules des codes composants à installer. L'utilisation d'espaces n'est pas autorisée. Si le paramètre -install n'est pas spécifié, le processus d'installation vous invite à installer séparément tous les composants disponibles sur le système.

   REMARQUE :

   Dans le cas d'une mise à niveau du client, si vous ne spécifiez pas le paramètre -install, le processus d'installation sélectionnera, sans émettre d'invite, les composants qui étaient installés sur le système avant le début de la mise à niveau.

   La liste des composants est présentée dans le tableau ci-dessous. La liste exacte des composants dépend de leur disponibilité sur ce système particulier. Les composants sont décrits à la section "Composants Data Protector" à la page 73.

Tableau 7 - Codes des composants Data Protector

Code composant	Composant
`cc`	Interface utilisateur
`da`	Agent de disque
`ma`	Agent de support général
`ndmp`	Agent de support NDMP
`informix`	Intégration Informix
`lotus`	Intégration Lotus
`oracle`	Intégration Oracle
`vmware`	Intégration VMware
`ov`	HP Network Node Manager
`sybase`	Intégration Sybase
`sap`	Intégration SAP R/3
`sapdb`	Intégration SAP DB
`db2`	Intégration DB2
`emc`	Agent EMC Symmetrix
`ssea`	Agent HP StorageWorks Disk Array XP
`snapa`	Agent HP StorageWorks VA
`smisa`	Agent HP StorageWorks EVA SMI-S
`vls_am`	Auto-migration VLS
`docs`	Documentation et aide en ligne en français
`javagui`	Interface graphique utilisateur Java
`fra_ls`	Support de langue français
`jpn_ls`	Support de langue japonais

Exemple

L'exemple ci-dessous présente l'installation des composants `Agent de disque`, `Agent général de support`, `Interface utilisateur` et `Informix` sur un client qui sera automatiquement importé dans la cellule avec le Gestionnaire de cellule `anapola.company.com`:

```
./omnisetup.sh -server anapola.company.com -install
da,ma,cc,informix
```

3. Le processus d'installation vous indique si l'installation est terminée et si le client a été importé dans la cellule Data Protector.

   Le composant `CORE` est installé la première fois qu'un composant logiciel est sélectionné pour l'installation.

   Le composant `CORE-INTEG` est installé la première fois qu'un composant du logiciel d'intégration est sélectionné pour l'installation ou la réinstallation.

Exécution de l'installation à partir du disque dur

Si vous souhaitez copier le DVD-ROM sur votre ordinateur et exécuter l'installation/la mise à niveau des clients UNIX clients à partir du disque dur, copiez au moins le répertoire `DP_DEPOT` et la commande `LOCAL_INSTALL/omnisetup.sh`. Par exemple, si vous copiez les packages d'installation vers `/var/dp61`, `DP_DEPOT` doit être un sous-répertoire de `/var/dp61` :

```
# pwd
/var/dp61
# ls
DP_DEPOT
omnisetup.sh
```

Après avoir copié ceci sur le disque dur, vous pouvez exécuter :

```
omnisetup.sh -source répertoire [-server nom] [-install
liste_composants]
```

Notez que l'option `-source` est obligatoire. Par exemple :

```
./omnisetup.sh -source /var/dp61
```

Etape suivante

Si au cours de l'installation, vous n'avez pas spécifié le nom du Gestionnaire de cellule, le client ne sera pas importé dans la cellule. Dans ce cas, vous devez l'importer à l'aide de l'interface graphique utilisateur de Data Protector. Pour connaître la procédure à suivre, reportez-vous à la section "Importation de clients dans une cellule" à la page 205. Pour plus d'informations sur les tâches de configuration supplémentaires, reportez-vous à l'aide en ligne.

Installation des clients d'intégration Data Protector

Les intégrations Data Protector sont des composants logiciels permettant d'exécuter une sauvegarde en ligne des applications de bases de données, telles qu'Oracle ou

Microsoft Exchange, avec Data Protector. Les intégrations ZDB Data Protector sont des composants logiciels permettant d'exécuter une sauvegarde ZDB à l'aide de baies de disques ZDB, telles que HP StorageWorks Enterprise Virtual Array.

Les systèmes exécutant des applications de base de données sont appelés clients d'intégration ; les systèmes utilisant les baies de disques ZDB pour la sauvegarde et la restauration des données sont appelés clients d'intégration ZDB. Ces clients sont installés à l'aide de la même procédure que tout autre client sous Windows ou UNIX, à condition que le composant logiciel approprié ait été sélectionné (par exemple, le composant `Intégration MS Exchange` pour la sauvegarde d'une base de données MS Exchange, le composant `Agent HP StorageWorks EVA SMI-S` pour une sauvegarde avec temps d'indisponibilité nul sur HP StorageWorks Enterprise Virtual Array, etc.).

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes, processeurs et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- Une licence est nécessaire pour utiliser l'intégration Data Protector avec une application de base de données (à l'exception de l'intégration VSS). Pour plus d'informations sur l'attribution des licences, consultez la section "Extensions fonctionnelles" à la page 354.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation (éventuellement pour une installation distante) doivent être installés sur votre réseau. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 42 pour de plus amples informations.

Avant de lancer la procédure d'installation, choisissez les autres composants logiciels Data Protector à installer sur le client avec un composant d'intégration. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section "Composants Data Protector" à la page 73.

Notez que dans les situations exposées ci-dessous, vous devez installer les composants Data Protector suivants :

- Le composant `Agent de disque` pour pouvoir sauvegarder des données de système de fichiers avec Data Protector. Vous pouvez utiliser l'Agent de disque dans les cas suivants :
  - Pour exécuter une sauvegarde du système de fichiers de données importantes pour lesquelles la sauvegarde de l'application de base de données *ne peut pas* être utilisée.
  - Pour exécuter un essai de sauvegarde du système de fichiers d'un serveur d'application de base de données (serveur Oracle ou MS SQL Server, par exemple). Vous devez procéder à un essai de sauvegarde de système de fichier *avant* de configurer l'intégration Data Protector avec une

application de base de données et résoudre les problèmes - notamment de communication - liés à l'application et à Data Protector.
  - Pour exécuter une image disque et un client ZDB de système de fichiers.
  - Pour effectuer une restauration à partir d'un support de sauvegarde vers le système d'application sur le réseau LAN dans le cas d'intégrations ZDB SAP R/3.
- Le composant `Interface utilisateur` pour obtenir l'accès à l'interface graphique utilisateur et à l'interface de ligne de commande de Data Protector sur le client d'intégration de Data Protector.
- Le composant `Agent général de support` si des périphériques de sauvegarde sont connectés au client d'intégration Data Protector. Sur les clients Data Protector utilisés pour accéder à un lecteur dédié NDMP via le serveur NDMP, l'`Agent de support NDMP` est requis.

Les clients d'intégration peuvent être installés en local à partir du DVD-ROM d'installation du Serveur d'installation pour Windows ou UNIX ou à distance à l'aide du Serveur d'installation pour Windows ou UNIX.

Pour plus d'informations sur des clients d'intégration spécifiques, reportez-vous aux paragraphes correspondants ci-après :

- "Clients Microsoft Exchange Server" à la page 149
- "Clients Microsoft SQL Server" à la page 149
- "Clients Microsoft SharePoint Portal Server" à la page 150
- "Clients Sybase" à la page 150
- "Clients Informix Server" à la page 150
- "Clients SAP R/3" à la page 151
- "Clients SAP DB/MaxDB" à la page 151
- "Clients Oracle" à la page 152
- "Clients VMware Virtual Infrastructure" à la page 152
- "Clients DB2" à la page 153
- "Clients NNM" à la page 153
- "Clients NDMP" à la page 153
- "Clients Microsoft Volume Shadow Copy Service" à la page 153
- "Clients Lotus Notes/Domino Server" à la page 154
- "Intégration EMC Symmetrix" à la page 154
- "Intégration HP StorageWorks Disk Array XP" à la page 159
- "Intégration HP StorageWorks Virtual Array" à la page 165
- "Intégration HP StorageWorks Enterprise Virtual Array" à la page 171
- "Clients IAP" à la page 178
- "Clients d'auto-migration VLS" à la page 179

Une fois que vous avez terminé l'installation du logiciel d'intégration Data Protector sur les clients d'intégration Data Protector comme la décrivent les sections indiquées, reportez-vous au *Guide d'intégration HP Data Protector*, au *Guide de l'administrateur ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector* ou au *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector pour configurer les clients d'intégration Data Protector*.

Installation en local

Si vous ne disposez pas d'un Serveur d'installation pour le système d'exploitation installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation Windows ou UNIX, selon la plate-forme sur laquelle vous installez un client. Reportez-vous à la section "Installation de clients Windows" à la page 87 ou "Installation locale de clients UNIX" à la page 142 pour connaître la procédure de cette installation.

Si vous ne choisissez pas de Gestionnaire de cellule pendant l'installation, le système du client doit être importé manuellement dans la cellule après l'installation en local. Reportez-vous également à la section "Importation de clients dans une cellule" à la page 205.

Installation distante

Vous devez installer le logiciel client à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface graphique utilisateur Data Protector. Pour connaître la procédure détaillée pour installer le logiciel à distance, reportez-vous à la section "Installation distante de clients Data Protector" à la page 78.

Une fois l'installation à distance terminée, le système client devient automatiquement membre de la cellule Data Protector.

Installation des intégrations compatibles cluster

Les clients d'intégration Data Protector compatibles cluster doivent être installés localement, à partir du DVD-ROM, sur chaque nœud cluster. Lors de la configuration locale du client, installez les composants logiciels d'intégration appropriés (tels que `Intégration Oracle` ou `Agent HP StorageWorks EVA SMI-S`) en plus des autres composants logiciels client.

Vous pouvez également installer une application de base de données compatible cluster et un Agent ZDB sur le Gestionnaire de cellule Data Protector. Sélectionnez le composant logiciel d'intégration approprié lors de la configuration du Gestionnaire de cellule.

La procédure d'installation dépend de l'environnement de cluster dans lequel vous installez votre client d'intégration. Consultez les paragraphes relatifs à la gestion de clusters correspondant à votre système d'exploitation :

- "Installation de Data Protector sur MC/ServiceGuard" à la page 186.

- "Installation de Data Protector sur Microsoft Cluster Server" à la page 187.
- "Installation de clients Data Protector sur un cluster Veritas" à la page 200.
- "Installation de clients Data Protector sur un cluster Novell NetWare" à la page 201.
- "Installation de Data Protector sur un cluster IBM HACMP" à la page 203.

Pour plus d'informations sur la gestion de clusters, reportez-vous à l'index de l'aide en ligne (rubrique "cluster, MC/ServiceGuard") et au *Guide conceptuel HP Data Protector*.

Etape suivante

Une fois l'installation terminée, reportez-vous au *Guide d'intégration HP Data Protector* approprié pour obtenir des informations sur la configuration de l'intégration.

Clients Microsoft Exchange Server

Votre serveur Microsoft Exchange est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données Microsoft Exchange Server, vous devez sélectionner le composant `Intégration MS Exchange` lors de la procédure d'installation.

L'agent d'intégration Boîte aux lettres unique de Microsoft Exchange sera installé en tant que partie du package d'intégration Microsoft Exchange Server de Data Protector.

Sur des systèmes Microsoft Exchange Server 2007, vous devez installer un autre package pour permettre la fonctionnalité de l'intégration Microsoft Exchange Single Mailbox Data Protector. Ce package s'appelle Microsoft Exchange Server MAPI Client and Collaboration Data Objects (`ExchangeMapiCdo.EXE`) et vous pouvez le télécharger gratuitement à partir du site Web de Microsoft à l'adresse http://www.microsoft.com/downloads/Search.aspx?DisplayLang=en.

Clients Microsoft SQL Server

Votre serveur Microsoft SQL Server est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données Microsoft SQL Server, vous devez sélectionner le composant `Intégration MS SQL` lors de la procédure d'installation.

Sur les systèmes Microsoft SQL Server 2005, vous devez installer un package spécifique pour permettre le fonctionnement normal de l'intégration Data Protector, et ce avant le composant `Intégration MS SQL Server`. Vous pouvez installer le package de l'une des façons suivantes :

- Dans l'assistant d'installation de Microsoft SQL Server 2005, dans la fenêtre de sélection des fonctions, développez Client Components (Composants client) et sélectionnez Legacy Components (Composants existants). Suivez les instructions de l'assistant pour finaliser l'installation.

- Accédez au site Web de Microsoft http://www.microsoft.com/downloads/details.aspx?familyid=D09C1D60-A13C-4479-9B91-9E8B9D835CDC&DisplayLang=en. Téléchargez le package Microsoft SQL Server 2005 Backward Compatibility Components et installez-le.

Clients Microsoft SharePoint Portal Server

Les instances de Microsoft SharePoint Portal Server et de Microsoft SQL Server sont supposées en cours de fonctionnement.

Pour pouvoir sauvegarder des objets Microsoft SharePoint Portal Server, installez les composants Data Protector suivants :

- `Intégration MS SharePoint` - sur des systèmes Microsoft SharePoint Portal Server
- `Intégration MS SQL` - sur des systèmes Microsoft SQL Server

Clients Sybase

Votre serveur Sybase Backup Server est supposé sous tension et en cours de fonctionnement.

Pour sauvegarder la base de données Sybase, vous devez sélectionner les composants Data Protector suivants lors de la procédure d'installation :

- `Intégration Sybase` - pour la sauvegarde d'une base de données Sybase ;
- `Agent de disque` - installez l'Agent de disque pour deux raisons :
  - Pour exécuter une sauvegarde du système de fichiers de Sybase Backup Server. Effectuez cette sauvegarde *avant* de configurer votre intégration Data Protector Sybase et résolvez tous les problèmes liés à Sybase Backup Server et à Data Protector.
  - Pour exécuter une sauvegarde du système de fichiers de données importantes pour lesquelles Sybase Backup Server *ne peut pas* être utilisé.

Clients Informix Server

Votre serveur Informix Server est supposé sous tension et en cours de fonctionnement.

Pour sauvegarder la base de données Informix Server, vous devez sélectionner les composants Data Protector suivants lors de la procédure d'installation :

- `Intégration Informix` - pour la sauvegarde d'une base de données Informix Server ;
- `Agent de disque` - installez l'Agent de disque pour deux raisons :
  - Pour exécuter une sauvegarde du système de fichiers Informix Server. Effectuez cette sauvegarde *avant* de configurer votre intégration Data Protector Informix Server et résolvez tous les problèmes liés à Informix Server et à Data Protector.

- Pour exécuter une sauvegarde du système de fichiers pour les données Informix Server importantes (telles que le fichier ONCONFIG, le fichier `sqlhosts`, le fichier d'amorçage de secours ON-Bar, `oncfg_INFORMIXSERVER.SERVERNUM`, les fichiers de configuration, etc.) qui *ne peuvent pas* être sauvegardés avec ON-Bar.

IBM HACMP Cluster

Si Informix Server est installé dans l'environnement de cluster IBM HACMP, installez le composant `Intégration Informix` sur tous les noeuds du cluster.

Clients SAP R/3

Configuration système requise

- Vérifiez que les logiciels Oracle suivants sont installés et configurés :
  - Oracle Enterprise Server (RDBMS) ;
  - logiciel Oracle Net8 ;
  - SQL*Plus.
- Votre serveur SAP R/3 Database est supposé sous tension et en cours de fonctionnement.

REMARQUE :

Les spécifications de sauvegarde de l'intégration SAP R/3 Data Protector sont entièrement compatibles avec la version antérieure de Data Protector. Data Protector exécute toutes les spécifications de sauvegarde créées par les versions antérieures. En revanche, vous ne pouvez pas utiliser sur une version antérieure de Data Protector les spécifications de sauvegarde créées avec la version actuelle.

Pour pouvoir sauvegarder la base de données SAP R/3, sélectionnez les composants suivants lors de la procédure d'installation :

- `Intégration SAP R/3`
- `Agent de disque`
  Data Protector requiert l'installation d'un Agent de disque sur les serveurs de sauvegarde (clients comportant des données de système de fichiers à sauvegarder).

Clients SAP DB/MaxDB

Votre serveur SAP DB/MaxDB est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données SAP DB/MaxDB, vous devez sélectionner les composants Data Protector suivants lors de la procédure d'installation :

- `Intégration SAP DB` - pour pouvoir exécuter une sauvegarde en ligne intégrée d'une base de données SAP DB/MaxDB
- `Agent de disque` - pour pouvoir exécuter une sauvegarde hors ligne non intégrée d'une base de données SAP DB/MaxDB

Clients Oracle

Votre serveur Oracle est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données Oracle, vous devez sélectionner le composant `Intégration Oracle` lors de la procédure d'installation.

HP OpenVMS

Sous OpenVMS, après avoir installé l'intégration Oracle et l'avoir configurée selon les indications du *Guide d'intégration HP Data Protector pour Oracle et SAP*, vérifiez que l'entrée `-key Oracle8` figure dans `OMNI$ROOT:[CONFIG.CLIENT]omni_info`, par exemple :

```
-key oracle8 -desc "Oracle Integration" -nlsset 159 -nlsId
12172 -flags 0x7 -ntpath "" -uxpath "" -version A.06.10
```

Si l'entrée est absente, copiez-la dans le fichier `OMNI$ROOT:[CONFIG.CLIENT]omni_format`. Sinon, l'installation de l'intégration Oracle ne sera pas indiquée sur le client OpenVMS.

Clients VMware Virtual Infrastructure

Les systèmes VirtualCenter et ESX Server sont supposés en cours de fonctionnement. Pour pouvoir installer les clients VMware à distance, vous devez d'abord définir OpenSSH. Pour plus d'informations, recherchez l'entrée suivante dans l'index de l'aide en ligne : "installation, systèmes client".

Installez le composant `Intégration VMware` Data Protector sur les clients suivants :

- Tous les systèmes ESX Server à partir desquels vous prévoyez de sauvegarder des machines virtuelles
- Systèmes VirtualCenter (le cas échéant)
- Systèmes de sauvegarde proxy (si vous envisagez d'utiliser les méthodes de sauvegarde VCBfile et VCBimage)
- Systèmes Windows (physiques ou virtuels) sur lesquels vous prévoyez de restaurer des systèmes de fichiers de machines virtuelles

Clusters

Installez le composant `Intégration VMware` sur les deux noeuds de cluster, quels que soient les systèmes qui figurent dans un cluster (ESX Server ou VirtualCenter).

Clients DB2

Votre serveur DB2 est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données DB2, vous devez sélectionner les composants `Intégration DB2` et `Agent de disque` lors de la procédure d'installation.

Dans un environnement à partition physique, installez les composants `Intégration DB2` et `Agent de disque` sur chaque nœud physique (système) sur lequel réside la base de données.

REMARQUE :

Connectez-vous comme utilisateur `root` pour effectuer l'installation.

Clients NNM

Votre système NNM est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données NNM, vous devez sélectionner les composants `Intégration de sauvegarde HP NNM` et `Agent de disque` lors de la procédure d'installation. Vous aurez besoin de l'Agent de disque pour exécuter les scripts antérieurs et postérieurs à la sauvegarde utilisés pour les opérations de sauvegarde.

Clients NDMP

Votre serveur NDMP est supposé sous tension et en cours de fonctionnement.

Au cours de la procédure d'installation, sélectionnez l'`agent de support NDMP` et installez-le sur tous les clients Data Protector ayant accès aux lecteurs NDMP dédiés.

REMARQUE :

Dans le cas où un client Data Protector ne doit pas être utilisé pour accéder à un lecteur NDMP dédié par le serveur NDMP et sera uniquement utilisé pour commander le robot de la bibliothèque, on peut installer sur ce client soit l'`Agent de support NDMP`, soit l'`Agent général de support`.

Notez que seul un Agent de support peut être installé sur un client Data Protector.

Clients Microsoft Volume Shadow Copy Service

Pour effectuer des sauvegardes des modules d'écriture VSS (Microsoft Exchange Server et Microsoft SQL Server) ou uniquement du système de fichiers avec VSS, installez

les composants logiciels Data Protector suivants sur les systèmes d'application et de sauvegarde, ou en cas de sauvegarde locale, uniquement sur le système d'application :

- l'`Intégration MS Volume Shadow Copy`.
- l'`Agent HP StorageWorks XP` ou l'`Agent HP StorageWorks EVA SMI-S` (selon la baie de disques utilisée),
- `Agent de support général`

Clients Lotus Notes/Domino Server

Votre serveur Lotus Notes/Domino Server est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données Lotus Notes/Domino Server, vous devez sélectionner les composants `Intégration Lotus` et `Agent de disque` lors de la procédure d'installation. Vous avez besoin du composant `Agent de disque` pour pouvoir sauvegarder les données du système de fichiers avec Data Protector pour les tâches suivantes :

- Sauvegarde des données importantes qui *ne peuvent* être sauvegardées avec l'agent d'intégration Lotus. Il s'agit de fichiers "non-bases de données", qui doivent être sauvegardés pour fournir une solution complète de protection des données pour un serveur Lotus Domino R5, par exemple `notes.ini`, `desktop.dsk` et tous les fichiers `*.id`.
- Essai de sauvegarde du système de fichiers pour résoudre les problèmes - notamment de communication - liés à l'application et à Data Protector.

Cluster Lotus Domino

Installez les composants `Intégration Lotus` et `Agent de disque` sur les serveurs Domino qui seront utilisés pour la sauvegarde et, si vous envisagez de restaurer des bases de données Domino sur d'autres serveurs Domino contenant des répliques de ces bases, installez également les composants sur ces serveurs.

Intégration EMC Symmetrix

Pour intégrer EMC Symmetrix à Data Protector, installez les composants logiciels Data Protector suivants sur les systèmes d'application et de sauvegarde :

- `Agent EMC Symmetrix` (SYMA)
- `Agent général de support`
  Installez le composant `Agent général de support` sur le système de sauvegarde pour sauvegarder les données en bloc. Installez-le sur le système d'application pour sauvegarder les journaux d'archive ou pour restaurer le système.
- `Agent de disque`

Installez le composant `Agent de disque` sur les systèmes d'application et de sauvegarde pour exécuter des sauvegardes ZDB d'image disque et de système de fichiers. Les clients sans Agent de disque ne sont pas répertoriés dans les listes déroulantes `Système d'application` et `Système de sauvegarde` lors de la création d'une spécification ZDB.

Installation sur un cluster

Vous pouvez installer l'intégration EMC Symmetrix dans un environnement de cluster. Pour connaître les configurations de clusters prises en charge et la configuration requise pour l'installation, reportez-vous au *Guide de l'administrateur ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Intégration à d'autres applications

Si vous souhaitez installer l'intégration EMC Symmetrix avec une application de base de données, installez le composant Data Protector spécifique à l'intégration de cette application sur les systèmes d'application et de sauvegarde, et effectuez les tâches spécifiques à cette intégration. Vous pouvez installer l'intégration EMC Symmetrix avec Oracle et SAP R/3.

Intégration EMC Symmetrix avec Oracle

Configuration système requise

- Les logiciels suivants doivent être installés sur le système d'application :
  - Oracle Enterprise Server (RDBMS) ;
  - Services Oracle Net ;
  - SQL*Plus.
- Les fichiers de la base de données Oracle utilisés par le système d'application doivent être installés sur des périphériques EMC Symmetrix qui sont mis en miroir sur le système de sauvegarde.
  La base de données peut être installée sur des images disque, des volumes logiques ou des systèmes de fichiers. Les fichiers Oracle suivants doivent être mis en miroir :
  - fichiers de données ;
  - fichier de contrôle ;
  - fichiers journaux de rétablissement en ligne.

  Les fichiers journaux de rétablissement archivés doivent résider sur des disques qui ne sont pas en miroir.

Procédure d'installation

Procédez aux tâches d'installation suivantes :

1. Installez la base de données du catalogue de récupération Oracle. De préférence, installez-la sur un autre système, sur des disques qui ne sont pas en miroir. Laissez le catalogue de récupération non enregistré. Pour plus d'informations sur l'installation de la base de données, reportez-vous à la documentation Oracle.
2. Installez les composants logiciels Data Protector suivants :
   - `Agent EMC Symmetrix` - sur le système d'application et le système de sauvegarde ;
   - `Intégration Oracle` - sur le système d'application et le système de sauvegarde.

REMARQUE :

- Le composant `Intégration Oracle` Data Protector sur le système de sauvegarde n'est nécessaire que pour la méthode de jeu de sauvegarde ZDB. Il n'est pas nécessaire pour la méthode proxy-copy ZDB.
- Dans un environnement de cluster RAC, plusieurs instances Oracle accèdent à la base de données d'application Oracle. Par conséquent, installez les composants `Intégration Oracle` et `Agent EMC Symmetrix` Data Protector sur tous les systèmes sur lesquels s'exécutent les instances Oracle.
- Si vous avez installé la base de données du catalogue de récupération Oracle sur un autre système, il n'est pas nécessaire d'y installer des composants logiciels Data Protector.

Intégration EMC Symmetrix avec SAP R/3

Configuration système requise

- Les logiciels Oracle suivants doivent être installés sur le système d'application :
  - Oracle Enterprise Server (RDBMS) ;
  - logiciel Oracle Net8 ;
  - SQL*Plus.
- Si vous envisagez d'exécuter des sessions ZDB compatibles SAP (BRBACKUP démarré sur le système de sauvegarde et non sur le système d'application), le système de sauvegarde doit être configuré. Pour plus de détails, reportez-vous au guide de la base de données SAP pour Oracle (sauvegarde split mirror, configuration du logiciel).
- La base de données du système d'application peut être installée sur des images disque, des volumes logiques ou des systèmes de fichiers.
  - Les fichiers de données Oracle *doivent* résider sur une baie de disques.

- Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne ne doivent pas nécessairement résider sur une baie de disques. En revanche, pour les sessions ZDB *en ligne* compatibles SAP, les fichiers de contrôle doivent résider sur une baie de disques.
- Pour la *sauvegarde hors ligne*, le fichier de contrôle et les journaux de rétablissement en ligne *doivent* résider sur une baie de disques.
- Les fichiers journaux de rétablissement archivés ne doivent pas nécessairement résider sur une baie de disques.

REMARQUE :

Si certains des fichiers de données Oracle sont installés sur des liens symboliques, créez les liens également sur le système de sauvegarde.

UNIX seulement : si la base de données Oracle est installée sur des partitions brutes (image disque ou volumes logiques bruts), vérifiez que les noms de volume/groupe de disques sont identiques sur le système d'application et le système de sauvegarde.

- Sous UNIX, vérifiez que les utilisateurs suivants sont définis sur le système d'application :
  - `ora`*`ORACLE_SID`* dans le groupe principal `dba`
  - *`ORACLE_SID`*`adm` dans le groupe UNIX `sapsys`
- Le logiciel SAP R/3 doit être correctement installé sur le système d'application. Les répertoires standard suivants doivent être installés sur le système d'application après l'installation de SAP R/3 :

REMARQUE :

L'emplacement des répertoires dépend des variables d'environnement. Reportez-vous à la documentation SAP R/3 pour plus d'informations.

- *`ORACLE_HOME`*`/dbs` - les profils Oracle et SAP R/3
- *`ORACLE_HOME`*`/bin` - les fichiers binaires Oracle
- *`SAPDATA_HOME`*`/sapbackup` - le répertoire SAPBACKUP contenant les fichiers journaux BRBACKUP
- *`SAPDATA_HOME`*`/sapbackup` - le répertoire SAPARCH contenant les fichiers journaux BRARCHIVE
- *`SAPDATA_HOME`*`/sapreorg`
- *`SAPDATA_HOME`*`/sapcheck`
- *`SAPDATA_HOME`*`/saptrace`
- `/usr/sap/`*`ORACLE_SID`*`/SYS/exe/run`

REMARQUE :

Si vous envisagez d'effectuer une restauration instantanée, vérifiez que les répertoires `sapbackup`, `saparch` et `sapreorg` figurent sur d'autres volumes source que les fichiers de données Oracle.

Si les six derniers répertoires ne sont pas aux emplacements indiqués ci-dessus, créez les liens appropriés vers eux.
Le propriétaire du répertoire `/usr/sap/`*`ORACLE_SID`*`/SYS/exe/run` doit être l'utilisateur UNIX `ora`*`ORACLE_SID`*. Le propriétaire des fichiers SAP R/3 doit être l'utilisateur UNIX `ora`*`ORACLE_SID`* et le groupe UNIX `dba` avec le bit setuid à 1 (chmod 4755 ...). L'exception est le fichier BRRESTORE, dont le propriétaire doit être l'utilisateur UNIX *`ORACLE_SID`*`adm`.

Exemple

Si *`ORACLE_SID`* est PRO, les droits à l'intérieur du répertoire `/usr/sap/PRO/SYS/exe/run` doivent ressembler à ce qui suit :

```
-rwsr-xr-x   1 orapro dba 4598276 Apr 17  1998 brarchive
-rwsr-xr-x   1 orapro dba 4750020 Apr 17  1998 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  1998 brconnect
-rwsr-xr-x   1 proadm sapsys 430467 Apr 17  1998 brrestore
-rwsr-xr-x   1 orapro dba 188629 Apr 17  1998 brtools
```

Procédure d'installation

1. Installez SAP R/3 BRTOOLS sur le système d'application.
2. Installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :
   - `Agent EMC Symmetrix`
   - `Intégration SAP R/3`
   - `Agent de disque`

REMARQUE :

Il n'est pas nécessaire d'installer `Intégration SAP R/3` sur le système de sauvegarde si vous envisagez d'exécuter des sessions ZDB compatibles SAP lors desquelles BRBACKUP est démarré sur ce système.

Intégration d'EMC Symmetrix avec Microsoft SQL Server

Conditions préalables

Microsoft SQL Server doit être installé sur le système d'application. Les bases de données utilisateur *doivent* se trouver sur les volumes source de la baie de disques, tandis que les bases de données système peuvent être installées n'importe où. Cependant, si les bases de données système sont elles aussi installées sur la baie de disques, elles *doivent* l'être sur des volumes source *différents* de ceux des bases de données utilisateur.

Procédure d'installation

Installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :

- `Agent EMC Symmetrix`
- `Intégration MS SQL`

Intégration HP StorageWorks Disk Array XP

Pour intégrer HP StorageWorks Disk Array XP à Data Protector, installez les composants logiciels Data Protector suivants sur les systèmes d'application et de sauvegarde :

- `Agent HP StorageWorks XP`
- `Agent général de support`
  Installez le composant `Agent général de support` sur le système de sauvegarde pour sauvegarder les données en bloc. Installez-le sur le système d'application pour sauvegarder les journaux d'archive ou pour restaurer le système.
- `Agent de disque`
  Installez le composant `Agent de disque` sur les systèmes d'application et de sauvegarde pour exécuter des sauvegardes ZDB d'image disque et de système de fichiers. Les clients sans Agent de disque ne sont pas répertoriés dans les listes déroulantes `Système d'application` et `Système de sauvegarde` lors de la création d'une spécification ZDB.

Installation sur un cluster

Vous pouvez installer l'intégration HP StorageWorks Disk Array XP dans un environnement de cluster. Pour connaître les configurations de clusters prises en charge et la configuration requise pour l'installation, reportez-vous au *Guide de l'administrateur ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Intégration à d'autres applications

Si vous souhaitez installer l'intégration HP StorageWorks XP avec une application de base de données, installez le composant Data Protector spécifique à l'intégration de

cette application sur les systèmes d'application et de sauvegarde, et effectuez les tâches spécifiques à cette intégration. Vous pouvez installer l'intégration HP StorageWorks Disk Array XP avec Oracle, SAP R/3, Microsoft Exchange Server, Microsoft SQL Server et Microsoft VSS.

Intégration HP StorageWorks Disk Array XP avec Oracle

Configuration système requise

- Les logiciels suivants doivent être installés et configurés sur le système d'application et sur le système de sauvegarde pour la méthode de jeu de sauvegarde ZDB :
  - Oracle Enterprise Server (RDBMS) ;
  - Services Oracle Net ;
  - SQL*Plus.

  Le logiciel Oracle installé sur le système de sauvegarde doit l'être dans le même répertoire que sur le système d'application. Les binaires doivent être identiques à ceux du système d'application. Vous pouvez y parvenir en copiant les fichiers et l'environnement système du système d'application vers le système de sauvegarde ou par une installation "propre" des binaires Oracle sur le système de sauvegarde avec les mêmes paramètres d'installation que sur le système d'application.
- Les fichiers de données Oracle sur le système d'application doivent être installés sur des périphériques logiques HP StorageWorks Disk Array XP qui sont mis en miroir sur le système de sauvegarde.
  Dans le cas de la méthode de jeu de sauvegarde, si certains des fichiers de données Oracle sont installés sur des liens symboliques, créez ces liens également sur le système de sauvegarde.
  Selon l'emplacement du fichier de contrôle Oracle, des fichiers journaux de rétablissement en ligne et du fichier SPFILE, les deux options suivantes sont possibles :
  - Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et le fichier SPFILE résident sur un groupe de volumes (si LVM est utilisé) ou un volume source différent des fichiers de données Oracle.
    La restauration instantanée est activée par défaut dans ce type de configuration.
  - Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et le fichier SPFILE résident sur le même groupe de volumes (si LVM est utilisé) ou volume source que les fichiers de données Oracle.
    Par défaut, la restauration instantanée *n'est pas* activée dans ce type de configuration. Vous pouvez l'activer en définissant les variables `omnirc ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF` et `ZDB_ORA_NO_CHECKCONF_IR`. Pour plus d'informations, reportez-vous au *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Les fichiers journaux de rétablissement archivés Oracle ne doivent pas nécessairement résider sur des volumes source.

Procédure d'installation

Procédez aux tâches d'installation suivantes :

1. Installez la base de données du catalogue de récupération Oracle. De préférence, installez-la sur un autre système, sur des disques qui ne sont pas en miroir. Laissez le catalogue de récupération non enregistré. Pour plus d'informations sur l'installation de la base de données, reportez-vous à la documentation Oracle.
2. Installez les composants logiciels Data Protector suivants :
   - `Agent HP StorageWorks XP` - sur le système d'application et le système de sauvegarde ;
   - `Intégration Oracle` - sur le système d'application et le système de sauvegarde.

REMARQUE :

- Le composant `Intégration Oracle` Data Protector sur le système de sauvegarde n'est nécessaire que pour la méthode de jeu de sauvegarde ZDB. Il n'est pas nécessaire pour la méthode proxy-copy ZDB.
- Dans un environnement de cluster RAC, plusieurs instances Oracle accèdent à la base de données d'application Oracle. Par conséquent, installez les composants `Intégration Oracle` et `Agent HP StorageWorks XP` Data Protector sur tous les systèmes sur lesquels s'exécutent les instances Oracle.
- Si vous avez installé la base de données du catalogue de récupération Oracle sur un autre système, il n'est pas nécessaire d'y installer des composants logiciels Data Protector.

Intégration de HP StorageWorks Disk Array XP avec SAP R/3

Configuration système requise

- Les logiciels Oracle suivants doivent être installés sur le système d'application :
  - Oracle Enterprise Server (RDBMS) ;
  - Services Oracle Net ;
  - SQL*Plus.
- Si vous envisagez d'exécuter des sessions ZDB compatibles SAP (BRBACKUP démarré sur le système de sauvegarde et non sur le système d'application), le

système de sauvegarde doit être configuré. Pour plus de détails, reportez-vous au guide de la base de données SAP pour Oracle (sauvegarde split mirror, configuration du logiciel).

- La base de données du système d'application peut être installée sur des images disque, des volumes logiques ou des systèmes de fichiers.
  - Les fichiers de données Oracle *doivent* résider sur une baie de disques.
  - Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne ne doivent pas nécessairement résider sur une baie de disques. En revanche, pour les sessions ZDB *en ligne* compatibles SAP, les fichiers de contrôle doivent résider sur une baie de disques.
  - Pour la *sauvegarde hors ligne*, le fichier de contrôle et les journaux de rétablissement en ligne *doivent* résider sur une baie de disques.
  - Les fichiers journaux de rétablissement archivés ne doivent pas nécessairement résider sur une baie de disques.

  Si le fichier de contrôle Oracle, les journaux de rétablissement en ligne et le fichier SPFILE Oracle résident sur le *même* groupe de volume LVM ou volume source que les fichiers de données Oracle, définissez les variables `ZDB_ORA_NO_CHECKCONF_IR`, `ZDB_ORA_INCLUDE_CF_OLF` et `ZDB_ORA_INCLUDE_SPF` de la commande Data Protector `omnirc` Data Protector. Sinon, vous ne pourrez pas exécuter de sessions de sauvegarde ZDB sur disque et ZDB sur disque + bande. Pour plus d'informations, reportez-vous au *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

REMARQUE :

Si certains des fichiers de données Oracle sont installés sur des liens symboliques, créez les liens également sur le système de sauvegarde.

UNIX seulement : si la base de données Oracle est installée sur des partitions brutes (image disque ou volumes logiques bruts), vérifiez que les noms de volume/groupe de disques sont identiques sur le système d'application et le système de sauvegarde.

- Sous UNIX, vérifiez que les utilisateurs suivants sont définis sur le système d'application :
  - `ora`*`ORACLE_SID`* dans le groupe principal `dba`
  - *`ORACLE_SID`*`adm` dans le groupe UNIX `sapsys`
- Le logiciel SAP R/3 doit être correctement installé sur le système d'application. Les répertoires standard suivants doivent être installés sur le système d'application après l'installation de SAP R/3 :

REMARQUE :

L'emplacement des répertoires dépend des variables d'environnement (systèmes UNIX) ou de registre (systèmes Windows). Reportez-vous à la documentation SAP R/3 pour plus d'informations.

- *ORACLE_HOME*/dbs (systèmes UNIX)
  ORACLE_HOME\database (systèmes Windows - les profils Oracle et SAP R/3)
- *ORACLE_HOME*/bin ou (systèmes UNIX)
  ORACLE_HOME\bin (systèmes Windows) - les fichiers binaires Oracle
- *SAPDATA_HOME*/sapbackup (systèmes UNIX)
  SAPDATA_HOME\sapbackup (systèmes Windows) - le répertoire SAPBACKUP des fichiers journaux BRBACKUP
- *SAPDATA_HOME*/saparch (systèmes UNIX)
  SAPDATA_HOME\saparch (systèmes Windows) - le répertoire SAPARCH des fichiers journaux BRARCHIVE
- *SAPDATA_HOME*/sapreorg (systèmes UNIX)
  SAPDATA_HOME\sapreorg (systèmes Windows)
- *SAPDATA_HOME*/sapcheck (systèmes UNIX)
  SAPDATA_HOME\sapcheck (systèmes Windows)
- *SAPDATA_HOME*/saptrace (systèmes UNIX)
  SAPDATA_HOME\saptrace (systèmes Windows)
- /usr/sap/*ORACLE_SID*/SYS/exe/run (systèmes UNIX)
  c:\Oracle*ORACLE_SID*\sys\exe\run (systèmes Windows)

REMARQUE :

Si vous envisagez d'effectuer une restauration instantanée, vérifiez que les répertoires sapbackup, saparch et sapreorg figurent sur d'autres volumes source que les fichiers de données Oracle.

Systèmes UNIX

Sur les systèmes UNIX, si les six derniers répertoires ne sont pas aux emplacements indiqués ci-dessus, créez les liens appropriés vers eux.
Sur les systèmes UNIX, le propriétaire du répertoire /usr/sap/*ORACLE_SID*/SYS/exe/run doit être l'utilisateur UNIX ora*ORACLE_SID*. Le propriétaire des fichiers SAP R/3 doit être l'utilisateur UNIX ora*ORACLE_SID* et le groupe UNIX dba avec le bit setuid à 1 (chmod 4755 ...). L'exception est le fichier BRRESTORE, dont le propriétaire doit être l'utilisateur UNIX *ORACLE_SID*adm.

Exemple UNIX

Si *ORACLE_SID* est PRO, les droits à l'intérieur du répertoire /usr/sap/PRO/SYS/exe/run doivent ressembler à ce qui suit :

```
-rwsr-xr-x   1 orapro dba 4598276 Apr 17  2007 brarchive
-rwsr-xr-x   1 orapro dba 4750020 Apr 17  2007 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  2007 brconnect
-rwsr-xr-x   1 proadm sapsys 430467 Apr 17  2007

brrestore -rwsr-xr-x   1 orapro dba 188629 Apr 17  2007 brtools
```

Procédure d'installation

1. Installez SAP R/3 BRTOOLS sur le système d'application.
2. Installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :
   - Agent HP StorageWorks XP
   - Intégration SAP R/3
   - Agent de disque

REMARQUE :

Il n'est pas nécessaire d'installer Intégration SAP R/3 sur le système de sauvegarde si vous envisagez d'exécuter des sessions ZDB compatibles SAP lors desquelles BRBACKUP est démarré sur ce système.

Sur les systèmes Windows, les composants logiciels de Data Protector doivent être installés avec le compte administrateur SAP R/3, et ce groupe doit être inclus dans le groupe local ORA_DBA ou ORA_*SID*_DBA sur le système où l'instance SAP R/3 est exécutée.

Intégration HP StorageWorks Disk Array XP avec Microsoft Exchange Server

Condition préalable

La base de données Microsoft Exchange Server doit être installée sur le système d'application, sur les volumes (périphériques logiques) HP StorageWorks Disk Array XP qui sont mis en miroir sur le système de sauvegarde. La mise en miroir peut être BC ou CA et la base de données est installée sur un système de fichiers. Les objets suivants doivent être présents sur les volumes en miroir :

- Banque d'informations Microsoft (MIS)
- Service gestionnaire de clés (KMS, facultatif)
- Service de réplication de sites (SRS, facultatif)

Pour pouvoir sauvegarder des journaux de transactions, désactivez l'enregistrement circulaire sur le serveur Microsoft Exchange.

Procédure d'installation

Installez les composants logiciels Data Protector suivants :

- `Agent HP StorageWorks XP` - sur le système d'application et le système de sauvegarde
- `Intégration MS Exchange` - sur le système d'application uniquement

Intégration de HP StorageWorks Disk Array XP avec Microsoft SQL Server

Condition préalable

Microsoft SQL Server doit être installé sur le système d'application. Les bases de données utilisateur *doivent* se trouver sur les volumes source en baie de disques, tandis que les bases de données système peuvent être installées n'importe où. Cependant, si les bases de données système sont elles aussi installées sur la baie de disques, elles *doivent* l'être sur des volumes source *différents* de ceux des bases de données utilisateur.

Procédure d'installation

Installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :

- `Agent HP StorageWorks XP`
- `Intégration MS SQL`

Intégration HP StorageWorks Virtual Array

Pour intégrer HP StorageWorks VA à Data Protector, installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :

- `Agent HP StorageWorks VA`
- `Agent général de support`
  Installez le composant `Agent général de support` sur le système de sauvegarde pour sauvegarder les données en bloc. Installez-le sur le système d'application pour sauvegarder les journaux d'archive ou pour restaurer le système.
- `Agent de disque`
  Installez le composant `Agent de disque` sur les systèmes d'application et de sauvegarde pour exécuter des sauvegardes ZDB d'image disque et de système de fichiers. Les clients sans Agent de disque ne sont pas répertoriés dans les listes déroulantes `Système d'application` et `Système de sauvegarde` lors de la création d'une spécification ZDB.

Installation sur un cluster

Vous pouvez installer l'intégration HP StorageWorks VA dans un environnement de cluster. Pour connaître les configurations de clusters prises en charge et la configuration requise pour l'installation, reportez-vous au *Guide de l'administrateur ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Intégration à d'autres applications

Si vous souhaitez installer l'intégration HP StorageWorks VA avec une application de base de données, installez le composant Data Protector spécifique à l'intégration de cette application sur les systèmes d'application et de sauvegarde, et effectuez les tâches spécifiques à cette intégration. Vous pouvez installer l'intégration HP StorageWorks VA avec Oracle, SAP R/3, Microsoft Exchange Server et Microsoft SQL Server.

Intégration de HP StorageWorks VA avec Oracle

Configuration système requise

- Les logiciels suivants doivent être installés et configurés sur le système d'application et sur le système de sauvegarde pour la méthode de jeu de sauvegarde ZDB :
  - Oracle Enterprise Server (RDBMS) ;
  - Services Oracle Net ;
  - SQL*Plus.

  Le logiciel Oracle installé sur le système de sauvegarde doit l'être dans le même répertoire que sur le système d'application. Les binaires doivent être identiques à ceux du système d'application. Vous pouvez y parvenir en copiant les fichiers et l'environnement système du système d'application vers le système de sauvegarde ou par une installation "propre" des binaires Oracle sur le système de sauvegarde avec les mêmes paramètres d'installation que sur le système d'application.
- Les fichiers de base de données Oracle utilisés par le système d'application doivent être installés sur les volumes source qui seront dupliquées à l'aide de l'Agent VA (SNAPA).
  Selon l'emplacement du fichier de contrôle Oracle, des fichiers journaux de rétablissement en ligne et du fichier SPFILE, les deux options suivantes sont possibles :
  - Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et le fichier SPFILE résident sur un groupe de volumes (si LVM est utilisé) ou un volume source différent des fichiers de données Oracle.
    La restauration instantanée est activée par défaut dans ce type de configuration.

- Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et le fichier SPFILE résident sur le même groupe de volumes (si LVM est utilisé) ou volume source que les fichiers de données Oracle.
  Par défaut, la restauration instantanée *n'est pas* activée dans ce type de configuration. Vous pouvez l'activer en définissant les variables `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF_OLF` et `ZDB_ORA_NO_CHECKCONF_IR` de la commande `omnirc`. Pour plus d'informations, reportez-vous au *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Les fichiers journaux de rétablissement archivés Oracle ne doivent pas nécessairement résider sur des volumes source.

Procédure d'installation

Procédez aux tâches d'installation suivantes :

1. Installez la base de données du catalogue de récupération Oracle. De préférence, installez-la sur un autre système, sur des disques qui ne sont pas en miroir. Laissez le catalogue de récupération non enregistré. Pour plus d'informations sur l'installation de la base de données, reportez-vous à la documentation Oracle.
2. Installez les composants logiciels Data Protector suivants :
   - `Agent HP StorageWorks VA` - sur le système d'application et le système de sauvegarde ;
   - `Intégration Oracle` - sur le système d'application et le système de sauvegarde.

REMARQUE :

- Le composant `Intégration Oracle` Data Protector sur le système de sauvegarde n'est nécessaire que pour la méthode de jeu de sauvegarde ZDB. Il n'est pas nécessaire pour la méthode proxy-copy ZDB.
- Dans un environnement de cluster RAC, plusieurs instances Oracle accèdent à la base de données d'application Oracle. Par conséquent, installez les composants `Intégration Oracle` et `Agent HP StorageWorks VA` Data Protector sur tous les systèmes sur lesquels s'exécutent les instances Oracle.
- Si vous avez installé la base de données du catalogue de récupération Oracle sur un autre système, il n'est pas nécessaire d'y installer des composants logiciels Data Protector.

Intégration de HP StorageWorks VA avec SAP R/3

Configuration système requise

- Les logiciels Oracle suivants doivent être installés sur le système d'application :
  - Oracle Enterprise Server (RDBMS) ;
  - Services Oracle Net ;
  - SQL*Plus.
- Si vous envisagez d'exécuter des sessions ZDB compatibles SAP (BRBACKUP démarré sur le système de sauvegarde et non sur le système d'application), le système de sauvegarde doit être configuré. Pour plus de détails, reportez-vous au guide de la base de données SAP pour Oracle (sauvegarde split mirror, configuration du logiciel).
- La base de données du système d'application peut être installée sur des images disque, des volumes logiques ou des systèmes de fichiers.
  - Les fichiers de données Oracle *doivent* résider sur une baie de disques.
  - Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne ne doivent pas nécessairement résider sur une baie de disques. En revanche, pour les sessions ZDB *en ligne* compatibles SAP, les fichiers de contrôle doivent résider sur une baie de disques.
  - Pour la *sauvegarde hors ligne*, le fichier de contrôle et les journaux de rétablissement en ligne *doivent* résider sur une baie de disques.
  - Les fichiers journaux de rétablissement archivés ne doivent pas nécessairement résider sur une baie de disques.

  Si le fichier de contrôle Oracle, les journaux de rétablissement en ligne et le fichier SPFILE Oracle résident sur le *même* groupe de volume LVM ou volume source que les fichiers de données Oracle, définissez les variables `ZDB_ORA_NO_CHECKCONF_IR`, `ZDB_ORA_INCLUDE_CF_OLF` et `ZDB_ORA_INCLUDE_SPF` de la commande Data Protector `omnirc` Data Protector. Sinon, vous ne pourrez pas exécuter de sessions de sauvegarde ZDB sur disque et ZDB sur disque + bande. Pour plus d'informations, reportez-vous au *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

REMARQUE :

Si certains des fichiers de données Oracle sont installés sur des liens symboliques, créez les liens également sur le système de sauvegarde.

UNIX seulement : si la base de données Oracle est installée sur des partitions brutes (image disque ou volumes logiques bruts), vérifiez que les noms de volume/groupe de disques sont identiques sur le système d'application et le système de sauvegarde.

- Sous UNIX, vérifiez que les utilisateurs suivants sont définis sur le système d'application :
  - `ora`*`ORACLE_SID`* dans le groupe principal `dba`
  - *`ORACLE_SID`*`adm` dans le groupe UNIX `sapsys`
- Le logiciel SAP R/3 doit être correctement installé sur le système d'application. Les répertoires standard suivants doivent être installés sur le système d'application après l'installation de SAP R/3 :

REMARQUE :

L'emplacement des répertoires dépend des variables d'environnement (systèmes UNIX) ou de registre (systèmes Windows). Reportez-vous à la documentation SAP R/3 pour plus d'informations.

- *`ORACLE_HOME`*`/dbs` (systèmes UNIX)
  `ORACLE_HOME``\database` (systèmes Windows)
  - les profils Oracle et SAP)
- *`ORACLE_HOME`*`/bin` (systèmes UNIX)
  `ORACLE_HOME``\bin` (systèmes Windows)
  - les fichiers binaires Oracle
- *`SAPDATA_HOME`*`/sapbackup` (systèmes UNIX)
  `SAPDATA_HOME``\sapbackup` (systèmes Windows)
  - le répertoire SAPBACKUP des fichiers journaux BRBACKUP
- *`SAPDATA_HOME`*`/saparch` (systèmes UNIX)
  `SAPDATA_HOME``\saparch`
  (systèmes Windows) - le répertoire SAPARCH contenant les fichiers journaux BRARCHIVE
- *`SAPDATA_HOME`*`/sapreorg` (systèmes UNIX)
  `SAPDATA_HOME``\sapreorg` (systèmes Windows)
- *`SAPDATA_HOME`*`/sapcheck` (systèmes UNIX)
  `SAPDATA_HOME``\sapcheck` (systèmes Windows)
- *`SAPDATA_HOME`*`/saptrace` (systèmes UNIX)
  `SAPDATA_HOME``\saptrace` (systèmes Windows)
- `/usr/sap/`*`ORACLE_SID`*`/SYS/exe/run` (systèmes UNIX)
  BRTOOLS (systèmes Windows)

REMARQUE :

Si vous envisagez d'effectuer une restauration instantanée, vérifiez que les répertoires `sapbackup`, `saparch` et `sapreorg` figurent sur d'autres volumes source que les fichiers de données Oracle.

Systèmes UNIX

Sur les systèmes UNIX, si les six derniers répertoires ne sont pas aux emplacements indiqués ci-dessus, créez les liens appropriés vers eux.
Sur les systèmes UNIX, le propriétaire du répertoire `/usr/sap/`*`ORACLE_SID`*`/SYS/exe/run` doit être l'utilisateur UNIX `ora`*`ORACLE_SID`*. Le propriétaire des fichiers SAP R/3 doit être l'utilisateur UNIX `ora`*`ORACLE_SID`* et le groupe UNIX `dba` avec le bit setuid à 1 (chmod 4755 ...). L'exception est le fichier BRRESTORE, dont le propriétaire doit être l'utilisateur UNIX *`ORACLE_SID`*`adm`.

Exemple UNIX

Si *`ORACLE_SID`* est PRO, les droits à l'intérieur du répertoire `/usr/sap/`*`ORACLE_SID`*`/SYS/exe/run` doivent ressembler à ce qui suit :

```
-rwsr-xr-x   1 orapro dba 4598276 Apr 17  1998 brarchive
-rwsr-xr-x   1 orapro dba 4750020 Apr 17  1998 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  1998 brconnect
-rwsr-xr-x   1 proadm sapsys 430467 Apr 17  1998

brrestore
-rwsr-xr-x   1 orapro dba 188629 Apr 17  1998 brtools
```

Procédure d'installation

1. Installez SAP R/3 BRTOOLS sur le système d'application.
2. Installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :
   - `Agent HP StorageWorks VA`
   - `Intégration SAP R/3`
   - `Agent de disque`

REMARQUE :

Il n'est pas nécessaire d'installer `Intégration SAP R/3` sur le système de sauvegarde si vous envisagez d'exécuter des sessions ZDB compatibles SAP lors desquelles BRBACKUP est démarré sur ce système.

Sur les systèmes Windows, les composants logiciels de Data Protector doivent être installés avec le compte administrateur SAP R/3, et ce groupe doit être inclus dans le groupe local `ORA_DBA` ou `ORA_`*`SID`*`_DBA` sur le système où l'instance SAP R/3 est exécutée.

Intégration HP StorageWorks VA avec Microsoft Exchange Server

Condition préalable

La base de données Microsoft Exchange Server doit être installée sur les volumes source du système d'application. Les objets suivants doivent se trouver sur les volumes source :

- Banque d'informations Microsoft (MIS)
- Service gestionnaire de clés (KMS, facultatif)
- Service de réplication de sites (SRS, facultatif)

Pour pouvoir sauvegarder des journaux de transactions, désactivez l'enregistrement circulaire sur le serveur Microsoft Exchange.

Procédure d'installation

Installez les composants logiciels Data Protector suivants :

- `Agent HP StorageWorks VA` - sur le système d'application et le système de sauvegarde
- `Intégration MS Exchange` - sur le système d'application uniquement

Intégration de HP StorageWorks VA avec Microsoft SQL Server

Condition préalable

Microsoft SQL Server doit être installé sur le système d'application. Les bases de données utilisateur *doivent* se trouver sur les volumes source en baie de disques, tandis que les bases de données système peuvent être installées n'importe où. Cependant, si les bases de données système sont elles aussi installées sur la baie de disques, elles *doivent* l'être sur des volumes source *différents* de ceux des bases de données utilisateur.

Procédure d'installation

Installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :

- `Agent HP StorageWorks VA`
- `Intégration MS SQL`

Intégration HP StorageWorks Enterprise Virtual Array

Pour intégrer HP StorageWorks EVA à Data Protector, installez les composants logiciels Data Protector suivants sur les systèmes d'application et de sauvegarde :

- `Agent HP StorageWorks EVA SMI-S`
- `Agent général de support`

Installez le composant `Agent général de support` sur le système de sauvegarde pour sauvegarder les données en bloc. Installez-le sur le système d'application pour sauvegarder les journaux d'archive ou pour restaurer le système.

- `Agent de disque`
  Installez le composant `Agent de disque` sur les systèmes d'application et de sauvegarde pour exécuter des sauvegardes ZDB d'image disque et de système de fichiers. Les clients sans Agent de disque ne sont pas répertoriés dans les listes déroulantes `Système d'application` et `Système de sauvegarde` lors de la création d'une spécification ZDB.

Installation sur un cluster

Vous pouvez installer l'intégration HP StorageWorks EVA dans un environnement de cluster. Pour connaître les configurations de clusters prises en charge et la configuration requise pour l'installation, reportez-vous au *Guide de l'administrateur ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Intégration à d'autres applications

Pour installer l'intégration HP StorageWorks EVA avec une application de base de données, installez le composant Data Protector spécifique à l'intégration de cette application sur les systèmes d'application et de sauvegarde, et effectuez les tâches spécifiques à cette intégration. Vous pouvez installer l'intégration HP StorageWorks EVA avec Oracle, SAP R/3, Microsoft Exchange Server et Microsoft SQL Server et Microsoft VSS.

Intégration de HP StorageWorks EVA avec Oracle

Configuration système requise

- Les logiciels suivants doivent être installés et configurés sur le système d'application et sur le système de sauvegarde pour la méthode de jeu de sauvegarde ZDB :
  - Oracle Enterprise Server (RDBMS) ;
  - Services Oracle Net ;
  - SQL*Plus.

  Le logiciel Oracle installé sur le système de sauvegarde doit l'être dans le même répertoire que sur le système d'application. Les binaires doivent être identiques à ceux du système d'application. Vous pouvez y parvenir en copiant les fichiers et l'environnement système du système d'application vers le système de sauvegarde ou par une installation "propre" des binaires Oracle sur le système de sauvegarde avec les mêmes paramètres d'installation que sur le système d'application.

- Les fichiers de base de données Oracle du système d'application doivent être installés sur les volumes source qui seront dupliqués à l'aide de l'agent SMI-S que vous avez installé.
  Selon l'emplacement du fichier de contrôle Oracle, des fichiers journaux de rétablissement en ligne et du fichier SPFILE, les deux options suivantes sont possibles :
  - Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et le fichier SPFILE résident sur un groupe de volumes (si LVM est utilisé) ou un volume source différent des fichiers de données Oracle.
    La restauration instantanée est activée par défaut dans ce type de configuration.
  - Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et le fichier SPFILE résident sur le même groupe de volumes (si LVM est utilisé) ou volume source que les fichiers de données Oracle.
    Par défaut, la restauration instantanée *n'est pas* activée dans ce type de configuration. Vous pouvez l'activer en définissant les variables `omnirc ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF` et `ZDB_ORA_NO_CHECKCONF_IR`. Pour plus d'informations, reportez-vous au *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

  Les fichiers journaux de rétablissement archivés Oracle ne doivent pas nécessairement résider sur des volumes source.
  Si certains des fichiers de données Oracle sont installés sur des liens symboliques, vous devez créer ces liens également sur le système de sauvegarde.

Procédure d'installation

Procédez aux tâches d'installation suivantes :

1. Installez la base de données du catalogue de récupération Oracle. De préférence, installez-la sur un autre système, sur des disques qui ne sont pas en miroir. Laissez le catalogue de récupération non enregistré. Pour plus d'informations sur l'installation de la base de données, reportez-vous à la documentation Oracle.
2. Installez les composants logiciels Data Protector suivants :
   - `Agent HP StorageWorks EVA SMI-S` - à la fois sur le système d'application et le système de sauvegarde ;
   - `Intégration Oracle` - sur le système d'application et le système de sauvegarde.

REMARQUE :

- Le composant `Intégration Oracle` Data Protector sur le système de sauvegarde n'est nécessaire que pour la méthode de jeu de sauvegarde ZDB. Il n'est pas nécessaire pour la méthode proxy-copy ZDB.

- Dans un environnement de cluster RAC, plusieurs instances Oracle accèdent à la base de données d'application Oracle. Par conséquent, installez les composants `Intégration Oracle` et `Agent HP StorageWorks EVA SMI-S` Data Protector sur tous les systèmes sur lesquels s'exécutent les instances Oracle.

- Si vous avez installé la base de données du catalogue de récupération Oracle sur un autre système, il n'est pas nécessaire d'y installer des composants logiciels Data Protector.

Intégration de HP StorageWorks EVA avec SAP R/3

Configuration système requise

- Les logiciels Oracle suivants doivent être installés sur le système d'application.
  - Oracle Enterprise Server (RDBMS) ;
  - Services Oracle Net ;
  - SQL*Plus.
- Si vous envisagez d'exécuter des sessions ZDB compatibles SAP (BRBACKUP démarré sur le système de sauvegarde et non sur le système d'application), le système de sauvegarde doit être configuré. Pour plus de détails, reportez-vous au guide de la base de données SAP pour Oracle (sauvegarde split mirror, configuration du logiciel).
- La base de données du système d'application peut être installée sur des images disque, des volumes logiques ou des systèmes de fichiers.
  - Les fichiers de données Oracle *doivent* résider sur une baie de disques.
  - Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne ne doivent pas nécessairement résider sur une baie de disques. En revanche, pour les sessions ZDB *en ligne* compatibles SAP, les fichiers de contrôle doivent résider sur une baie de disques.
  - Pour la *sauvegarde hors ligne*, le fichier de contrôle et les journaux de rétablissement en ligne *doivent* résider sur une baie de disques.
  - Les fichiers journaux de rétablissement archivés ne doivent pas nécessairement résider sur une baie de disques.

  Si le fichier de contrôle Oracle, les journaux de rétablissement en ligne et le fichier SPFILE Oracle résident sur le *même* groupe de volume LVM ou volume source que les fichiers de données Oracle, définissez les variables `ZDB_ORA_NO_CHECKCONF_IR`, `ZDB_ORA_INCLUDE_CF_OLF` et `ZDB_ORA_INCLUDE_SPF` de la commande Data Protector `omnirc` Data Protector. Sinon, vous ne pourrez pas exécuter de sessions de sauvegarde ZDB sur disque et ZDB sur disque + bande. Pour plus d'informations, reportez-vous

au *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

REMARQUE :

Si certains des fichiers de données Oracle sont installés sur des liens symboliques, créez les liens également sur le système de sauvegarde.

UNIX seulement : si la base de données Oracle est installée sur des partitions brutes (image disque ou volumes logiques bruts), vérifiez que les noms de volume/groupe de disques sont identiques sur le système d'application et le système de sauvegarde.

- Sous UNIX, vérifiez que les utilisateurs suivants sont définis sur le système d'application :
  - `ora`*`ORACLE_SID`* dans le groupe principal `dba`
  - *`ORACLE_SID`*`adm` dans le groupe UNIX `sapsys`
- Le logiciel SAP R/3 doit être correctement installé sur le système d'application. Les répertoires standard suivants doivent être installés sur le système d'application après l'installation de SAP R/3 :

REMARQUE :

L'emplacement des répertoires dépend des variables d'environnement (systèmes UNIX) ou de registre (systèmes Windows). Reportez-vous à la documentation SAP R/3 pour plus d'informations.

- *`ORACLE_HOME`*`/dbs` (systèmes UNIX) *`ORACLE_HOME`*`\database` (systèmes Windows) - les profils Oracle et SAP)
- *`ORACLE_HOME`*`/bin` (systèmes UNIX) *`ORACLE_HOME`*`\bin` (systèmes Windows) - les fichiers binaires Oracle
- *`SAPDATA_HOME`*`/sapbackup` (systèmes UNIX) *`SAPDATA_HOME`*`\sapbackup` (systèmes Windows) - le répertoire SAPBACKUP avec fichiers journaux BRBACKUP
- *`SAPDATA_HOME`*`/sapbarch` (systèmes UNIX) *`SAPDATA_HOME`*`\sapbarch` (systèmes Windows) - le répertoire SAPARCH avec fichiers journaux BRARCHIVE
- *`SAPDATA_HOME`*`/sapreorg` (systèmes UNIX) *`SAPDATA_HOME`*`\sapreorg` (systèmes Windows)
- *`SAPDATA_HOME`*`/sapcheck` (systèmes UNIX) *`SAPDATA_HOME`*`\sapcheck` (systèmes Windows)
- *`SAPDATA_HOME`*`/saptrace` (systèmes UNIX) *`SAPDATA_HOME`*`\saptrace` (systèmes Windows)
- `/usr/sap/`*`ORACLE_SID`*`/SYS/exe/run` (systèmes UNIX) `c:\Oracle\`*`ORACLE_SID`*`\sys\exe\run` (systèmes Windows)

REMARQUE :

Si vous envisagez d'effectuer une restauration instantanée, vérifiez que les répertoires `sapbackup`, `saparch` et `sapreorg` figurent sur d'autres volumes source que les fichiers de données Oracle.

Systèmes UNIX

Sur les systèmes UNIX, si les six derniers répertoires ne sont pas aux emplacements indiqués ci-dessus, créez les liens appropriés vers eux.
Sur les systèmes UNIX, le propriétaire du répertoire `/usr/sap/`*`ORACLE_SID`*`/SYS/exe/run` doit être l'utilisateur UNIX `ora`*`ORACLE_SID`*. Le propriétaire des fichiers SAP R/3 doit être l'utilisateur UNIX `ora`*`ORACLE_SID`* et le groupe UNIX `dba` avec le bit setuid à 1 (chmod 4755 ...). L'exception est le fichier BRRESTORE, dont le propriétaire doit être l'utilisateur UNIX *`ORACLE_SID`*`adm`.

Exemple UNIX

Si *`ORACLE_SID`* est PRO, les droits à l'intérieur du répertoire `/usr/sap/PRO/SYS/exe/run` doivent ressembler à ce qui suit :

```
-rwsr-xr-x   1 orapro dba 4598276 Apr 17  2007 brarchive
-rwsr-xr-x   1 orapro dba 4750020 Apr 17  2007 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  2007 brconnect
-rwsr-xr-x   1 proadm sapsys 430467 Apr 17  2007

brrestore
-rwsr-xr-x   1 orapro dba 188629 Apr 17  2007 brtools
```

Procédure d'installation

1. Installez SAP R/3 BRTOOLS sur le système d'application.
2. Installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :
   - `Agent HP StorageWorks EVA SMI-S`
   - `Intégration SAP R/3`
   - `Agent de disque`

REMARQUE :

Il n'est pas nécessaire d'installer `Intégration SAP R/3` sur le système de sauvegarde si vous envisagez d'exécuter des sessions ZDB compatibles SAP lors desquelles BRBACKUP est démarré sur ce système.

Sur les systèmes Windows, les composants logiciels de Data Protector doivent être installés avec le compte administrateur SAP R/3, et ce groupe doit être inclus dans le groupe local `ORA_DBA` ou `ORA_`*`SID`*`_DBA` sur le système où l'instance SAP R/3 est exécutée.

Intégration HP StorageWorks EVA avec Microsoft Exchange Server

Condition préalable

La base de données Microsoft Exchange Server doit être installée sur les volumes source du système d'application. Les objets suivants doivent se trouver sur les volumes source :

- Banque d'informations Microsoft (MIS)
- Service gestionnaire de clés (KMS, facultatif)
- Service de réplication de sites (SRS, facultatif)

Pour pouvoir sauvegarder des journaux de transactions, désactivez l'enregistrement circulaire sur le serveur Microsoft Exchange.

Procédure d'installation

Installez les composants logiciels Data Protector suivants :

- `Agent HP StorageWorks EVA SMI-S` à la fois sur le système d'application et le système de sauvegarde
- `Intégration MS Exchange` - sur le système d'application uniquement

Intégration de HP StorageWorks EVA avec MS SQL

Condition préalable

Microsoft SQL Server doit être installé sur le système d'application. Les bases de données utilisateur *doivent* se trouver sur les volumes source en baie de disques, tandis que les bases de données système peuvent être installées n'importe où. Cependant, si les bases de données système sont elles aussi installées sur la baie de disques, elles *doivent* l'être sur des volumes sources *différents* de ceux des bases de données utilisateur.

Procédure d'installation

Installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :

- `Agent HP StorageWorks EVA SMI-S` à la fois sur le système d'application et le système de sauvegarde
- `Intégration MS SQL`

Clients IAP

L'intégration de Data Protector avec HP Integrated Archive Platform (IAP) permet de sauvegarder les données directement dans le système IAP. Cette solution tire le meilleur parti des puissantes fonctionnalités d'IAP, telles que la capacité de contenir plusieurs téraoctets de données, l'élimination des redondances dans les données stockées, des outils de recherche perfectionnés et des restaurations ponctuelles de fichiers individuels fiables et rapides.

Pour intégrer IAP avec Data Protector, installez les composants logiciels Data Protector suivants sur le système client :

- `Extension de l'agent de disque IAP`
- `Agent de déduplication IAP`

Configuration requise

Avant de lancer l'installation, effectuez les opérations suivantes dans l'IAP :

1. Configurez la DAS (Domain Account Synchronization) pour connecter l'IAP à Microsoft Active Directory. Importez dans l'IAP un sous-ensemble d'utilisateurs de domaine qui pourront alors accéder à l'IAP. Pour plus d'informations, voir la documentation de HP File Gateway et IAP.
2. Ajoutez l'utilisateur qui exécutera les sauvegardes IAP au groupe d'utilisateurs de l'application dans l'IAP :

   `/opt/fg/fgcreate appuser` *`nom_du_compte`* `[-d | --description` *`description`*`]` *`mot_de_passe`*

   Pour vérifier si un utilisateur donné fait partie du groupe d'utilisateurs de l'application, exécutez la commande :

   `/opt/fg/fglist appusers`

3. Enregistrez le système à utiliser pour les sauvegardes. Pour les sauvegardes avec Data Protector, cela implique l'importation du serveur IAP dans la cellule. Avant cette opération, une règle d'enregistrement doit être définie, c'est-à-dire un modèle correspondant au système enregistré. Pour cela, exécutez la commande :

   `/opt/fg/fgcreate regrule` *`nom_de_la_règle`* `[-h | --hostdns` *`dns-regex`*`] [-n | --network` *`adresse_réseau`*`]` *`nom_du_domaine_iap`*, par exemple :

   ```
   /opt/fg/fgcreate regrule testRule -h test.*\.mydomain\.com$
   iap
   ```

   L'exemple ci-dessus permet d'enregistrer les systèmes dont les noms commencent par test et qui se trouvent dans `mydomain.com`. Le système est enregistré et l'AIP lui attribue un ID client. Si le système n'est pas enregistré, les sauvegardes avec Data Protector échoueront. Pour vérifier que la règle d'enregistrement est créée, exécutez la commande :

   ```
   /opt/fg/fglist regrules
   ```

Pour plus d'informations, voir le guide utilisateur de *HP File Gateway*.

En outre, téléchargez le certificat d'accès au système IAP dans le Gestionnaire de cellule et importez au moins un serveur IAP dans la cellule Data Protector.

Clients d'auto-migration VLS

La fonction de copie de supports de Data Protector vous permet de copier des supports après une sauvegarde. L'intégration avec HP StorageWorks Virtual Library System (VLS) améliore cette fonctionnalité en offrant une solution qui associe les fonctions de copie internes de VLS aux fonctions de gestion et de suivi des supports de Data Protector.

Pour intégrer Data Protector avec l'auto-migration VLS pour réaliser des copies de supports intelligentes, installez les composants logiciels d'`auto-migration VLS` Data Protector.

Configuration requise

Effectuez les opérations suivantes :

1. Configurez le stockage virtuel VLS selon la configuration requise en utilisant Command View VLS. Pour plus d'informations, voir la documentation de VLS.
2. Connectez une ou plusieurs bibliothèques physiques au VLS.
3. Importez le client VLS dans la cellule Data Protector.

Installation de l'interface utilisateur localisée de Data Protector

Data Protector A.06.10 dispose d'une interface graphique utilisateur localisée de Data Protector sur les systèmes Windows et UNIX. Elle se compose de l'interface graphique utilisateur et de l'interface de ligne de commande de Data Protector localisées. L'aide en ligne et la documentation papier sont également disponibles en version localisée. Pour savoir quels sont les manuels Data Protector localisés, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.

REMARQUE :

Le support de langue anglais est installé par défaut pendant l'installation de Data Protector. Lorsque vous installez un support de langue supplémentaire, l'interface utilisateur localisée de Data Protector démarre en fonction de l'environnement local paramétré sur le système.

Installation de l'interface utilisateur localisée de Data Protector sur les systèmes Windows

Installation en local

Pour installer l'interface utilisateur localisée de Data Protector sur des systèmes Windows, sélectionnez le support de langue approprié (français ou japonais) dans la page Installation personnalisée de l'assistant d'installation, comme indiqué à la Figure 24 à la page 181.

Pour connaître la procédure d'installation en local, reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 42.

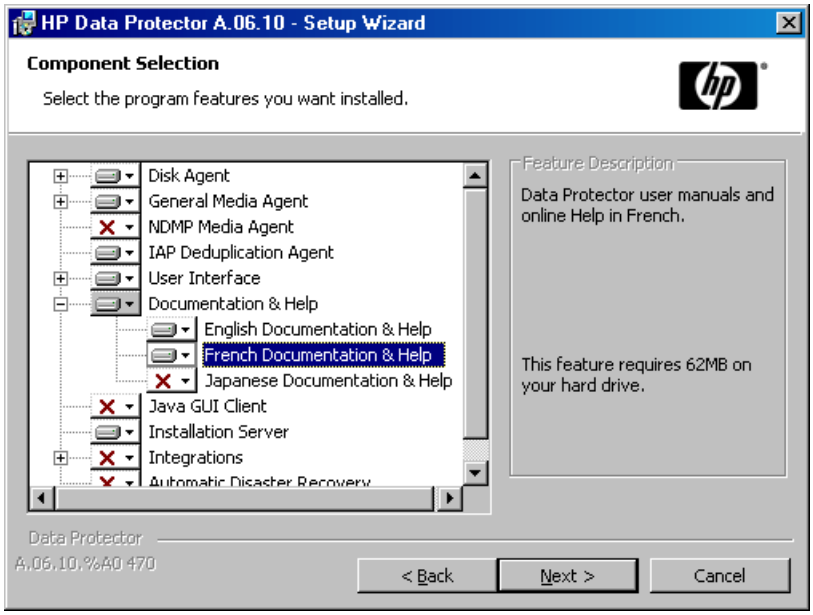

Figure 24 - Sélection du support de langue lors de l'installation

Installation distante

Lors de la distribution à distance du support de langue de Data Protector à l'aide du Serveur d'installation, sélectionnez le support de langue approprié dans la page Sélection des composants de l'assistant Ajouter composants, comme indiqué à la Figure 25 à la page 182.

Pour connaître la procédure pour ajouter à distance des composants logiciels Data Protector à des clients, reportez-vous à la section "Installation distante de clients Data Protector" à la page 78.

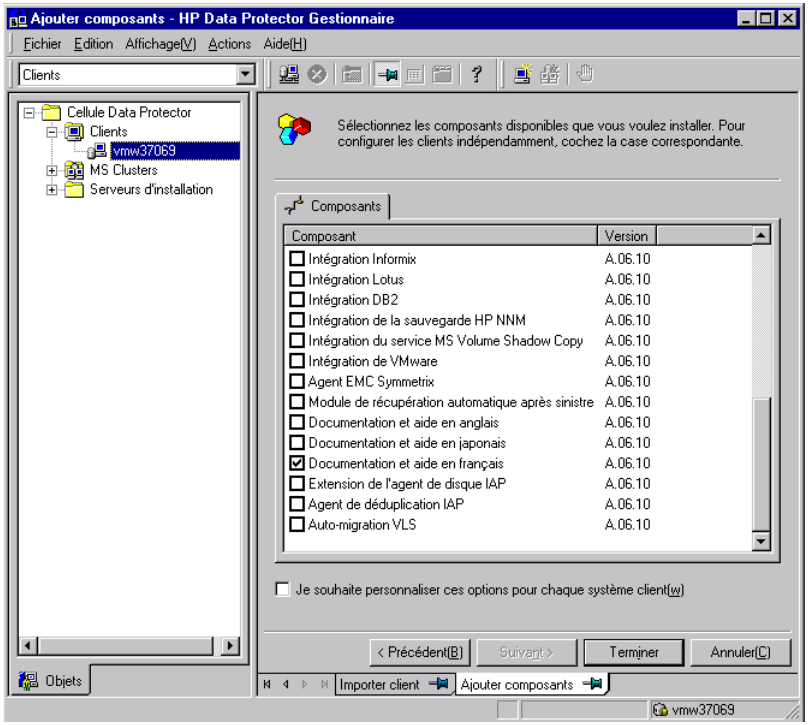

Figure 25 - Installation à distance du support de langue

Installation de l'interface utilisateur localisée de Data Protector sur les systèmes UNIX

Installation en local

Vous pouvez installer en local le support de langue japonais ou français uniquement sur un client Data Protector à l'aide de la commande `omnisetup.sh`. Spécifiez le composant logiciel `jpn_ls` ou `fra_ls`, en fonction du support de langue dont vous avez besoin. Pour connaître la procédure détaillée, reportez-vous à la section "Installation locale de clients UNIX" à la page 142.

Si vous utilisez l'utilitaire `swinstall`, `pkgadd` ou `rpm` pour installer le Gestionnaire de cellule ou le Serveur d'installation de Data Protector, vous ne pouvez installer que le support de langue anglais. Si vous souhaitez que l'interface utilisateur localisée de Data Protector réside sur le même système que le Gestionnaire de cellule ou le Serveur d'installation, vous devez installer le support de langue supplémentaire à distance.

Installation distante

Lors de la distribution à distance du support de langue de Data Protector à l'aide du Serveur d'installation, sélectionnez le support de langue approprié dans la page Sélection des composants de l'assistant Ajouter composants, comme indiqué à la Figure 25 à la page 182.

Pour connaître la procédure pour ajouter à distance des composants logiciels Data Protector à des clients, reportez-vous à la section "Installation distante de clients Data Protector" à la page 78.

Dépannage

Si la version anglaise de l'interface utilisateur d'origine de Data Protector démarre après que vous avez installé un support de langue différent, effectuez les vérifications suivantes :

1. Assurez-vous que les fichiers suivants existent :

   Pour le support de langue français :

   - Sous Windows : `répertoire_Data_Protector\bin\OmniFra.dll`
   - Sous HP-UX : `/opt/omni/lib/nls/fr.iso88591/omni.cat`
   - Sous Solaris : `/opt/omni/lib/nls/fr.ISO8859-1/omni.cat`

   Pour le support de langue japonais :

   - Sous Windows : `répertoire_Data_Protector\bin\OmniJpn.dll`
   - Sous HP-UX : `/opt/omni/lib/nls/ja.eucJP/omni.cat` et `/opt/omni/lib/nls/ja.SJIS/omni.cat`
   - Sous Solaris : `/opt/omni/lib/nls/ja.eucJP/omni.cat` et `/opt/omni/lib/nls/ja.PCK/omni.cat`

2. Vérifiez les paramètres régionaux sur votre système :
   - Sous Windows : dans le `Panneau de configuration` de Windows, cliquez sur `Options régionales` et vérifiez que la langue sélectionnée dans les paramètres régionaux et de langue est appropriée.
   - Sous UNIX : exécutez la commande suivante pour configurer les paramètres régionaux :
     `export LANG=langue locale`
     où *`langue`* représente le paramètre régional dans le format suivant :
     `langue[_région].jeu de code.`
     Par exemple, `ja_JP.eucJP`, `ja_JP.SJIS` ou `ja_JP.PCK` pour le paramètre régional japonais et `fr_FR.iso88591` pour le paramètre régional français. Notez que la partie jeu de code de la variable `LANG` est obligatoire et doit correspondre à la partie jeu de code du nom du répertoire apparenté.

Installation de l'Edition serveur unique de Data Protector

L'Edition serveur unique (SSE) de Data Protector est conçue pour les environnements restreints dans lesquels les sauvegardes s'exécutent sur un seul périphérique connecté à un Gestionnaire de cellule. Elle est disponible pour les plates-formes Windows prises en charge ainsi que pour les plates-formes HP-UX et Solaris.

Pour installer le Gestionnaire de cellule et (le cas échéant) le Serveur d'installation, suivez les instructions figurant dans la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 42.

Limites

Lorsque vous examinez la licence de l'Edition serveur unique, tenez compte des limites suivantes :

Limites de l'Edition serveur unique pour Windows

- L'Edition serveur unique prend en charge les sauvegardes vers un seul périphérique à la fois, lequel est connecté à un seul Gestionnaire de cellule.
- Elle ne prend en charge qu'un changeur automatique DDS à 10 emplacements.
- Elle ne prend en charge ni les clients, ni les serveurs UNIX (et HP-UX). Si vous essayez d'effectuer une sauvegarde sur une machine UNIX, la session est abandonnée.
- Si une cellule contient un Gestionnaire de cellule Windows, vous ne pouvez sauvegarder que des clients Windows. L'Edition serveur unique ne prend pas en charge la sauvegarde vers les clients Novell NetWare.
- L'ajout de produits d'extension n'est pas pris en charge par l'Edition serveur unique.
- La gestion de clusters n'est pas prise en charge par l'Edition serveur unique.
- La récupération après sinistre n'est pas prise en charge.

Le nombre de clients Windows n'est pas limité.

Pour connaître les périphériques pris en charge, reportez-vous aux Références, notes de publication et annonces produits HP Data Protector.

Limites de l'Edition serveur unique pour HP-UX et Solaris

- L'Edition serveur unique prend en charge les sauvegardes vers un seul périphérique à la fois, lequel est connecté à un seul Gestionnaire de cellule.
- Elle ne prend en charge qu'un changeur automatique DDS à 10 emplacements.

- Sur un Gestionnaire de cellule UNIX, vous ne pouvez pas sauvegarder des serveurs, mais seulement des clients UNIX, des clients Windows, des clients Solaris et des clients Novell NetWare.
- L'ajout de produits d'extension n'est pas pris en charge par l'Edition serveur unique.
- La gestion de clusters n'est pas prise en charge par l'Edition serveur unique.

Le nombre de clients (UNIX, Windows) n'est pas limité.

Pour connaître les périphériques pris en charge, reportez-vous aux Références, notes de publication et annonces produits HP Data Protector.

Installation d'un mot de passe

Pour obtenir des instructions détaillées sur l'installation d'un mot de passe sur le Gestionnaire de cellule, reportez-vous à la section "Mots de passe Data Protector" à la page 321.

Installation des Rapports Web de Data Protector

Le composant Rapports Web de Data Protector est installé par défaut avec d'autres composants Data Protector et à ce titre, vous pouvez l'utiliser en local à partir de votre système.

Vous pouvez également l'installer sur un serveur Web et ainsi le rendre disponible sur les autres systèmes, sur lesquels l'installation des composants logiciels Data Protector n'est pas obligatoire.

Configuration système requise

Pour utiliser la génération de rapports Web de Data Protector sur votre système, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector* pour connaître la configuration requise et les limites.

Installation

Procédez comme suit pour installer le composant Rapports Web Data Protector sur un serveur Web :

1. Copiez les fichiers de rapport Java Data Protector suivants sur le serveur. Il n'est pas nécessaire que le serveur soit un client Data Protector.
   - Sur les systèmes Windows disposant de l'interface utilisateur Data Protector, les fichiers se trouvent dans le répertoire suivant : `répertoire_Data_Protector\java\bin`
   - Sur un système UNIX disposant de l'interface utilisateur Data Protector, les fichiers se trouvent dans le répertoire suivant : `/opt/omni/java/bin`

2. Ouvrez le fichier `WebReporting.html` dans votre navigateur pour accéder aux Rapports Web de Data Protector.

   Vous devez rendre le fichier disponible aux utilisateurs des Rapports Web sous forme d'URL complète. Par exemple, vous pouvez placer un lien vers ce fichier à partir de votre site Intranet.

CONSEIL :

Aucun mot de passe n'est requis par défaut pour utiliser les Rapports Web Data Protector. Vous pouvez cependant en indiquer un et restreindre ainsi l'accès aux Rapports Web. Pour connaître la procédure à suivre, reportez-vous à l'index de l'aide en ligne (rubrique "rapports Web, restriction d'accès").

Etape suivante

Une fois l'installation terminée, reportez-vous à l'index de l'aide en ligne (rubrique "interface de génération de rapports Web, configuration de notifications") pour plus d'informations sur les questions de configuration et la création de rapports personnalisés.

Installation de Data Protector sur MC/ServiceGuard

Data Protector prend en charge MC/ServiceGuard (MC/SG) pour HP-UX et Linux. Pour obtenir des informations détaillées sur les versions de systèmes d'exploitation prises en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.

Si votre Gestionnaire de cellule doit être compatible cluster, notez que l'adresse IP du serveur virtuel doit être utilisée pour les licences.

Installation d'un Gestionnaire de cellule compatible cluster

Configuration système requise

Avant d'installer un Gestionnaire de cellule Data Protector sur MC/ServiceGuard, vérifiez les éléments suivants :

- Décidez quels systèmes seront les Gestionnaires de cellule principal et secondaire. Ils doivent tous être équipés de MC/ServiceGuard et configurés en tant que membres du cluster.
- Data Protector Le Gestionnaire de cellule doté des correctifs recommandés, ainsi que tous les autres composants logiciels Data Protector des intégrations que vous souhaitez intégrer au cluster doivent être installés sur le nœud principal et sur chaque nœud secondaire.

La procédure d'installation est la procédure standard d'installation du système du Gestionnaire de cellule. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 42.

Etape suivante

Une fois l'installation terminée, vous devez configurer les Gestionnaires de cellule principal et secondaire, ainsi que le package de Gestionnaire de cellule. Reportez-vous à l'index de l'aide en ligne (rubrique "cluster, MC/ServiceGuard") pour plus d'informations sur la configuration de MC/ServiceGuard avec Data Protector.

Installation d'un client compatible cluster

IMPORTANT :

Les clients Data Protector compatibles cluster doivent être installés sur tous les nœuds de clusters.

La procédure d'installation est la procédure standard d'installation de Data Protector sur un client UNIX. Pour connaître la procédure détaillée, reportez-vous aux sections "Installation de clients HP-UX" à la page 94 et "Installation de clients Linux" à la page 103.

Etape suivante

Lorsque vous avez terminé l'installation, vous devez importer le serveur virtuel (nom d'hôte spécifié dans le package de clusters) dans la cellule Data Protector. Reportez-vous à la section "Importation d'un client compatible cluster dans une cellule" à la page 208.

Reportez-vous à *l'index de l'aide en ligne (rubrique "configuration")* pour plus d'informations sur la configuration de périphériques de sauvegarde ou de pools de supports ou sur toute autre tâche de configuration de Data Protector.

Installation de Data Protector sur Microsoft Cluster Server

Pour connaître les systèmes d'exploitation pour l'intégration Microsoft Cluster Server, reportez-vous au site http://www.hp.com/support/manuals.

Si votre Gestionnaire de cellule doit être compatible cluster, notez que l'adresse IP du serveur virtuel doit être utilisée pour les licences.

Installation d'un Gestionnaire de cellule compatible cluster

Configuration système requise

Avant d'installer le Gestionnaire de cellule compatible cluster, assurez-vous qu'il n'y a pas sur le cluster de ressources portant les noms suivants :

`OBVS_MCRS`, `OBVS_VELOCIS`, `OmniBack_Share`

S'il en existe, et que vous effectuez une nouvelle installation (pas une mise à niveau), vous devez supprimer ou renommer ces ressources car Data Protector utilise ces noms pour le serveur virtuel Data Protector.

Pour ce faire, procédez comme suit :

1. Cliquez sur Démarrer > Programmes >Outils d'administration > Administrateur de clusters.
2. Vérifiez la liste des ressources afin de les supprimer ou de les renommer, le cas échéant.

Pour installer et configurer correctement Data Protector dans un environnement Microsoft Cluster Server, vous devez fournir un compte disposant des droits utilisateur appropriés :

- Droits d'administrateur sur le Gestionnaire de cellule
- Droits administrateur de clusters dans le cluster
- Le mot de passe n'expire jamais
- Connexion comme un service
- L'utilisateur ne peut pas changer de mot de passe
- Tous les horaires d'accès sont autorisés

REMARQUE :

Lorsque vous installez un Gestionnaire de cellule Data Protector en tant qu'élément compatible cluster dans un environnement Microsoft Cluster, le compte utilisateur Data Protector doit être un compte d'utilisateur du domaine disposant de tous les droits mentionnés ci-dessus.

CONSEIL :

Pour installer un serveur de clusters, vous devez disposer d'un compte doté de droits d'administrateur sur tous les systèmes de clusters. Il est recommandé d'utiliser également ce compte pour installer Data Protector. Des droits utilisateur incorrects peuvent entraîner l'exécution de services Data Protector au mode standard au lieu du mode compatible cluster.

Avant d'installer le logiciel du Gestionnaire de cellule sur un cluster, vérifiez les éléments suivants :

- Un cluster doit être installé correctement avec la totalité de ses fonctions. Par exemple, vous devez pouvoir déplacer des groupes d'un nœud à l'autre autant de fois que cela est nécessaire, et ce sans aucun problème de disque partagé.
- Un groupe au moins du cluster doit disposer d'une ressource de cluster de fichiers définie. Data Protector installera certains de ses fichiers de données dans un dossier particulier de cette ressource de cluster de fichiers.
  Sous Windows Server 2008, les fichiers de données sont installés dans le dossier de la ressource `Serveur de fichiers` sélectionné par l'utilisateur lors de l'installation.
  Sur les autres systèmes Windows, les fichiers de données sont installés dans le dossier de la ressource `Partage de fichiers` défini lors de la création de la ressource de cluster de fichiers.
  Reportez-vous à la documentation propre aux clusters pour savoir comment définir une ressource de cluster de fichiers. Notez que le nom de partage de fichiers de cette ressource ne peut pas être `OmniBack`.
- Soit le serveur virtuel n'existe pas dans le même groupe en tant que ressource de cluster de fichiers, soit vous devez créer un serveur virtuel en utilisant une adresse IP libre enregistrée et en lui associant un nom de réseau.
- La ressource de cluster de fichiers dans laquelle Data Protector sera installé doit disposer d'une *adresse IP*, d'un *nom de réseau* et d'un ensemble de *disques physiques* parmi ses dépendances. Cela permet l'exécution du groupe de clusters Data Protector sur n'importe quel nœud, indépendamment de tout autre groupe.
- Vérifiez que seul l'administrateur de clusters a accès au dossier partagé de la ressource de cluster de fichiers et qu'il dispose d'un accès complet.
- L'installation doit être démarrée sous le compte de service cluster sur le système (nœud) sur lequel la ressource de cluster de fichiers est active, afin de permettre un accès direct à son dossier partagé. Le propriétaire de la ressource (le système sur lequel elle est active) peut être déterminé à l'aide de l'Administrateur de clusters.
- Chaque système du cluster doit être en cours d'exécution.
- Si le logiciel Data Protector est installé sur un système en tant que non compatible cluster, vous devez le désinstaller avant de procéder à l'installation. L'option de mise à niveau n'est prise en charge que si le logiciel Data Protector installé auparavant est le Gestionnaire de cellule compatible cluster.
- Data Protector doit être installé au même emplacement (lecteur et chemin d'accès) sur tous les nœuds de cluster. Assurez-vous que ces emplacements sont libres.
- Vérifiez qu'aucune autre installation basée sur Microsoft Installer n'est en cours d'exécution sur d'autres nœuds du cluster.

Installation en local

Vous devez installer en local le logiciel du Gestionnaire de cellule Data Protector compatible cluster à partir du DVD-ROM. Pour ce faire, procédez comme suit :

1. Insérez le DVD-ROM d'installation Windows.

   Sous Windows Server 2008, la fenêtre Contrôle du compte utilisateur s'affiche. Cliquez sur Continuer pour poursuivre l'installation.

2. Dans la fenêtre HP Data Protector, cliquez sur Installer Data Protector pour lancer l'assistant d'installation Data Protector.

3. Suivez les instructions de l'assistant et lisez attentivement le contrat de licence. Si vous en acceptez les termes, cliquez sur Suivant pour continuer.

4. Dans la page Type d'installation, sélectionnez Gestionnaire de cellule, puis cliquez sur Suivant pour installer le Gestionnaire de cellule Data Protector.

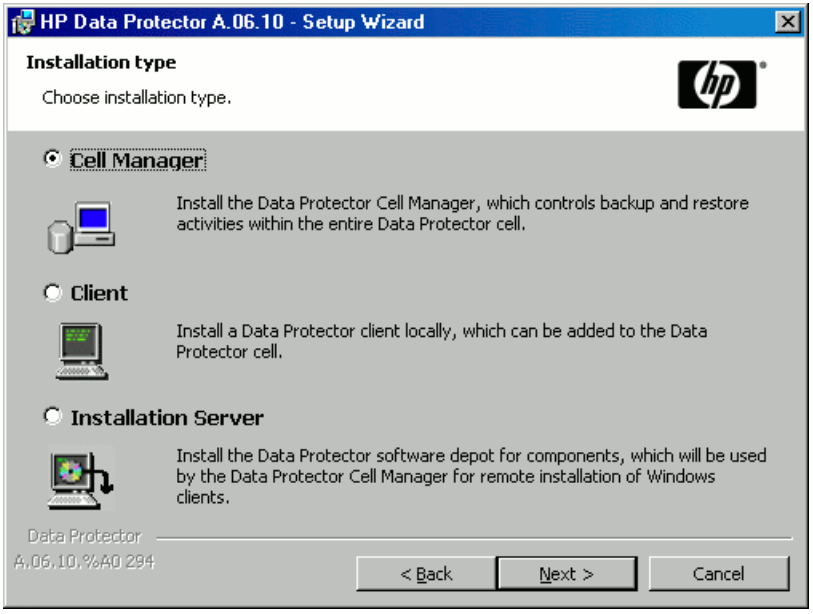

Figure 26 - Sélection du type d'installation

5. Le processus d'installation détecte automatiquement qu'il fonctionne dans un environnement de clusters. Sélectionnez Install cluster-aware Cell Manager (Installation du Gestionnaire de cellule compatible cluster) pour activer la configuration d'un cluster.

   Sélectionnez le groupe de clusters, le nom d'hôte virtuel et la ressource de cluster de fichiers sur laquelle résideront les fichiers partagés et la base de données de Data Protector.

REMARQUE :

Si vous sélectionnez Install Gestionnaire de cellule on this node only (Installer le Gestionnaire de cellule sur ce noeud uniquement), le Gestionnaire de cellule *ne* sera *pas* compatible cluster. Reportez-vous à la section "Installation d'un Gestionnaire de cellule Windows" à la page 52.

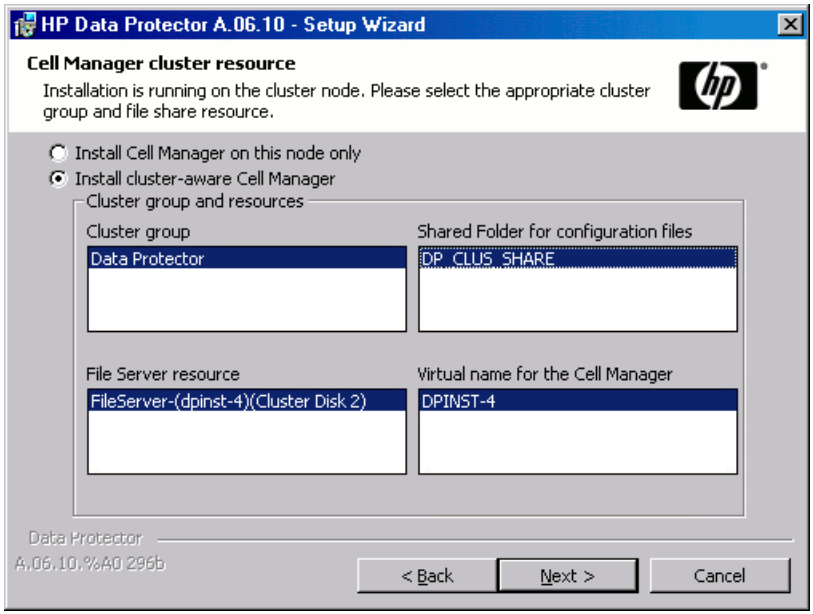

Figure 27 - Sélection de la ressource de cluster sous Windows Server 2008

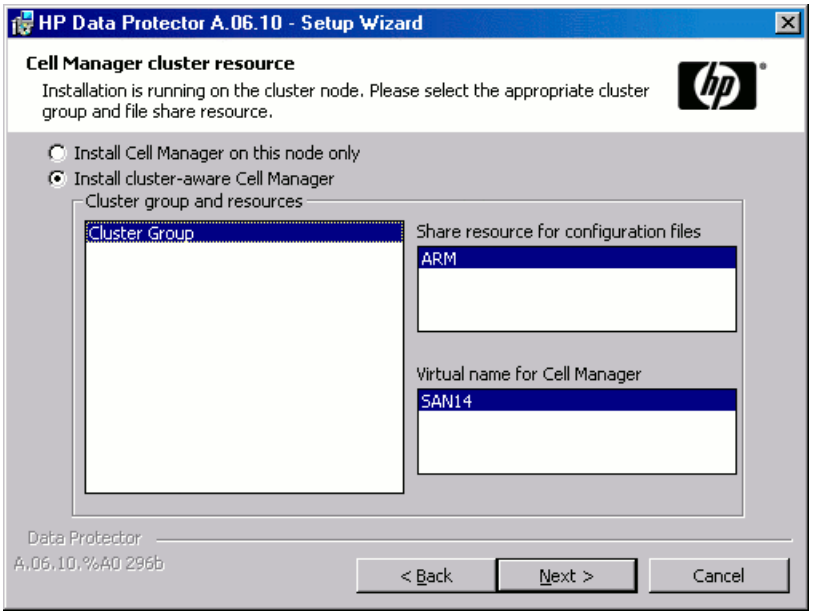

Figure 28 - Sélection de la ressource de cluster sur les autres systèmes Windows

6. Saisissez le nom d'utilisateur et le mot de passe correspondant au compte qui sera utilisé pour lancer les services Data Protector.

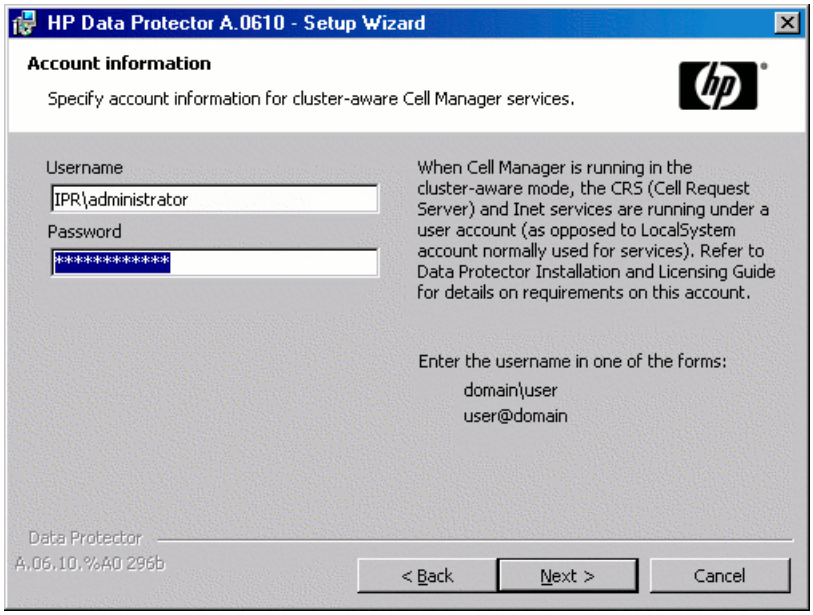

Figure 29 - Saisie des informations relatives au compte

7. Cliquez sur Suivant pour installer Data Protector dans le répertoire par défaut.

Sinon, cliquez sur Modifier pour ouvrir la fenêtre Modifier le dossier de destination actuel et entrez un autre chemin.

8. Dans la fenêtre Sélection des composants, sélectionnez les composants que vous souhaitez installer sur tous les nœuds cluster et les serveurs virtuels cluster. Cliquez sur Suivant.

   Le composant Prise en charge MS Cluster est automatiquement activé.

   Les composants sélectionnés seront installés sur tous les noeuds du cluster.

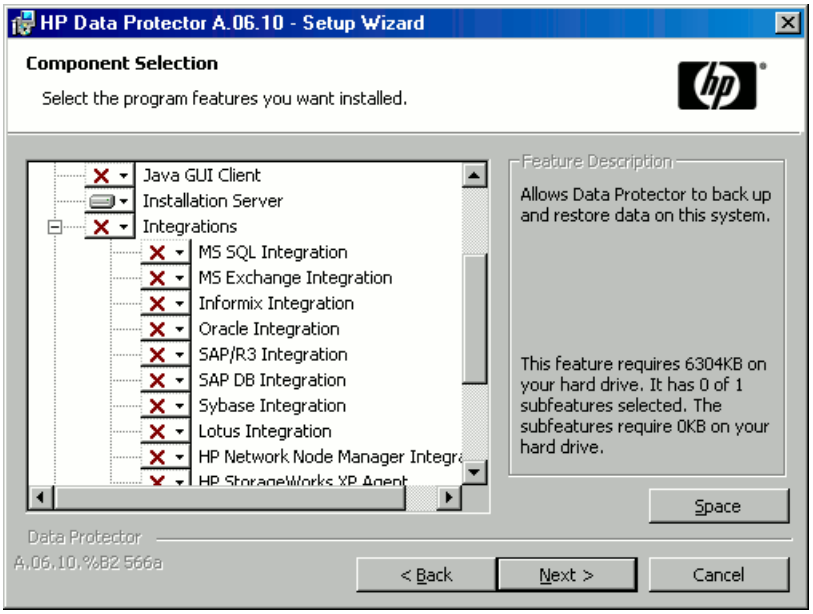

Figure 30 - Page de sélection des composants

9. La liste des composants sélectionnés s'affiche. Cliquez sur Installer.

10. La page Installation setup (Configuration de l'installation) s'affiche. Cliquez sur Suivant.

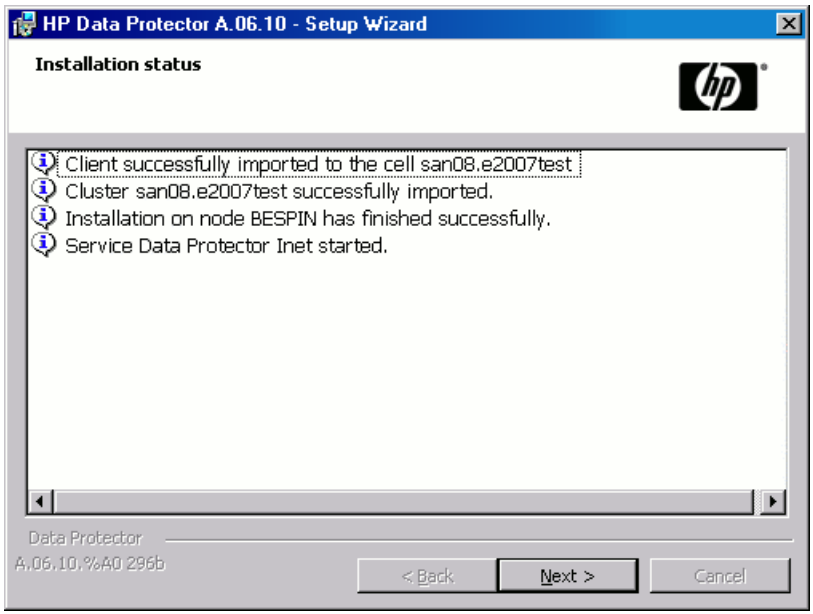

Figure 31 - Page d'état de l'installation

11. Pour commencer à utiliser Data Protector immédiatement après son installation, sélectionnez Start the Data Protector Manager (Lancer l'interface graphique du gestionnaire Data Protector).

    Pour consulter les *Références, notes de publication et annonces produits HP Data Protector*, sélectionnez Ouvrir les annonces sur les produits.

    Pour installer ou mettre à niveau l'utilitaire HP AutoPass, sélectionnez l'option Start AutoPass installation (Démarrer l'installation d'AutoPass) ou Upgrade AutoPass installation (Mettre à niveau l'installation d'AutoPass).

    Il n'est *pas* recommandé d'installer l'utilitaire HP AutoPass sur Microsoft Cluster, car il ne serait installé que sur le nœud utilisé pour l'installation. Si vous avez installé AutoPass, vous devez désinstaller Data Protector du même nœud sur lequel il était installé, une fois que vous décidez de supprimer Data Protector du système.

    AutoPass n'est pas installé *sur les systèmes d'exploitation Windows 2000 et 2003 x64, Windows Vista x64 et Windows Server 2008 x64*.

    Cliquez sur Terminer pour terminer l'installation.

Vérification de l'installation

Une fois l'installation terminée, vous pouvez vous assurer que le logiciel Data Protector a été installé correctement. Pour ce faire, procédez comme suit :

1. Vérifiez si le compte de service cluster est affecté au service `Inet` Data Protector sur chaque nœud du cluster. Vérifiez que le même utilisateur est également ajouté au groupe d'utilisateurs Admin de Data Protector. Le type de compte de connexion défini doit être `Ce compte` comme illustré dans la Figure 32 à la page 196 et la .

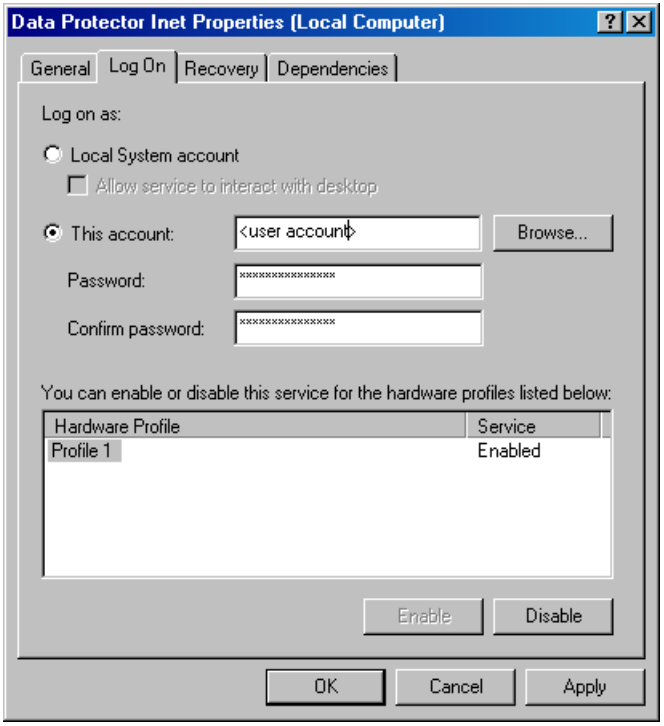

Figure 32 - Compte utilisateur Data Protector

2. Basculez vers le répertoire *répertoire_Data_Protector*`\bin` et exécutez la commande suivante :

   `omnirsh` *`hôte`* `INFO_CLUS`

   où *`hôte`* est le nom du serveur virtuel cluster (sensible à la casse). Le résultat doit contenir la liste des noms des systèmes se trouvant dans le cluster et le nom du serveur virtuel. Si `0 "NONE"` est affiché, Data Protector n'est pas installé en mode compatible cluster.

3. Lancez l'interface graphique utilisateur de Data Protector, sélectionnez le contexte Clients, puis cliquez sur MS Clusters. Les systèmes récemment installés doivent apparaître dans la zone de résultats.

Services Inet et CRS de Data Protector

Si nécessaire, modifiez les comptes sous lesquels s'exécutent les services Inet et CRS de Data Protector.

Installation de clients compatibles cluster

Configuration système requise

Avant d'installer un client Data Protector compatible cluster, les conditions préalables suivantes doivent être remplies :

- Un cluster doit être installé correctement avec la totalité de ses fonctionnalités sur tous les nœuds cluster. Par exemple, vous devez pouvoir déplacer des groupes d'un nœud à l'autre autant de fois que cela est nécessaire, et ce sans aucun problème de disque partagé.
- Chaque système du cluster doit être en cours d'exécution.

Installation en local

Les clients Data Protector compatibles cluster doivent être installés localement, à partir du DVD-ROM, sur chaque nœud cluster. Les nœuds cluster (clients cluster Data Protector) sont importés vers la cellule spécifiée lors du processus d'installation. Vous devrez ensuite importer le nom du serveur virtuel.

Les droits administrateur de clusters sont requis pour effectuer l'installation. Hormis cette exigence, la configuration d'un client cluster est la même que celle d'un client Windows. Le composant Intégration de cluster, sélectionné par défaut lors de l'installation, doit être installé en plus des Data Protector composants clients, tels que les Agents de disque et les Agents de support.

Reportez-vous à la section "Installation de clients Windows" à la page 87 pour savoir comment installer en local un système client Windows Data Protector.

Le processus d'installation de Data Protector signale qu'un cluster a été détecté. Sélectionnez Installer le client en mode compatible cluster.

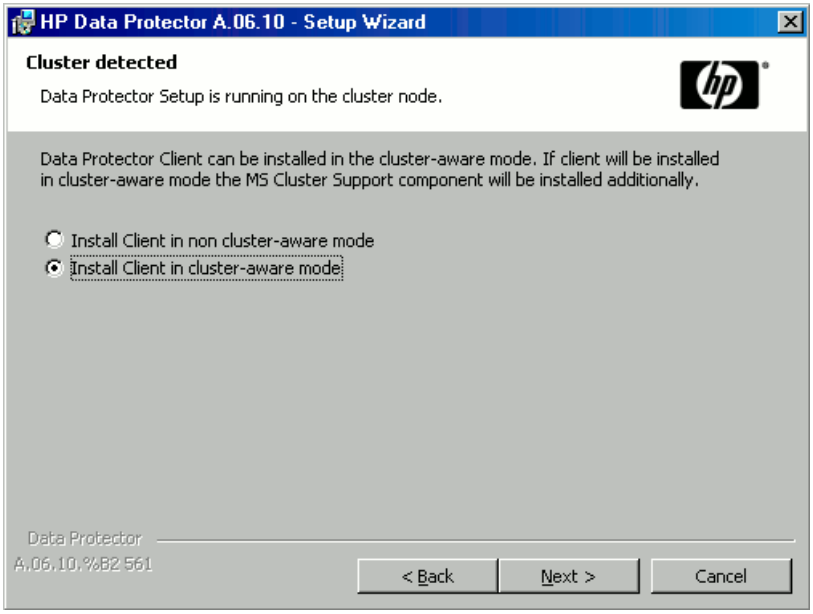

Figure 33 - Sélection du mode d'installation compatible cluster

Si vous installez l'intégration Data Protector Oracle, la procédure de configuration doit être effectuée sur tous les nœuds du cluster, ainsi que sur le serveur virtuel hébergeant le groupe de ressources Oracle.

REMARQUE :

Vous pouvez importer un client compatible cluster dans la cellule Data Protector qui est gérée par le Gestionnaire de cellule standard ou par le Gestionnaire de cellule compatible cluster.

Vérification de l'installation

Une fois l'installation terminée, vous pouvez vous assurer que le logiciel Data Protector a été installé correctement. Pour ce faire, procédez comme suit :

1. Vérifiez si le compte de service cluster est affecté au service `Inet` Data Protector sur chaque nœud du cluster. Vérifiez que le même utilisateur est également ajouté au groupe d'utilisateurs `Admin` de Data Protector. Le type de compte de connexion défini doit être Ce compte comme illustré dans la Figure 34 à la page 199.

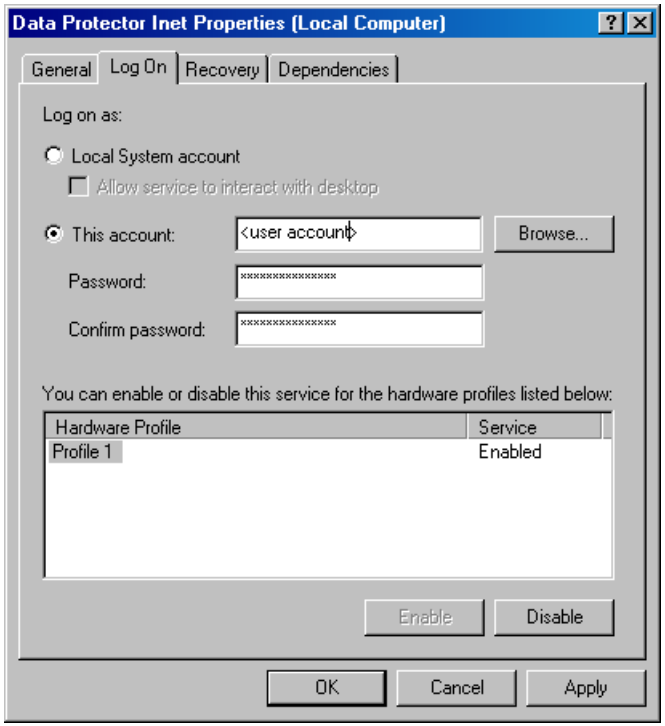

Figure 34 - Compte utilisateur Data Protector

2. Basculez vers le répertoire *`répertoire_Data_Protector`*`\bin`.
3. Exécutez la commande suivante :

   `omnirsh` *`hôte`* `INFO_CLUS`

   où *`hôte`* est le nom du système client cluster. Le nom du système client compatible cluster doit apparaître. Si `0 "NONE"` est affiché, Data Protector n'est pas installé en mode compatible cluster.

Veritas Volume Manager

Si Veritas Volume Manager est installé sur le cluster, des étapes supplémentaires sont requises après l'installation de Data Protector sur Microsoft Cluster Server. Pour connaître les opérations supplémentaires à effectuer, reportez-vous à la section "Installation de Data Protector sur Microsoft Cluster avec Veritas Volume Manager" à la page 441.

Etape suivante

Lorsque vous avez terminé l'installation, vous devez importer le nom d'hôte du serveur virtuel (application compatible cluster) dans la cellule Data Protector. Reportez-vous à la section "Importation d'un client compatible cluster dans une cellule" à la page 208.

Reportez-vous à l'index de l'aide en ligne (rubrique "configuration") pour plus d'informations sur la configuration de périphériques de sauvegarde ou de pools de supports ou sur toute autre tâche de configuration Data Protector.

Modification des comptes Inet et CRS

Si nécessaire, modifiez les comptes sous lesquels s'exécutent les services Inet et CRS de Data Protector.

Installation de clients Data Protector sur un cluster Veritas

Il est possible d'installer les clients Data Protector sur des nœuds cluster Veritas, à l'aide d'un Gestionnaire de cellule extérieur au cluster. Si vous utilisez cette configuration, la sauvegarde des disques locaux est prise en charge.

Notez que si vous souhaitez sauvegarder des disques partagés ou des applications compatibles cluster, il faut utiliser l'adresse IP du serveur virtuel pour les licences.

IMPORTANT :

Pour Data Protector, les sauvegardes compatibles cluster avec basculement ne sont pas prises en charge.

Installation d'un client

La procédure d'installation est identique à la procédure d'installation standard de Data Protector sur un système client Solaris. Pour connaître la procédure détaillée, reportez-vous à la section "Installation de clients Solaris" à la page 97.

Etape suivante

Une fois l'installation terminée :

- Si vous souhaitez sauvegarder le serveur virtuel, vous devez l'importer dans la cellule.
- Si vous souhaitez sauvegarder les nœuds physiques, vous devez également les importer dans la cellule.

Reportez-vous à la section "Importation d'un client compatible cluster dans une cellule" à la page 208. Consultez l'index de l'aide en ligne (rubrique "configuration")

pour plus d'informations sur la configuration de périphériques de sauvegarde ou de pools de supports ou sur toute autre tâche de configuration de Data Protector.

Installation de clients Data Protector sur un cluster Novell NetWare

Il est possible d'installer les clients Data Protector sur des nœuds cluster Novell NetWare Cluster Services, à l'aide d'un Gestionnaire de cellule extérieur au cluster. Si vous utilisez cette configuration, la sauvegarde des disques locaux, ainsi que la sauvegarde des pools de clusters partagés, sont prises en charge via le serveur virtuel. Pour connaître les systèmes d'exploitation pris en charge pour Microsoft Cluster Server, reportez-vous au document Références, notes de publication et annonces produits HP Data Protector.

Notez que si vous souhaitez sauvegarder des disques partagés ou des applications compatibles cluster, il faut utiliser l'adresse IP du serveur virtuel pour les licences.

IMPORTANT :

Les sauvegardes compatibles cluster avec basculement ne sont pas prises en charge. En cas de basculement, il faut redémarrer manuellement les sessions de sauvegarde ou de restauration.

Dans la mesure où les nœuds cluster contrôlent les périphériques, les périphériques de sauvegarde doivent être configurés sur les nœuds cluster et non sur le serveur virtuel.

Installation d'un client

Avant l'installation

Avant d'installer des clients Data Protector sur des nœuds cluster Novell NetWare Cluster Services, il est recommandé de modifier les scripts de déchargement pour *chaque* serveur virtuel présent dans le cluster, afin que l'adresse IP secondaire reste active pendant la migration du serveur virtuel vers un autre nœud. Vous pouvez modifier les scripts de déchargement à l'aide de l'utilitaire Console One de Novell ou de NetWare Remote Manager, conformément à la documentation Novell NetWare.

Exemple

Le script de déchargement par défaut pour chaque serveur virtuel est le suivant :

```
del secondary ipaddress 10.81.1.173
CLUSTER CVSBIND DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
NUDP DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
nss /pooldeactivate=FIRST /overridetype=question
```

Le script de déchargement modifié pour chaque serveur virtuel est le suivant :

```
nss /pooldeactivate=FIRST /overridetype=question
del secondary ipaddress 10.81.1.173
CLUSTER CVSBIND DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
NUDP DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
```

Le script de déchargement modifié commence par démonter et désactiver tous les pools de clusters partagés sur le serveur virtuel; alors seulement, il supprime l'adresse IP secondaire. Cela signifie que l'adresse IP secondaire reste active pendant la migration.

Pour activer le script de déchargement modifié, mettez le serveur virtuel hors ligne, puis de nouveau en ligne sur le nœud favori.

Modification du script smsrun.bas

Après avoir modifier le(s) script(s) de déchargement, vous devez modifier le script `smsrun.bas` afin d'inclure le chargement du module `TSA600.NLM` (ou `TSAFS.NLM` - selon le module que vous utilisez) avec le paramètre approprié désactivant la prise en charge du cluster. Pour plus d'informations, consultez la rubrique "Known Backup/Restore Issues for NetWare 6.x" (problèmes de sauvegarde/restauration connus pour NetWare 6.x) de la base de données Novell Support Knowledge.

Pour modifier le script `smsrun.bas`, procédez comme suit :

1. Modifiez la protection en écriture du script `SYS:NSN/user/smsrun.bas` en le faisant passer de `lecture seule` à `lecture/écriture`, puis ouvrez-le dans un éditeur standard de la console.
2. Modifiez la ligne `nlmArray = Array("SMDR", "TSA600", "TSAPROXY")` (ou `nlmArray = Array("SMDR", "TSAFS /NoCluster")`) dans la section `Sub Main()` en indiquant :
   - `nlmArray = Array("SMDR", "TSA600 /cluster=off", "TSAPROXY")` si `TSA600` est installé.
   - `nlmArray = Array("SMDR", "TSAFS /NoCluster")` si `TSAFS` est installé.

   Enregistrez les modifications.
3. Sur la console du serveur de fichiers, tapez `SMSSTOP`.
4. Sur la console du serveur de fichiers, tapez `SMSSTART`.

Les volumes partagés du cluster sont désormais visibles pour le module `TSA600.NLM`(`TSAFS.NLM`).

Installation

La procédure est identique à celle utilisée pour l'installation standard locale de Data Protector sur un client Novell NetWare. Pour connaître la procédure détaillée, reportez-vous à la section "Installation locale de clients Novell NetWare" à la page 126.

Etape suivante

Une fois l'installation terminée :

- Si vous souhaitez sauvegarder les nœuds physiques, vous devez également les importer dans la cellule.
- Pour sauvegarder le serveur virtuel (volumes partagés du cluster), vous devez l'importer dans la cellule.

Reportez-vous à la section "Importation d'un client compatible cluster dans une cellule" à la page 208. Consultez l'index de l'aide en ligne (rubrique "configuration") pour plus d'informations sur la configuration de périphériques de sauvegarde ou de pools de supports ou sur toute autre tâche de configuration de Data Protector.

Installation de Data Protector sur un cluster IBM HACMP

Data Protector prend en charge IBM HACMP (High Availability Cluster Multi-Processing) pour AIX.

IMPORTANT :

Installez le composant Agent de disque Data Protector sur tous les noeuds du cluster.

Installation de clients compatibles cluster

Pour installer des composants Data Protector sur un noeud du cluster, utilisez la procédure d'installation standard de Data Protector sur des systèmes UNIX. Pour plus d'informations, reportez-vous aux sections "Installation locale de clients UNIX" à la page 142 ou "Installation distante de clients Data Protector" à la page 78.

Etape suivante

Après l'installation, importez les nœuds du cluster et le serveur virtuel (adresse IP du package de l'environnement virtuel) dans la cellule Data Protector. Reportez-vous à la section "Importation d'un client compatible cluster dans une cellule" à la page 208.

Pour plus d'informations sur la configuration de périphériques de sauvegarde ou de pools de supports ou sur toute autre tâche de configuration de Data Protector, recherchez l'entrée suivante dans l'index de l'aide en ligne : configuration.

3 Gestion de l'installation

Description du chapitre

Ce chapitre décrit les procédures les plus utilisées pour modifier la configuration de votre environnement de sauvegarde. Les sections suivantes contiennent des informations relatives aux éléments suivants :

- Comment importer des clients dans une cellule à l'aide de l'interface graphique utilisateur. Reportez-vous à la section "Importation de clients dans une cellule" à la page 205.
- Comment importer un Serveur d'installation dans une cellule à l'aide de l'interface graphique utilisateur. Reportez-vous à la section "Importation d'un serveur d'installation dans une cellule" à la page 207.
- Comment importer des clusters/serveurs virtuels à l'aide de l'interface graphique utilisateur. Reportez-vous à la section "Importation d'un client compatible cluster dans une cellule" à la page 208.
- Comment exporter des clients à l'aide de l'interface graphique utilisateur. Reportez-vous à la section "Désinstallation du logiciel Data Protector" à la page 230.
- Comment garantir la sécurité à l'aide de l'interface graphique utilisateur. Reportez-vous à la section "Considérations sur la sécurité" à la page 214.
- Comment vérifier quels correctifs Data Protector sont installés. Reportez-vous à la section "Contrôle des correctifs Data Protector installés" à la page 228.
- Comment désinstaller le logiciel Data Protector. Reportez-vous à la section "Désinstallation du logiciel Data Protector" à la page 230.
- Comment ajouter ou supprimer des composants logiciels Data Protector. Reportez-vous à la section "Changement de composants logiciels Data Protector" à la page 242.

Importation de clients dans une cellule

Lorsque vous distribuez le logiciel Data Protector à des clients à l'aide du Serveur d'installation, les systèmes client sont automatiquement ajoutés à la cellule. Dès que l'installation distante est terminée, le client devient membre de la cellule.

Quand faut-il importer ?

Certains clients, comme Novell NetWare, HP OpenVMS et Windows XP Edition familiale, doivent être importés dans la cellule après l'installation. Importer signifie

ajouter manuellement un ordinateur à une cellule une fois le logiciel Data Protector installé. Une fois ajouté à une cellule Data Protector, le système devient un client Data Protector. Dès lors que le système est membre de la cellule, les informations relatives au nouveau client sont écrites dans la base IDB, située dans le Gestionnaire de cellule.

Un client ne peut être membre que d'une cellule. Si vous souhaitez déplacer un client vers une autre cellule, vous devez d'abord l'*exporter* à partir de sa cellule actuelle, puis l'*importer* dans la nouvelle cellule. Pour connaître la procédure à suivre pour exporter des clients, reportez-vous à la section "Exportation de clients d'une cellule" à la page 211.

REMARQUE :

Avant d'importer un serveur IAP, vous devez avoir ajouté au Gestionnaire de cellule un fichier de certificat pour l'accès au dispositif IAP. Pour connaître la procédure exacte, recherchez l'entrée suivante dans l'index de l'aide en ligne : "ajout, certificats IAP".

IMPORTANT :

Après avoir installé les clients Data Protector et les avoir importés dans une cellule, il est vivement recommandé de les protéger afin d'empêcher l'accès d'autorités de cellule non autorisées. Reportez-vous à la section "Sécurisation de clients" à la page 217.

Comment importer ?

Vous importez un système client à l'aide de l'interface graphique utilisateur en effectuant les opérations suivantes :

1. Dans le menu contextuel, cliquez sur Clients.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur Clients, puis cliquez sur Importer clients.
3. Saisissez le nom du client ou parcourez le réseau pour sélectionner le client (seulement si vous utilisez une interface graphique Windows) à importer. Reportez-vous à la Figure 35 à la page 207.

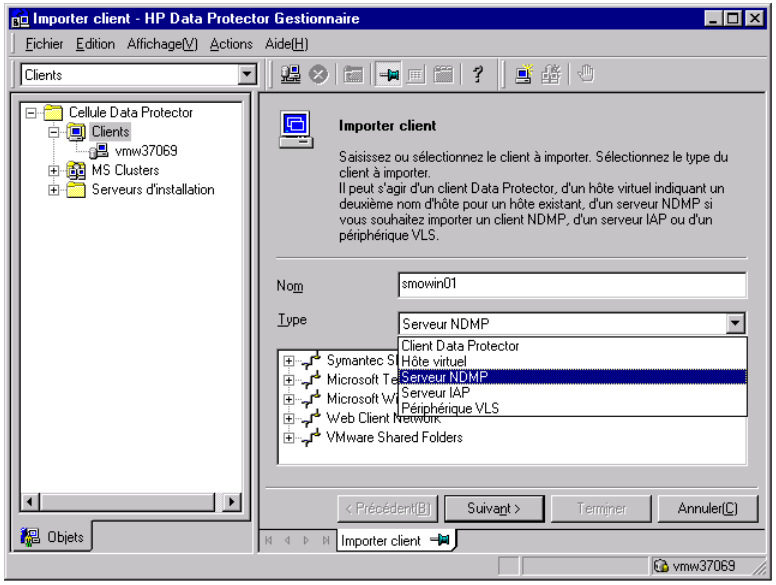

Figure 35 - Importation d'un client vers la cellule

Si vous importez un client configuré avec plusieurs cartes réseau LAN, sélectionnez l'option Hôte virtuel. Avec cette option, vous devez importer tous les noms du même système.

Si vous importez un client NDMP, sélectionnez l'option Serveur NDMP puis cliquez sur Suivant. Spécifiez les informations relatives au serveur NDMP.

Si vous importez un client HP OpenVMS, saisissez son nom TCP/IP dans la zone de texte `Nom`.

Si vous importez un serveur IAP, sélectionnez l'option Serveur IAP puis cliquez sur Suivant. Spécifiez les informations sur le serveur IAP.

Si vous importez un périphérique VLS, sélectionnez l'option Périphérique VLS puis cliquez sur Suivant. Spécifiez les informations relatives au périphérique VLS.

Cliquez sur Terminer pour importer le client.

Le nom du client importé s'affiche dans la zone de résultats.

Importation d'un serveur d'installation dans une cellule

Quand effectuer l'ajout ?

Vous devez installer un Serveur d'installation sur une cellule dans les cas suivants :

- S'il est installé en tant que Serveur d'installation UNIX indépendant, c'est-à-dire s'il n'est pas installé sur un Gestionnaire de cellule.
  Dans ce cas, il ne sera pas possible d'installer (charger) des clients dans une cellule avant que le Serveur d'installation n'ait été ajouté à cette cellule.
- S'il est installé sur un Gestionnaire de cellule, mais que vous voulez aussi l'utiliser pour effectuer des installations à distance dans une autre cellule. Il doit alors être ajouté dans l'autre cellule (à l'aide de l'interface graphique utilisateur connectée au Gestionnaire de cellule de l'autre cellule).

Contrairement à un client, un Serveur d'installation peut appartenir à plusieurs cellules. Par conséquent, il n'est pas nécessaire de le supprimer d'une cellule (exporter) pour pouvoir l'ajouter à une autre cellule (importer).

Comment effectuer l'ajout ?

Le processus d'importation d'un Serveur d'installation ressemble à celui d'un client. Pour exécuter cette tâche à l'aide de l'interface graphique utilisateur Data Protector (connectée au Gestionnaire de cellule de la cellule à laquelle le Serveur d'installation doit être ajouté), procédez comme suit :

1. Dans la liste de contextes, cliquez sur Clients.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur Serveurs d'installation, puis cliquez sur Importer Serveur d'installation pour lancer l'assistant. Reportez-vous à la Figure 35 à la page 207.
3. Saisissez ou sélectionnez le nom du système que vous souhaitez importer. Cliquez sur Terminer pour importer le Serveur d'installation.

Importation d'un client compatible cluster dans une cellule

Après avoir installé le logiciel Data Protector en local sur un client compatible cluster, importez le serveur virtuel représentant le client compatible cluster dans la cellule Data Protector.

Configuration système requise

- Data Protector doit être installé sur tous les nœuds cluster.
- Tous les packages cluster doivent s'exécuter au sein du cluster.

Microsoft Cluster Server

Pour importer un client Microsoft Cluster Server dans la cellule Data Protector, procédez comme suit :

1. Dans Data Protector, affichez le contexte Clients.

2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur MS Clusters, puis cliquez sur Importer cluster.
3. Saisissez le nom du serveur virtuel qui représente le client cluster à importer ou parcourez le réseau pour sélectionner le serveur virtuel. Reportez-vous à la Figure 36 à la page 209 .

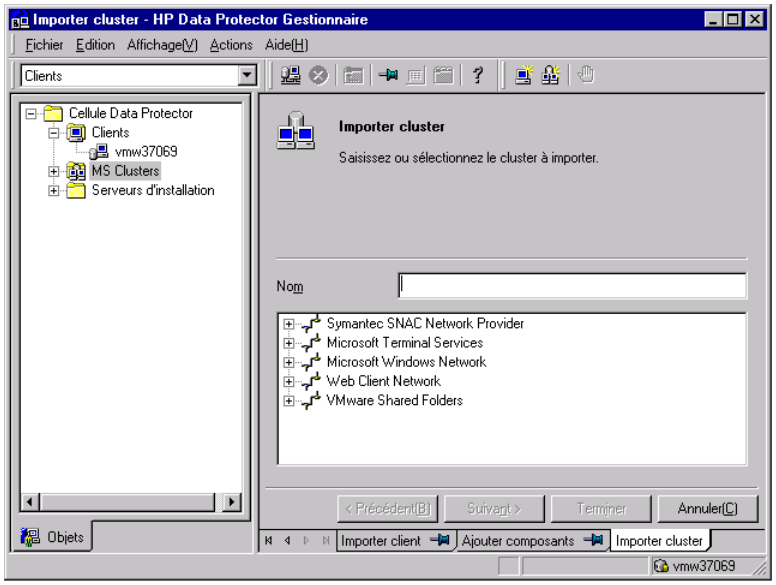

Figure 36 - Importation d'un client Microsoft Cluster Server dans une cellule

4. Cliquez sur Terminer pour importer le client cluster.

CONSEIL :

Pour importer un nœud cluster ou un serveur virtuel spécifique, cliquez avec le bouton droit sur son cluster dans la fenêtre de navigation et cliquez sur Importer nœud cluster ou Importer serveur virtuel cluster.

Autres clusters

Configuration requise pour les clusters Tru64

Avant d'importer les noms d'hôtes de clusters, assurez-vous que :

- Data Protector est installé sur le disque partagé dans le cluster

- Tous les nœuds cluster Tru64 s'exécutent au sein du cluster
- Data Protector Le processus `inetd` s'exécute sur chaque nœud

Procédure

Pour importer un client MC/ServiceGuard, Veritas, Tru64 Cluster, IBM HACMP Cluster ou Novell NetWare Cluster Services dans la cellule Data Protector, procédez comme suit :

1. Dans le Gestionnaire Data Protector, basculez vers le contexte Clients.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur Clients, puis cliquez sur Importer clients.
3. Saisissez le nom d'hôte du serveur virtuel tel qu'il est spécifié dans le package de clusters d'applications ou parcourez le réseau pour sélectionner le serveur virtuel (seulement si vous utilisez une interface graphique Windows) à importer.

   Sélectionnez l'option Hôte virtuel pour indiquer qu'il s'agit d'un serveur virtuel cluster. Reportez-vous à la Figure 37 à la page 211.
4. Cliquez sur Terminer pour importer le serveur virtuel.

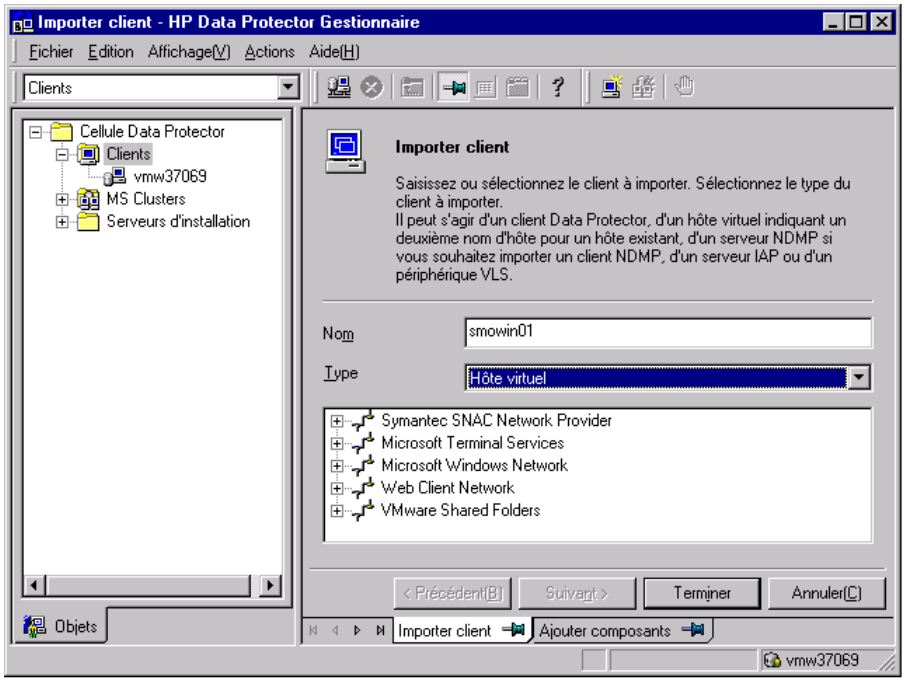

Figure 37 - Importation d'un client MC/ServiceGuard, Veritas ou Novell NetWare Cluster Services dans une cellule

CONSEIL :

Pour configurer des sauvegardes de données sur les disques locaux des nœuds cluster, vous devez importer les nœuds cluster représentant les clientsData Protector. Pour connaître la procédure, reportez-vous à la section "Importation de clients dans une cellule" à la page 205

Exportation de clients d'une cellule

Exportationd'un client d'une cellule Data Protector revient à supprimer ses références de la base de données IDB sur le Gestionnaire de cellule sans pour autant désinstaller le logiciel du client. Cette procédure peut être réalisée à l'aide de l'interface graphique utilisateur Data Protector.

Vous pouvez avoir besoin de la fonction d'exportation dans les cas suivants :

- Vous souhaitez déplacer un client vers une autre cellule.
- Vous souhaitez supprimer un client des configurations de cellule Data Protector qui ne font plus partie du réseau.

- Vous souhaitez régler des problèmes dus à des licences insuffisantes. Lorsque vous exportez un client d'une cellule, la licence devient disponible pour un autre système.

Configuration système requise

Avant d'exporter un client, vérifiez les éléments suivants :

- Toutes les occurrences du client sont supprimées des spécifications de sauvegarde. Dans le cas contraire, Data Protector essaiera de sauvegarder des clients inconnus et cette partie de la spécification de sauvegarde échouera. Recherchez l'entrée suivante dans l'index de l'aide en ligne : "modification, spécification de sauvegarde" pour de plus amples informations sur la modification des spécifications de sauvegarde.
- Aucun périphérique de sauvegarde n'est connecté au client ni configuré sur ce dernier. Une fois le système exporté, Data Protector ne peut plus utiliser ses périphériques de sauvegarde dans la cellule d'origine.

Comment effectuer l'exportation ?

Afin d'exporter un client à l'aide de l'interface graphique utilisateur de Data Protector, procédez comme suit ::

1. Dans le menu contextuel, cliquez sur Clients.
2. Dans la fenêtre de navigation, cliquez sur Clients, cliquez avec le bouton droit de la souris sur le système client à exporter, puis cliquez sur Supprimer. Reportez-vous à la Figure 38 à la page 213.

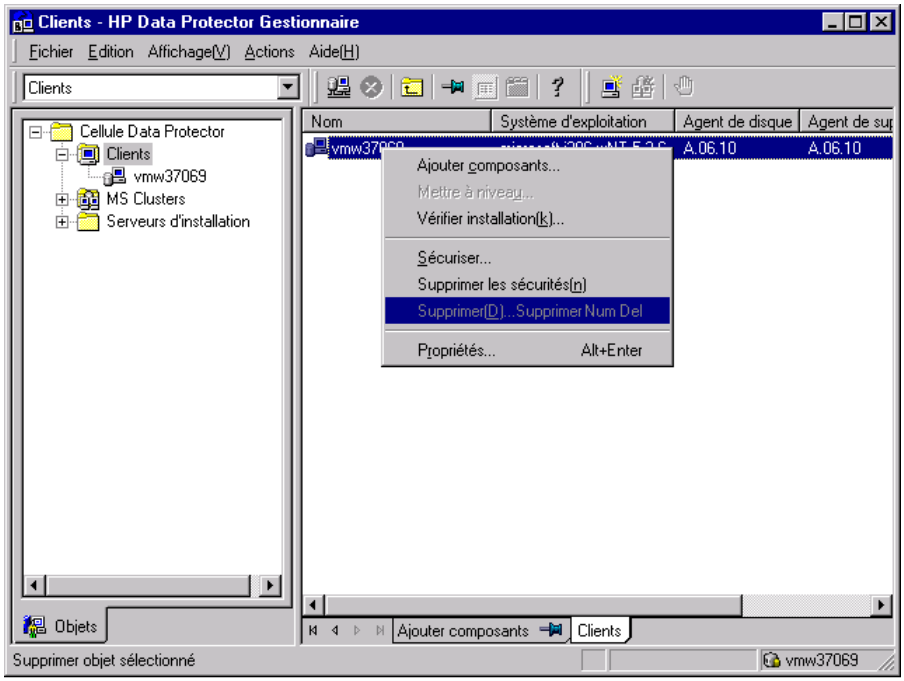

Figure 38 - Exportation d'un système client

3. Un message vous demande si vous souhaitez également désinstaller le logiciel Data Protector. Cliquez sur Non pour exporter le client, puis sur Terminer.

Le client est supprimé de la liste dans la zone de résultats.

REMARQUE :

Vous ne pouvez pas exporter ou supprimer un client Data Protector si le Gestionnaire de cellule est installé sur le même système que le client à exporter. Toutefois, vous pouvez exporter les clients à partir des systèmes où seuls le client et le Serveur d'installation sont installés. Dans ce cas, le Serveur d'installation est supprimé de la cellule.

Clients Microsoft Cluster Server

Pour exporter un client Microsoft Cluster Server à partir de la cellule Data Protector, procédez comme suit :

1. Dans le menu contextuel, cliquez sur Clients.
2. Dans la fenêtre de navigation, développez MS Clusters, cliquez avec le bouton droit de la souris sur le client cluster que vous souhaitez exporter, puis cliquez sur Supprimer.

3. Un message vous demande si vous souhaitez également désinstaller le logiciel Data Protector. Cliquez sur Non pour uniquement exporter le client cluster.

Le client cluster est supprimé de la liste dans la zone de résultats.

CONSEIL :

Pour exporter un nœud cluster ou un serveur virtuel spécifique, cliquez avec le bouton droit de la souris sur le nœud cluster ou le serveur virtuel dans la fenêtre de navigation et cliquez sur Supprimer.

Considérations sur la sécurité

Cette section décrit les éléments de sécurité de Data Protector. Elle décrit les paramètres avancés pouvant être utilisés en vue d'améliorer la sécurité de Data Protector en tenant compte des connaissances préalables et des considérations requises.

L'amélioration de la sécurité dans un environnement complet étant assez complexe, de nombreuses fonctions de sécurité ne peuvent pas être activées par défaut.

Les considérations décrites dans ce chapitre s'appliquent non seulement lorsque des paramètres de sécurité sont modifiés, mais également lors de la configuration de nouveaux utilisateurs, de l'ajout de clients et de la configuration d'Agents d'application (ou toute autre modification à laquelle ces considérations s'appliquent). Toute modification apportée aux paramètres de sécurité peut avoir des répercussions dans la cellule toute entière et doit par conséquent être soigneusement planifiée.

Couches de sécurité

La sécurité doit être planifiée, testée et mise en oeuvre dans des couches de sécurité critique différentes afin d'assurer le fonctionnement sécurisé de Data Protector. Ces différentes couches correspondent aux clients Data Protector, aux Gestionnaire de cellule et aux utilisateurs. Cette section détaille la procédure de configuration de la sécurité sur chacune de ces couches.

Sécurité client

Les agents Data Protector installés sur les clients appartenant à la cellule offrent de nombreuses fonctionnalités puissantes, telles que l'accès à l'ensemble des données sur le système. Il est primordial que ces fonctionnalités ne soient disponibles que pour les processus s'exécutant sur les autorités de cellule (Gestionnaire de cellule et Serveur d'installation), et que toutes les autres requêtes soient refusées.

Avant de sécuriser les clients, il faut établir une liste d'hôtes fiables. Cette liste doit comprendre :

- Gestionnaire de cellule

- Serveurs d'installation concernés
- Pour certains clients, une liste de clients qui auront accès au robot à distance

IMPORTANT :

La liste doit contenir tous les noms d'hôte (ou adresses IP) possibles d'où les connexions peuvent provenir. Il est possible que plusieurs noms d'hôte soient nécessaires si l'un des clients mentionnés ci-dessus est multirésident (possède plusieurs cartes réseau et/ou plusieurs adresses IP) ou s'il s'agit d'un cluster.

Si la configuration DNS dans la cellule n'est pas uniforme, des considérations supplémentaires peuvent s'appliquer. Pour plus d'informations, reportez-vous à la section "Sécurisation de clients" à la page 217.

Même s'il peut ne pas être toujours indispensable de sécuriser chacun des clients contenus dans la cellule, il est important que les ordinateurs auxquels se fient d'autres clients soient eux-mêmes sécurisés :

- Gestionnaire de cellule / MoM
- Serveurs d'installation
- Clients Agent de support (MA)

REMARQUE :

Les clients de l'interface utilisateur ne doivent pas être nécessairement ajoutés à la liste des clients fiables. En fonction des droits utilisateur, vous pouvez utiliser l'interface graphique utilisateur pour accéder à l'ensemble des fonctionnalités de Data Protector ou pour accéder seulement à des contextes spécifiques.

Utilisateurs de Data Protector

Pour procéder à la configuration des utilisateurs de Data Protector, vous devez tenir compte des aspects importants énumérés ci-dessous :

- Certains droits utilisateur accordent à l'utilisateur un grand pouvoir. Par exemple, les droits utilisateur `Configuration utilisateur` et `Configuration des clients` permettent à l'utilisateur de modifier les paramètres de sécurité. `Le droit utilisateur Restaurer vers autres clients` est également très puissant, en particulier (mais pas exclusivement) s'il est associé à l'un des droits utilisateur suivants : `Sauvegarder en tant que root` ou `Restaurer en tant que root`.
- Même les droits utilisateur se caractérisant par un pouvoir moins important recèlent certains risques. Il est possible de configurer Data Protector en vue de restreindre certains droits utilisateur dans le but de réduire ces risques. Ces paramétrages sont décrits ultérieurement dans ce chapitre. Reportez-vous

également à la section “Droit utilisateur de démarrage de spécification de sauvegarde” à la page 225.

- Data Protector est fourni seulement avec quelques groupes d’utilisateurs prédéfinis. Il est conseillé de définir des groupes spécifiques pour chaque type d’utilisateur dans l’environnement de Data Protector afin de limiter l’ensemble des droits qui leur sont octroyés.
- La configuration des utilisateurs dépend de la validation des utilisateurs (reportez-vous à la section “Vérification stricte du nom d’hôte” à la page 223). La validation renforcée peut s’avérer inutile en l’absence d’une configuration utilisateur détaillée et vice versa : la configuration utilisateur, aussi détaillée soit-elle, pourra être contournée si la validation renforcée n’est pas présente.
- Il est important que la liste des utilisateurs de Data Protector ne comporte pas de spécifications utilisateur "faibles".

REMARQUE :

La partie *hôte* d’une spécification utilisateur constitue la partie éprouvée (en particulier avec la validation renforcée), alors que les parties *utilisateur* et *groupe* ne peuvent pas être vérifiées de manière fiable. Tout utilisateur doté de droits utilisateur puissants doit être configuré en particulier pour le client qu’il utilisera pour l’administration de Data Protector. S’il utilise plusieurs clients, une entrée doit être ajoutée pour chaque client supplémentaire. Evitez de spécifier l’utilisateur ainsi : *utilisateur*, *groupe*, *<Tout>*. L’accès à l’un de ces systèmes doit être interdit aux utilisateurs non fiables.

Dans l’index de l’aide en ligne, recherchez : “configuration, utilisateurs” pour plus d’informations sur la configuration des utilisateurs.

Sécurité du Gestionnaire de cellule

Il est essentiel de garantir la sécurité du Gestionnaire de cellule car ce dernier a accès à l’ensemble des clients et des données de la cellule.

La sécurité du Gestionnaire de cellule peut être renforcée via la fonctionnalité de vérification stricte de nom d’hôte. Il est toutefois important de sécuriser le Gestionnaire de cellule en tant que client et de configurer avec attention les utilisateurs de Data Protector. Reportez-vous aux sections “Vérification stricte du nom d’hôte” à la page 223 et “Sécurisation de clients” à la page 217.

Autres aspects de la sécurité

Vous devez également prendre en compte d’autres aspects liés à la sécurité :

- Les utilisateurs ne doivent pas avoir accès aux clients fiables (Gestionnaire de cellule, Serveur d’installation, MA et clients côté robotique). Même le fait

d'autoriser une session `anonyme` ou un accès `ftp` peut présenter un risque sérieux pour l'ensemble de la sécurité.

- Les bibliothèques de supports et de bandes (et les clients qui y sont connectés) doivent être protégées physiquement contre l'accès de toute personne non autorisée ou non fiable.
- Pendant les opérations de sauvegarde, , de restauration, de copie d'objets ou de supports, ou encore de consolidation d'objets, les données sont transférées via le réseau. Si la segmentation du réseau ne permet pas d'assurer une indépendance suffisante par rapport au réseau non sécurisé, il convient d'utiliser des périphériques connectés en local ou une bibliothèque de codage personnalisée. Notez qu'il est préférable d'effectuer une sauvegarde complète après la modification de la bibliothèque de codage.

Pour obtenir des informations sur les autres aspects liés à la sécurité, reportez-vous également au *Guide conceptuel HP Data Protector*.

Sécurisation de clients

Après avoir installé les clients Data Protector et les avoir importés dans une cellule, il est vivement recommandé de les protéger afin d'empêcher l'accès de clients non autorisés.

Data Protector vous permet de spécifier les autorités de cellule (Gestionnaire de cellule, MoM et Serveur d'installation) dont un client acceptera les requêtes sur le port Data Protector `5555`. Ainsi, les autres ordinateurs ne seront pas en mesure d'accéder à ce client. Reportez-vous également à la section "Sécurité client" à la page 214.

REMARQUE :

Les clients qui auront accès au robot de bibliothèque doivent être ajoutés à la liste des autorités de cellule destinée aux clients du robot de bibliothèque.

Pour les activités telles que la restauration, la sauvegarde, le lancement pré-exécution ou post-exécution, l'importation et l'exportation de clients, le client vérifie si l'ordinateur qui déclenche l'une de ces tâches via le port Data Protector (port par défaut `5555`), est autorisé à le faire. Ce mécanisme de sécurité donne l'instruction au client de n'accepter ce genre d'action que de la part des autorités de cellule spécifiées.

Situations exceptionnelles

Avant de commencer à restreindre l'accès aux clients, prenez en compte les cas suivants, qui peuvent poser des problèmes :

- Une autorité de cellule possède plusieurs cartes réseau et plusieurs adresses IP/noms de client.
- Le Gestionnaire de cellule est compatible cluster.
- Le robot d'une bibliothèque de bandes est configuré sur un système séparé (ou dédié).

Data Protector vous permet de définir toute une liste de systèmes explicitement autorisés à se connecter au client en tant qu'autorité de cellule. Afin d'éviter tout problème, préparez à l'avance la liste de tous les noms de client valides possibles pour d'autres autorités de cellule.

La liste doit contenir :

- Tous les noms de client supplémentaires (pour toutes les cartes réseau) de l'autorité de cellule.
- Les noms de client de tous les nœuds cluster sur lesquels le Gestionnaire de cellule risque de basculer, ainsi qu'un nom d'hôte de serveur virtuel cluster.
- Le nom du système cible vers lequel l'autorité de cellule sera déplacée en cas de panne matérielle totale de l'autorité de cellule. Ce système cible doit être défini dans la stratégie de récupération après sinistre.
- Pour les clients autorisés à accéder à un client commandant le robot d'une bibliothèque, tous les clients utilisant les lecteurs de cette dernière.

Le concept d'autorisation et de refus d'accès peut s'appliquer à l'ensemble des systèmes sur lesquels Data Protector est installé. Vous pouvez par exemple autoriser ou refuser l'accès d'un Gestionnaire de cellule à un client, d'un Gestionnaire de cellule à un Gestionnaire de cellule, d'un Serveur d'installation à un client ou d'un client à un client.

REMARQUE :

Si le Serveur d'installation résidant sur un système autre que le Gestionnaire de cellule n'est pas ajouté à la liste des clients autorisés, il n'a pas accès à un client sécurisé. Dans ce cas, les opérations dépendant du Serveur d'installation (vérification de l'installation, ajout de composants et suppression de clients, par exemple) échoueront. Si vous souhaitez que ces opérations soient disponibles sur le client sécurisé, ajoutez le Serveur d'installation à la liste des clients autorisés.

Procédure de sécurisation d'un client

Pour autoriser la vérification d'une autorité de cellule du côté client (sécuriser un client), effectuez les opérations suivantes dans l'interface graphique utilisateur de Data Protector :

1. Dans le menu contextuel, cliquez sur Clients.
2. Dans la fenêtre de navigation, développez Clients, cliquez avec le bouton droit de la souris sur le ou les clients que vous voulez sécuriser, puis cliquez sur Sécuriser. Reportez-vous à la Figure 39 à la page 219.

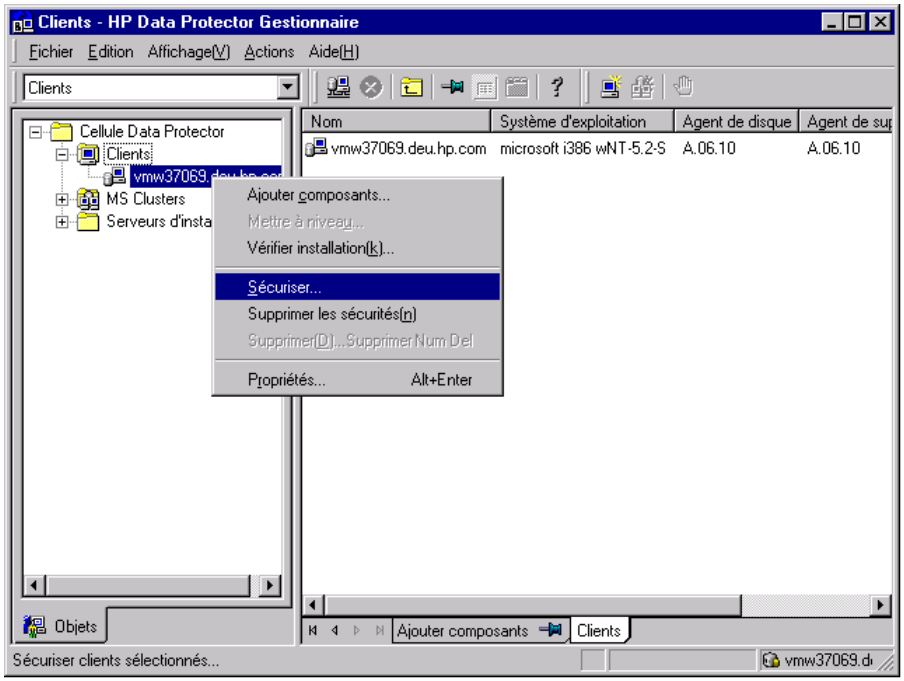

Figure 39 - Sécurisation d'un client

3. Saisissez les noms des systèmes qui auront accès aux clients sélectionnés ou recherchez ces systèmes en utilisant les onglets Réseau ou Recherche. Cliquez sur Ajouter pour ajouter chaque système à la liste. Reportez-vous à la Figure 40 à la page 220.

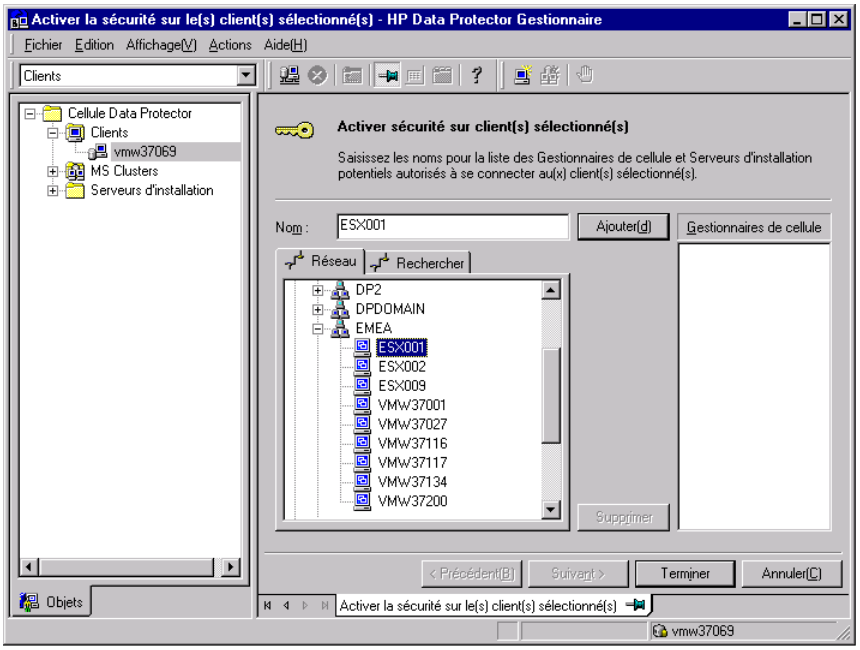

Figure 40 - Activation de la sécurité sur les clients sélectionnés

Le Gestionnaire de cellule reçoit automatiquement une autorisation d'accès et il ajouté à la liste des clients fiables. Vous ne pouvez pas exclure le Gestionnaire de cellule de la liste.

4. Cliquez sur Terminer pour ajouter les systèmes sélectionnés au fichier `allow_hosts`.

Que se passe-t-il ?

Les clients vérifient la source de chaque requête provenant d'autres clients et n'autorisent que les requêtes reçues des clients sélectionnés dans la fenêtre Activer la sécurité sur le(s) client(s) sélectionné(s). Ces clients sont répertoriés dans le fichier `allow_hosts`. Si une demande est refusée, l'événement est consigné dans le fichier `inet.log` dans le répertoire suivant :

- Sous Windows Vista, Windows Server 2008 : *`donnes_programme_Data_Protector`*`\log`
- Sur les autres systèmes Windows : *`répertoire_Data_Protector`*`\log`
- Sous HP-UX, Solaris et Linux : `/var/opt/omni/log`
- Sous les autres systèmes UNIX : `/usr/omni/log`

Pour sécuriser tous les clients de la cellule, procédez comme suit dans l'interface graphique de Data Protector :

1. Dans le menu contextuel, cliquez sur Clients.

2. Saisissez les noms des systèmes qui auront accès à tous les clients dans la cellule ou recherchez ces systèmes en utilisant les onglets `Réseau` (seulement si vous utilisez une interface graphique Windows) ou Recherche. Cliquez sur Ajouter pour ajouter chaque système à la liste. Reportez-vous à la Figure 41 à la page 221.

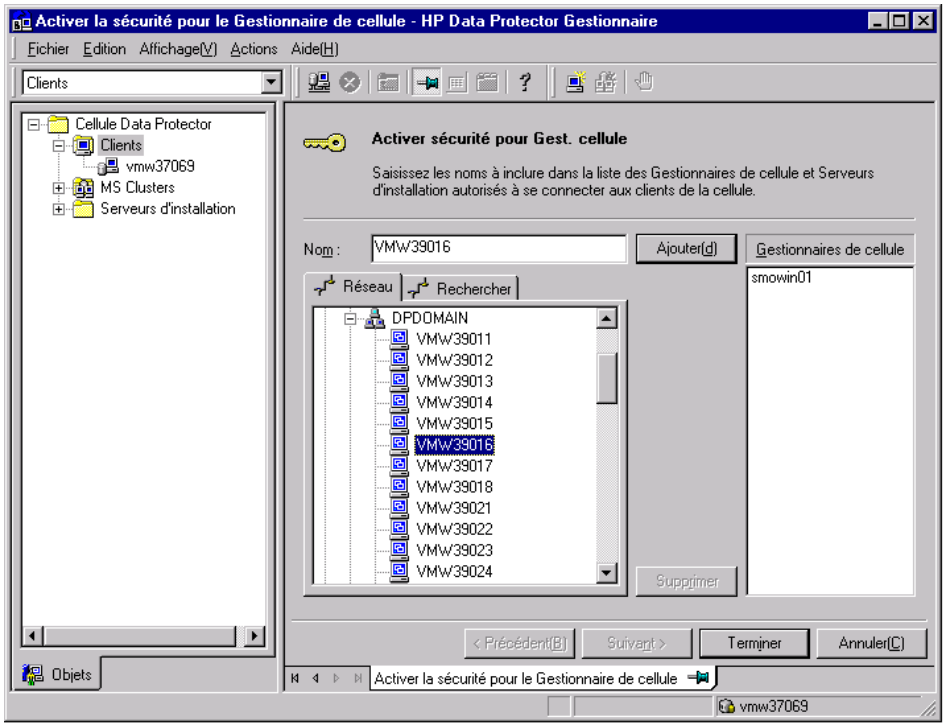

Figure 41 - Activation de la sécurité pour tous les clients de la cellule

3. Cliquez sur Terminer pour ajouter les systèmes sélectionnés au fichier `allow_hosts`.

Que se passe-t-il ?

Les clients vérifient la source de chaque requête provenant d'autres clients et n'autorisent que les requêtes reçues des clients sélectionnés dans la fenêtre Activer la sécurité sur le Gestionnaire de cellule. Ces clients sont répertoriés dans le fichier `allow_hosts`. Si une demande est refusée, l'événement est consigné dans le fichier `inet.log` dans le répertoire suivant :

- Sous Windows Vista, Windows Server 2008 : *`donnes_programme_Data_Protector`*`\log`
- Sur les autres systèmes Windows : *`répertoire_Data_Protector`*`\log`
- Sous HP-UX, Solaris et Linux : `/var/opt/omni/log`

- Sous les autres systèmes UNIX : `/usr/omni/log`

Lorsque vous sécurisez une cellule entière, tous les clients qui résident dans cette cellule sont sécurisés. Lorsque vous ajoutez un nouveau client à la cellule, sécurisez-le également.

Suppression de la sécurité

Pour supprimer la sécurité du ou des systèmes sélectionnés, procédez comme suit via l'interface graphique de Data Protector :

1. Dans le menu contextuel, cliquez sur Clients.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur le ou les clients pour lesquels vous voulez supprimer la sécurité, puis cliquez sur Supprimer les sécurités.
3. Cliquez sur Oui pour confirmer que vous autorisez l'accès aux clients sélectionnés.

Si vous voulez supprimer la sécurité de tous les clients présents dans la cellule, procédez comme suit:

1. Dans le menu contextuel, cliquez sur Clients.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur Clients, puis cliquez sur Suppression des sécurités de cellule.
3. Cliquez sur Oui pour confirmer que vous autorisez l'accès à tous les clients présents dans votre cellule.

Les fichiers allow_hosts et deny_hosts

Lorsque vous sécurisez un client, les noms de client des systèmes autorisés à accéder à un client figurent dans le fichier `allow_hosts`. Vous pouvez aussi refuser explicitement l'accès à un client par certains ordinateurs en ajoutant leurs noms au fichier `deny_hosts`. Ces fichiers se trouvent dans le répertoire suivant :

- Sous Windows Vista, Windows Server 2008 : *`donnes_programme_Data_Protector`*`\Config\client`
- Sur les autres systèmes Windows : *`répertoire_Data_Protector`*`\Config\client`
- Sur les systèmes HP-UX, Solaris et Linux : `/etc/opt/omni/client`
- Sous les autres systèmes UNIX : `/usr/omni/config/client`

Indiquez un nom de client par ligne distincte.

REMARQUE :

Si vous verrouillez un client par mégarde, vous pouvez modifier (ou supprimer) manuellement le fichier `allow_hosts` de ce client.

Sur les systèmes Windows, les fichiers sont au format codé sur deux octets (Unicode) ; sur les systèmes HP-UX, Solaris et Linux, en revanche, ils sont au format codé sur un octet ou sur plusieurs octets (Shift-JIS, par exemple).

Enregistrement excessif dans le fichier inet.log

Si les clients ne sont pas sécurisés et que le Gestionnaire de cellule est configuré dans l'environnement MC/ServiceGuard ou qu'il comporte plusieurs noms ou numéros IP, le fichier `inet.log` peut contenir plusieurs entrées dont le type est le suivant :

`Une requête 0 a été émise par l'hôte` *`nom.entreprise.com`* `qui n'est pas un Gestionnaire de cellule de ce client`

Ces entrées résultent du fait que le client, qui n'est pas sécurisé, ne reconnaît que le nom d'hôte principal du Gestionnaire de cellule. Les demandes provenant de tous les autres clients sont autorisées et enregistrées dans le fichier `inet.log`.

Lorsqu'un client est sécurisé, les demandes provenant des clients répertoriés dans le fichier `allow_hosts` sont acceptées et ne sont donc pas enregistrées. Les demandes provenant d'autres clients sont refusées.

La sécurisation des clients peut être une solution permettant d'éviter les entrées inutiles dans les fichiers `inet.log`. Néanmoins, il est préférable de répertorier tous les noms de client possibles pour le Gestionnaire de cellule dans le fichier `allow_hosts` de chaque client. L'accès au client est ainsi garanti, même en cas de basculement.

Si cette solution est impossible dans votre environnement pour une raison quelconque, vous pouvez sécuriser les clients et spécifier `*` comme plage d'adresses IP pour les systèmes auxquels vous souhaitez autoriser l'accès. Cela signifie que vos clients accepteront les requêtes provenant de tous les systèmes (n'importe quelle adresse IP) et ne seront pratiquement pas sécurisés, mais que vous pourrez néanmoins résoudre le problème des connexions excessives.

Vérification stricte du nom d'hôte

Par défaut, le Gestionnaire de cellule utilise une méthode relativement simple pour valider les utilisateurs. Il utilise le nom d'hôte tel qu'il est connu du client lorsqu'une interface utilisateur ou un agentd'application est démarré. Cette méthode est plus facile à configurer, offre un niveau de sécurité convenable dans les environnements où la sécurité est considérée comme "conseillée" (c'est-à-dire où des attaques malveillantes ne se produisent normalement pas).

D'autre part, le paramètre de vérification stricte du nom d'hôte offre une validation renforcée des utilisateurs. Cette validation utilise le nom d'hôte tel qu'il est résolu par le Gestionnaire de cellule à l'aide de la recherche DNS inverse à partir de l'adresse IP obtenue par la connexion. Cela impose les limites et considérations suivantes :

Limites

- La validation des utilisateurs sur la base de l'adresse IP ne peut être qu'équivalente au niveau de protection contre l'usurpation d'adresse sur le réseau. Le concepteur du système de sécurité doit déterminer si le réseau en place offre un degré suffisant de protection contre l'usurpation d'adresse pour ces exigences de sécurité en particulier. La protection contre l'usurpation d'adresse peut être ajoutée en segmentant le réseau à l'aide de pare-feux, de routeurs, de VPN, etc.
- La séparation des utilisateurs au sein d'un client donné n'a pas un effet aussi important que la séparation des clients. Dans un environnement hautement sécurisé, il ne faut pas mélanger les utilisateurs courants et les utilisateurs dotés de droits importants au sein du même client.
- Les hôtes utilisés dans les spécifications utilisateur ne peuvent pas être configurés pour utiliser DHCP, sauf s'ils sont liés à une adresse IP fixe et configurés dans le DNS.

Soyez conscients des limites qui s'appliquent afin d'évaluer correctement le degré de sécurité pouvant être atteint avec la vérification stricte du nom d'hôte.

Résolution du nom d'hôte

Le nom d'hôte utilisé par Data Protector pour la validation peut varier entre la validation de l'utilisateur par défaut et la vérification stricte du nom d'hôte dans les situations suivantes :

- La recherche DNS inverse renvoie un nom d'hôte différent. Ce renvoi peut être volontaire ou peut révéler une mauvaise configuration du client ou de la table de DNS inverse.
- Le client est multirésident (possède plusieurs cartes réseau et/ou plusieurs adresses IP). L'application de cette considération à un client multirésident particulier dépend du rôle joué par ce dernier sur le réseau et de la manière dont il est configuré dans le DNS.
- Le client est un cluster.

En raison de la nature des vérifications pouvant être effectuées avec ce paramétrage, une reconfiguration des utilisateurs de Data Protector peut s'avérer nécessaire. Les spécifications existantes des utilisateurs de Data Protector doivent être vérifiées afin de savoir si elles peuvent être attribuées à l'une des raisons mentionnées ci-dessus. Selon le cas, les spécifications existantes devront éventuellement être modifiées ou de nouvelles spécifications ajoutées pour toutes les adresses IP possibles d'où peuvent provenir des connexions.

Notez que les utilisateurs doivent également être reconfigurés lorsque vous revenez à la validation de l'utilisateur par défaut, si vous avez dû modifier les spécifications de l'utilisateur lorsque vous avez activé la vérification stricte du nom d'hôte. Il est par conséquent recommandé de choisir une validation d'utilisateur et de la conserver.

Pour que la recherche DNS inverse soit fiable, le serveur DNS doit être sécurisé. Vous devez empêcher l'accès physique et la connexion à l'ensemble du personnel non autorisé.

En configurant des utilisateurs avec des adresses IP au lieu de noms d'hôte, vous pouvez éviter certains problèmes de validation liés au DNS ; toutefois, une telle configuration est plus difficile à gérer.

Conditions requises

La validation renforcée ne donne pas automatiquement accès à certaines connexions internes. Par conséquent, lorsque cette validation est utilisée, un nouvel utilisateur doit être ajouté pour chacun des éléments suivants :

- Un Agent d'application (OB2BAR) sur des clients Windows. Pour les clients Windows, il faut ajouter l'utilisateur `SYSTEM`, `NT AUTHORITY`, *`client`* pour chaque client disposant d'un Agent d'application installé. Remarquez que si `Inet` sur un client donné est configuré de manière à utiliser un compte spécifique, ce compte doit déjà avoir été paramétré. Pour plus d'informations, recherchez l'entrée suivante dans l'index de l'aide en ligne : "Vérification stricte du nom d'hôte".
- Si vous utilisez la fonctionnalité de génération de rapports Web, l'utilisateur `java`, `applet`, *`nom_hôte`* doit être ajouté pour chaque nom d'hôte à partir duquel la fonctionnalité de génération de rapports Web sera utilisée. Notez que pour bénéficier pleinement de la fonctionnalité de génération de rapports Web, les utilisateurs doivent appartenir au même groupe `admin`. Par conséquent, ces clients doivent être sécurisés. De même, avant de mettre à disposition des utilisateurs des données ou la fonctionnalité de génération de rapports Web (par exemple, via un serveur Web), tenez compte des implications que la mise à la disposition générale de ce type de données engendre pour la sécurité.

Pour obtenir des informations détaillées sur la configuration utilisateur, recherchez l'entrée suivante dans l'index de l'aide en ligne : "configuration, utilisateurs".

Activation de la fonction

Pour activer la vérification stricte du nom d'hôte, paramétrez l'indicateur `StrictSecurityFlags 0x0003` dans le fichier d'options globales.

Pour plus d'informations sur le fichier d'options globales, reportez-vous au *Guide de dépannage HP Data Protector*.

Droit utilisateur de démarrage de spécification de sauvegarde

Pour obtenir des informations d'ordre général sur les utilisateurs de Data Protector et les droits utilisateur, recherchez l'entrée suivante dans l'index de l'aide en ligne : "utilisateurs".

Le droit utilisateur `Démarrage de spécification de sauvegarde` seul ne permet pas à un utilisateur d'utiliser le contexte de sauvegarde dans l'interface graphique utilisateur. L'utilisateur peut démarrer une spécification de sauvegarde à partir de la ligne de commande à l'aide de la commande omnib associée à l'option -datalist.

REMARQUE :

S'il associe les droits utilisateur `Démarrer spécification de sauvegarde` et `Démarrer la sauvegarde`, un utilisateur peut visualiser les spécifications de sauvegarde configurées dans l'interface graphique utilisateur et il est en mesure de démarrer une spécification de sauvegarde ou une sauvegarde interactive.

Il n'est pas toujours souhaitable de permettre aux utilisateurs d'effectuer des sauvegardes interactives. Pour autoriser des sauvegardes interactives uniquement aux utilisateurs ayant le droit d'enregistrer une spécification de sauvegarde, paramétrez l'indicateur StrictSecurityFlags 0x0200 dans le fichier d'options globales.

Pour plus d'informations sur le fichier d'options globales, reportez-vous au *Guide de dépannage HP Data Protector*.

Masquage du contenu des spécifications de sauvegarde

Dans un environnement hautement sécurisé, le contenu des spécifications de sauvegarde enregistrées peut être considéré comme sensible, voire confidentiel. Il est possible de configurer Data Protector pour qu'il dissimule le contenu des spécifications de sauvegarde à tous les utilisateurs, à l'exception de ceux qui disposent des droits d'utilisateur *Enregistrer spécification de sauvegarde*. Pour ce faire, réglez l'indicateur StrictSecurityFlags sur 0x0400 dans le fichier d'options globales.

Pour plus d'informations sur le fichier d'options globales, reportez-vous au *Guide de dépannage HP Data Protector*.

Groupement d'hôtes approuvés

La fonctionnalité de groupement d'hôtes approuvés réduit la nécessité d'accorder des droits d'utilisateur Restaurer vers autres clients lorsqu'ils doivent seulement restaurer les données d'un client à un autre parmi un nombre limité de clients. Vous pouvez définir des groupes d'hôtes qui échangeront des données en toute confiance.

Les groupements d'hôtes approuvés sont habituellement utilisés dans les situations suivantes :

- Pour les clients d'un même cluster (noeuds et serveur virtuel).
- Si le nom d'hôte d'un client est modifié et que les données des anciens objets sauvegarde doivent être restaurées.
- En cas d'incohérence entre le nom d'hôte du client et les objets sauvegarde en raison de problèmes liés au DNS.

- Si un utilisateur détient plusieurs clients et doit restaurer les données d'un client vers un autre.
- Lors de la migration de données d'un hôte vers un autre.

Configuration

Pour configurer les groupements d'hôtes approuvés, sur le Gestionnaire de cellule, créez le fichier *donnes_programme_Data_Protector*\Config\Server\cell\host_trusts (Windows Server 2008), *répertoire_Data_Protector*\Config\Server\cell\host_trusts (autres systèmes Windows) ou /etc/opt/omni/server/cell/host_trusts (systèmes UNIX).

Les groupes d'hôtes qui se font confiance mutuellement sont définis en tant que listes de noms d'hôtes placées entre crochets. Par exemple :

Exemple

```
GROUP="cluster.domain.com"
{
    cluster.domain.com
    node1.domain.com
    node2.domain.com
}
GROUP="Bajo"
{
    computer.domain.com
    anothercomputer.domain.com
}
```

Surveillance des événements de sécurité

Si vous rencontrez un problème lors de l'utilisation de Data Protector, vous pouvez consulter les informations des fichiers journaux pour en trouver la cause. Par exemple, les événements consignés pourront vous aider à déterminer les utilisateurs ou clients incorrectement configurés.

Evénements de sécurité client

Les événements de sécurité client sont journalisés dans le fichier inet.log sur chaque client dans le répertoire de la cellule :

- Sous Windows Vista, Windows Server 2008 : *donnes_programme_Data_Protector*\log
- Sur les autres systèmes Windows : *répertoire_Data_Protector*\log
- Sous HP-UX, Solaris et Linux : /var/opt/omni/log
- Sous les autres systèmes UNIX : /usr/omni/log

Evénements de sécurité Gestionnaire de cellule

Les événements de sécurité du Gestionnaire de cellule sont consignés dans le fichier `security.log` qui figure dans le répertoire sur le Gestionnaire de cellule :

- Sous Windows Server 2008 : *donnes_programme_Data_Protector*`\log\server`
- Sur les autres systèmes Windows : *répertoire_Data_Protector*`\log\server`
- Sur les systèmes UNIX : `/var/opt/omni/server/log`

Contrôle des correctifs Data Protector installés

Vous pouvez vérifier quels correctifs Data Protector sont installés sur chaque système de la cellule.

Condition préalable

Pour utiliser cette fonctionnalité, le composant Interface utilisateur ou le client de l'interface Java doit être installé.

REMARQUE :

Si vous avez installé un correctif spécifique pour un site par le passé, celui-ci sera toujours répertorié dans le rapport des correctifs, même s'il a été par la suite inclus dans d'autres correctifs.

Pour vérifier quels sont les correctifs Data Protector installés sur un système donné dans une cellule, utilisez l'interface graphique utilisateur ou l'interface de ligne de commande Data Protector.

Limites

Les limites relatives au contrôle des correctifs sont les suivantes :

- Le contrôle des correctifs vérifie quels correctifs sont installés uniquement sur les membres de la même cellule.

Contrôle des correctifs Data Protector à l'aide de l'interface graphique utilisateur

Pour vérifier quels sont les correctifs installés sur un client en particulier à l'aide de l'interface graphique utilisateur de Data Protector, procédez comme suit :

1. Dans le menu contextuel, cliquez sur Clients.

2. Dans la fenêtre de navigation, développez Clients et sélectionnez un système de la cellule pour lequel vous souhaitez contrôler les correctifs installés.
3. Dans la zone de résultats, cliquez sur Correctifs pour ouvrir la fenêtre Correctifs.

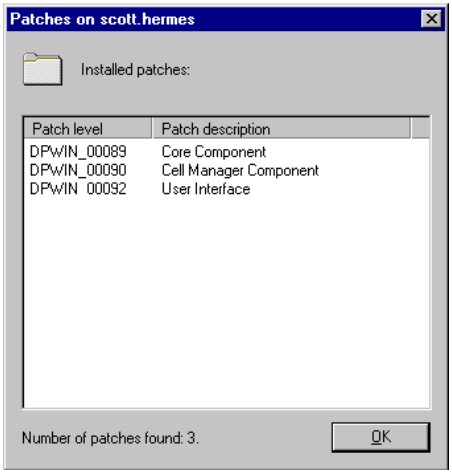

Figure 42 - Vérification des correctifs installés

Si des correctifs sont trouvés sur le système, la procédure de vérification retourne le niveau et la description de chaque chemin, ainsi que le nombre de correctifs installés.

S'il n'existe aucun correctif Data Protector sur le système, la procédure de vérification retourne une liste vide.

Si le système vérifié n'est pas un membre de la cellule, qu'il n'est pas disponible ou qu'une erreur se produit, la procédure de vérification retourne un message d'erreur.

4. Cliquez sur OK pour fermer la fenêtre.

Contrôle des correctifs Data Protector à l'aide de l'interface de ligne de commande

Pour vérifier quels sont les correctifs installés sur un client en particulier à l'aide de l'interface graphique utilisateur de Data Protector, exécutez la commande `omnicheck -patches -host` *`nom_hôte`* à partir du répertoire suivant :

- Sous Windows : *`répertoire_Data_Protector`*`\bin`
- Sous UNIX :`/opt/omni/bin`

où *`nom_hôte`* est le nom du système à vérifier.

Pour en savoir plus sur la commande `omnicheck`, reportez-vous à la page `omnicheck` du manuel.

Désinstallation du logiciel Data Protector

Si la configuration de votre système change, vous souhaiterez peut-être désinstaller Data Protector du système ou retirer certains de ses composants logiciels.

La désinstallation consiste à supprimer tous les composants Data Protector du système, dont *toutes* les références à ce système provenant de la base de données IDB sur l'ordinateur du Gestionnaire de cellule. Cependant, les données de configuration de Data Protector restent sur le système par défaut pour que vous puissiez les utiliser pour la prochaine mise à niveau de Data Protector. Si vous souhaitez supprimer les données de configuration après la désinstallation du logiciel Data Protector, supprimez les répertoires dans lesquels Data Protector a été installé.

Si le répertoire dans lequel Data Protector est installé comporte d'autres données, vérifiez que vous les avez copiées dans un autre emplacement avant de procéder à la désinstallation de Data Protector. Dans le cas contraire, elles seront supprimées au moment de la désinstallation.

La désinstallation du logiciel Data Protector d'une cellule se déroule comme suit :

1. Désinstallation du logiciel client Data Protector à l'aide de l'interface graphique utilisateur. Reportez-vous à la section "Désinstallation d'un client Data Protector" à la page 231.
2. Désinstallation du Gestionnaire de cellule Data Protector et du Serveur d'installation. Reportez-vous à la section "Désinstallation du Gestionnaire de cellule et du Serveur d'installation" à la page 232.

Vous pouvez aussi désinstaller des composants logiciels de Data Protector sans désinstaller le Gestionnaire de cellule ou le client. Reportez-vous à la section "Changement de composants logiciels Data Protector" à la page 242.

Sous UNIX, vous pouvez également supprimer manuellement le logiciel Data Protector. Reportez-vous à la section "Suppression manuelle du logiciel Data Protector sous UNIX" à la page 241.

Configuration système requise

Avant de désinstaller le logiciel Data Protector d'un ordinateur, vérifiez les points suivants :

- Vérifiez que toutes les références à l'ordinateur ont été supprimées des spécifications de sauvegarde. Dans le cas contraire, Data Protector essaiera de sauvegarder des systèmes inconnus et cette partie de la spécification de sauvegarde échouera. Recherchez l'entrée suivante dans l'index de l'aide en ligne : "modification, spécification de sauvegarde" pour de plus amples informations sur la modification des spécifications de sauvegarde.

- Vérifiez qu'aucun périphérique de sauvegarde n'est connecté ou configuré sur le système que vous voulez désinstaller. Une fois le système exporté, Data Protector ne peut plus utiliser ses périphériques de sauvegarde dans la cellule d'origine.

Désinstallation d'un client Data Protector

REMARQUE :

La procédure de désinstallation à distance nécessite que le Serveur d'installation soit installé pour les plates-formes à partir desquelles vous désinstallez le logiciel de Data Protector.

Pour désinstaller un client à distance, procédez comme suit dans l'interface graphique de Data Protector :

1. Dans le menu contextuel, sélectionnez Clients.
2. Dans la fenêtre de navigation, développez Clients, cliquez avec le bouton droit de la souris sur le client à désinstaller, puis cliquez sur Supprimer. Un message vous demande si vous souhaitez également désinstaller le logiciel Data Protector.
3. Cliquez sur Oui pour désinstaller tous les composants logiciels du client, puis sur Terminer.

Le client sera supprimé de la liste figurant dans la zone de résultats et le logiciel Data Protector sera supprimé de son disque dur.

Notez que les données de configuration de Data Protector restent sur le système client. Si vous souhaitez supprimer les données de configuration, supprimez les répertoires dans lesquels Data Protector a été installé.

La désinstallation de Data Protector supprime également le client de l'interface Java. A moins que vous ne décochiez l'option Supprimer définitivement les données de configuration lorsque vous désinstallez Data Protector, les données de configuration de l'interface Java restent sur le système.

Clients cluster

Si votre environnement Data Protector comprend des clients compatibles cluster dans et que vous souhaitez les désinstaller, vous devez le faire localement. La procédure est la même que pour la désinstallation du Gestionnaire de cellule ou du Serveur d'installation. Reportez-vous à la section "Désinstallation du Gestionnaire de cellule et du Serveur d'installation" à la page 232.

Le client cluster sera supprimé de la liste figurant dans la zone de résultats et le logiciel Data Protector sera supprimé de son disque dur.

TruCluster

Pour désinstaller des clients TruCluster, exportez d'abord le noeud virtuel. Désinstallez ensuite les clients Data Protector du (des) noeud(s).

Clients HP OpenVMS

Un client OpenVMS Data Protector ne peut être supprimé à distance avec un Serveur d'installation. Il doit être désinstallé localement.

Pour désinstaller un client Data Protector d'un système OpenVMS, procédez comme suit :

1. Commencez par exporter le client concerné à partir de la cellule Data Protector dans l'interface graphique de ce dernier, comme l'indique la section "Exportation de clients d'une cellule" à la page 211.

   A la question demandant si vous souhaitez désinstaller également le logiciel Data Protector, répondez Non.

2. Pour supprimer le logiciel client Data Protector, connectez-vous au compte `SYSTEM` du client OpenVMS et exécutez la commande suivante : `$ PRODUCT REMOVE DP`. A l'invite, répondez `OUI`.

IMPORTANT :

Cette action ferme le service Data Protector et supprime tous les répertoires, fichiers et comptes associés à Data Protector sur le système OpenVMS.

Désinstallation du Gestionnaire de cellule et du Serveur d'installation

Cette section décrit la procédure permettant de désinstaller le Gestionnaire de cellule et le Serveur d'installation Data Protector des systèmes Windows, HP-UX, Solaris et Linux.

Désinstallation dans un système Windows

Désinstallation sur un système Microsoft Cluster Server

Si vous avez installé l'utilitaire HP AutoPass en même temps que Data Protector sur un noeud Microsoft Cluster Server, vous devez désinstaller Data Protector de ce même noeud ; dans le cas contraire, AutoPass *ne* sera *pas* désinstallé.

Pour désinstaller le logiciel Data Protector d'un système Windows, procédez comme suit :

1. Assurez-vous que toutes les sessions de Data Protector sont terminées et que vous avez quitté l'interface graphique utilisateur.

2. Dans le Panneau de configuration de Windows, cliquez sur Ajout/Suppression de programmes.

3. Selon que vous ayez installé HP AutoPass ou non et selon que vous souhaitiez supprimer les données de configuration de Data Protector ou non, différentes actions sont possibles.

IMPORTANT :

Si vous laissez les données de configuration de Data Protector sur le système après la désinstallation et que vous réinstallez plus tard une version antérieure du Gestionnaire de cellule Data Protector à celle qui était installée, notez que les données de configuration ne seront pas compatibles.

Pour installer correctement une version antérieure, lors de l'installation, choisissez l'option qui supprime les données de configuration.

Pour ce faire, procédez comme suit :

- Si l'utilitaire AutoPass a été installé avec Data Protector : sélectionnez HP Data Protector A.06.10 et cliquez sur Changer puis sur Suivant. Dans la boîte de dialogue Maintenance du programme, cliquez sur Supprimer. Pour supprimer définitivement les données de configuration de Data Protector, sélectionnez Supprimer définitivement les données de configuration. Dans le cas contraire, cliquez sur Suivant.
  Si AutoPass a été installé en même temps que Data Protector et que Data Protector est la seule application qui l'utilise, AutoPass est supprimé. Dans le cas contraire, seul l'enregistrement d'AutoPass auprès de Data Protector est annulé, mais l'utilitaire reste installé. Pour supprimer manuellement AutoPass, exécutez :
  `msiexec.exe /X ID_interface graphique_package /qr INSTALLSTANDALONE=1`
  Vous trouverez l'ID de l'interface graphique sous l'entrée du registre `HKEY_LOCAL_MACHINE\Software\Hewlett-Packard\HpOvLic`.
- Si AutoPass n'a pas été installé :
  - Pour désinstaller Data Protector et conserver les données de configuration Data Protector sur le système, sélectionnez HP Data Protector A.06.10 et cliquez sur Supprimer.
  - Pour désinstaller Data Protector et supprimer ses données de configuration, sélectionnez HP Data Protector A.06.10, cliquez sur Changer puis sur Suivant. Dans la boîte de dialogue Maintenance du programme, cliquez sur Supprimer. Sélectionnez Supprimer définitivement les données de configuration et cliquez sur Suivant.

4. Lorsque la désinstallation est terminée, cliquez sur Terminer pour quitter l'assistant.

Si AutoPass est supprimé au cours de la désinstallation du Gestionnaire de cellule, appuyez sur F5dans la fenêtre Ajout/Suppression de programmes pour réactualiser la liste des programmes et composants installés.

Désinstallation dans un système HP-UX

IMPORTANT :

Si vous laissez les données de configuration de Data Protector sur le système après la désinstallation et que vous réinstallez plus tard une version antérieure du Gestionnaire de cellule Data Protector à celle qui était installée, notez que les données de configuration ne seront pas compatibles.

Pour installer correctement une version antérieure, après la désinstallation, supprimez les répertoires Data Protector de votre système.

Avant de commencer à désinstaller le logiciel Data Protector, arrêtez tous les processus Data Protector en cours d'exécution sur le système du Gestionnaire de cellule et/ou du Serveur d'installation :

1. Connectez-vous en tant que root et exécutez la commande `omnisv -stop` à partir du répertoire `/opt/omni/sbin`.
2. Entrez la commande `ps -ef | grep omni` pour vérifier si tous les processus ont bien été arrêtés. Aucun processus Data Protector ne devrait être répertorié sur exécution de la commande ps -ef | grep omni.

   Si vous avez des processus Data Protector en cours d'exécution, arrêtez-les à l'aide de la commande `kill -9 ID_processus` avant de procéder à la désinstallation.
3. Exécutez `/usr/sbin/swremove DATA-PROTECTOR` pour désinstaller le logiciel Data Protector.
4. L'utilitaire HP AutoPass n'est pas supprimé lors de la désinstallation de Data Protector. Vous pouvez le supprimer manuellement en exécutant la commande `/usr/sbin/swremove HPOVLIC` en tant qu'utilisateur root.

Pour supprimer les répertoires restants de Data Protector de votre système, reportez-vous à la section "Suppression manuelle du logiciel Data Protector sous UNIX" à la page 241.

Désinstallation du Gestionnaire de cellule et/ou du Serveur d'installation configuré(s) sur MC/ServiceGuard

Si votre Gestionnaire de cellule et/ou votre Serveur d'installation sont configurés sur un cluster MC/ServiceGuard, procédez comme suit pour désinstaller le logiciel.

Nœud principal

Connectez-vous au nœud principal et procédez comme suit :

1. Arrêtez le package Data Protector :

   `cmhaltpkg` *`nom_pkg`*

   où *`nom_pkg`* correspond au nom du package de clusters.

   Par exemple :

   `cmhaltpkg ob2cl`

2. Désactivez le mode cluster pour le groupe de volumes :

   `vgchange -c n` *`nom_gv`*

   (où *`nom_gv`* correspond au nom du chemin du groupe de volumes placé dans le sous-répertoire du répertoire `/dev`).

   Par exemple :

   `vgchange -c n /dev/vg_ob2cm`

3. Activez le groupe de volumes :

   `vgchange -a y -q y` *`nom_gv`*

   Par exemple :

   `vgchange -a y -q y /dev/vg_ob2cm`

4. Montez le volume logique sur le disque partagé :

   `mount` *`chemin_vl disque_partagé`*

   (où *`chemin_vl`* correspond au nom de chemin du volume logique et où *`disque_partagé`* correspond au point de montage ou répertoire partagé).

   Par exemple :

   `mount /dev/vg_ob2cm/lv_ob2cm /omni_shared`

5. Supprimez Data Protector à l'aide de l'outil swremove.

6. Supprimez les liens programmables :

   `rm /etc/opt/omni`

   `rm /var/opt/omni`

7. Supprimez les répertoires de sauvegarde :

   `rm -rf /etc/opt/omni.save`

   `rm -rf /var/opt/omni.save`

8. Supprimez le répertoire Data Protector et son contenu :

   `rm -rf /opt/omni`

9. Vous pouvez supprimer l'utilitaire HP AutoPass en exécutant la commande `/usr/sbin/swremove HPOVLIC` en tant qu'utilisateur root.

10. Démontez le disque partagé :

    `umount disque_partagé`

    Par exemple :

    `umount /omni_shared`

11. Désactivez le groupe de volumes :

    `vgchange -a n nom_gv`

    Par exemple :

    `vgchange -a n /dev/vg_ob2cm`

Nœud secondaire

Connectez-vous au nœud secondaire et procédez comme suit :

1. Activez le groupe de volumes :

   `vgchange -a y nom_gv`

2. Montez le disque partagé :

   `mount chemin_vl disque_partagé`

3. Supprimez Data Protector à l'aide de l'outil `swremove`.
4. Supprimez les liens programmables :

   `rm /etc/opt/omni`

   `rm /var/opt/omni`

5. Supprimez les répertoires de sauvegarde :

   `rm -rf /etc/opt/omni.save`

   `rm -rf /var/opt/omni.save`

6. Supprimez le répertoire Data Protector et son contenu :

   `rm -rf /opt/omni`

7. Supprimez les répertoires du système de fichiers partagé :

   `rm -rf disque_partagé/etc_opt_omni`

   `rm -rf disque_partagé/var_opt_omni`

   Par exemple :

   `rm -rf /omni_shared/etc_opt_omni`

   `rm -rf /omni_shared/etc_opt_omni`

8. Vous pouvez supprimer l'utilitaire HP AutoPass en exécutant la commande `/usr/sbin/swremove HPOVLIC` en tant qu'utilisateur root.

9. Démontez le disque partagé :

   `umount disque_partagé`

10. Désactivez le groupe de volumes :

   `vgchange -a n nom_gv`

Data Protector est complètement supprimé du système.

Désinstallation dans les systèmes Solaris

Gestionnaire de cellule

Le Gestionnaire de cellule pour Solaris est toujours installé en local, à l'aide de la commande `omnisetup.sh`. Par conséquent, il doit être désinstallé en local à l'aide de l'utilitaire `pkgrm`.

IMPORTANT :

Si vous laissez les données de configuration de Data Protector sur le système après la désinstallation et que vous réinstallez plus tard une version antérieure du Gestionnaire de cellule Data Protector à celle qui était installée, notez que les données de configuration ne seront pas compatibles.

Pour installer correctement une version antérieure, après la désinstallation, supprimez les répertoires Data Protector de votre système.

Pour désinstaller le Gestionnaire de cellule Data Protector, procédez comme suit :

1. Assurez-vous que vous avez terminé toutes les sessions de Data Protector et quitté l'interface graphique utilisateur.
2. Entrez la commande `pkginfo | grep OB2` pour répertorier tous les packages Data Protector installés sur le Gestionnaire de cellule.

   Les packages associés au Gestionnaire de cellule se répartissent comme suit :

OB2-CORE	Logiciel central Data Protector
OB2-C-IS	Logiciel du Serveur d'installation
OB2-CS	Logiciel du Gestionnaire de cellule
OB2-CC	Logiciel de la console de cellule, contenant l'interface graphique utilisateur et l'interface de ligne de commande

   Si des clients Data Protector ou Serveur d'installation sont aussi installés sur le système, les autres packages seront également répertoriés.

REMARQUE :

Si vous souhaitez laisser tout autre composant Data Protector installé, vous devez conserver le package OB2-CORE car il est indispensable au fonctionnement des autres packages.

3. Supprimez dans l'ordre inverse de celui où ils ont été installés les packages mentionnés dans l'étape précédente par la commande `pkgrm` *`nom du package`* et suivez les instructions qui apparaissent sur la ligne de commande.
4. L'utilitaire HP AutoPass n'est pas supprimé lors de la désinstallation de Data Protector. Vous pouvez le supprimer manuellement en exécutant les commandes suivantes en tant qu'utilisateur root :

   ```
   swremove HPOvLic
   ```

Serveur d'installation

Le Serveur d'installation pour UNIX sur Solaris est toujours installé en local à l'aide de la commande `omnisetup.sh`.. Par conséquent, il doit être désinstallé en local à l'aide de l'utilitaire `pkgrm`..

Pour désinstaller le Serveur d'installation Data Protector, procédez comme suit :

1. Assurez-vous que toutes les sessions de Data Protector sont terminées et que vous avez quitté l'interface graphique utilisateur.
2. Entrez la commande `pkginfo | grep OB2` pour répertorier tous les packages Data Protector installés sur le système du Serveur d'installation.

   Les packages associés au Serveur d'installation se répartissent comme suit :

OB2-CORE	Logiciel central Data Protector
OB2-C-IS	Logiciel central Serveur d'installation
OB2-SOLUX	Ensembles de l'Agent de disque, de l'Agent de support et de l'interface graphique utilisateur pour les systèmes Solaris distants
OB2-OTHUX	Ensembles de l'Agent de disque et de l'Agent de support pour systèmes UNIX non-Solaris distants

   Si d'autres composants Data Protector sont installés sur le système, ils seront également répertoriés.

REMARQUE :

Si vous souhaitez laisser tout autre composant Data Protector installé, vous devez conserver le package OB2-CORE car il est indispensable au fonctionnement des autres packages.

3. Supprimez dans l'ordre inverse de celui où ils ont été installés les packages mentionnés dans l'étape précédente par la commande `pkgrm` *`nom du package`* et suivez les instructions qui apparaissent sur la ligne de commande.

Désinstallation dans les systèmes Linux

Gestionnaire de cellule

Le Gestionnaire de cellule pour Linux est toujours installé en local, à l'aide de la commande `omnisetup.sh`. Par conséquent, il doit être désinstallé en local à l'aide de l'utilitaire `rpm`.

IMPORTANT :

Si vous laissez les données de configuration de Data Protector sur le système après la désinstallation et que vous réinstallez plus tard une version antérieure du Gestionnaire de cellule Data Protector à celle qui était installée, notez que les données de configuration ne seront pas compatibles.

Pour installer correctement une version antérieure, après la désinstallation, supprimez les répertoires Data Protector de votre système.

Pour désinstaller le Gestionnaire de cellule Data Protector, procédez comme suit :

1. Assurez-vous que vous avez terminé toutes les sessions de Data Protector et quitté l'interface graphique utilisateur.
2. Entrez la commande rpm -qa | grep OB2 pour répertorier tous les packages Data Protector installés sur le Gestionnaire de cellule.

   Les packages associés au Gestionnaire de cellule se répartissent comme suit :

OB2-CORE	Logiciel central Data Protector
OB2-CORE-IS	Logiciel du Serveur d'installation
OB2-CS	Logiciel du Gestionnaire de cellule
OB2-CC	Logiciel de la console de cellule, contenant l'interface de ligne de commande.

Si des clients Data Protector ou Serveur d'installation sont aussi installés sur le système, les autres packages seront également répertoriés.

REMARQUE :

Si vous souhaitez laisser tout autre composant Data Protector installé, vous devez conserver le package OB2-CORE car il est indispensable au fonctionnement des autres packages.

3. Supprimez dans l'ordre inverse de celui où il ont été installés les packages mentionnés dans l'étape précédente par la commande `rpm -e`*`nom du package`* et suivez les instructions qui apparaissent sur la ligne de commande.

Serveur d'installation

Le Serveur d'installation pour UNIX sous Linux est toujours installé en local à l'aide de la commande `omnisetup.sh`. Par conséquent, il doit être désinstallé en local à l'aide de l'utilitaire `rpm`.

Pour désinstaller le Serveur d'installation Data Protector, procédez comme suit :

1. Assurez-vous que toutes les sessions de Data Protector sont terminées et que vous avez quitté l'interface graphique utilisateur.
2. Entrez la commande rpm -qa | grep OB2 pour répertorier tous les packages Data Protector installés sur le Serveur d'installation.

   Les packages associés au Serveur d'installation se répartissent comme suit :

OB2-CORE	Logiciel central Data Protector
OB2-CORE-IS	Logiciel central Serveur d'installation
OB2-LINUXP	Ensembles de l'Agent de disque, de l'Agent de support et de l'interface graphique utilisateur pour les systèmes Linux distants
OB2-OTHUXP	Ensembles de l'Agent de disque et de l'Agent de support pour systèmes UNIX non-Linux distants

   Si d'autres composants Data Protector sont installés sur le système, ils seront également répertoriés.

REMARQUE :

Si vous souhaitez laisser tout autre composant Data Protector installé, vous devez conserver le package OB2-CORE car il est indispensable au fonctionnement des autres packages.

3. Supprimez dans l'ordre inverse de celui où il ont été installés les packages mentionnés dans l'étape précédente par la commande `rpm -e`*`nom du package`* et suivez les instructions qui apparaissent sur la ligne de commande.

Suppression manuelle du logiciel Data Protector sous UNIX

Avant de désinstaller un client UNIX, vous devez l'exporter de la cellule. Pour connaître la procédure, reportez-vous à la section "Exportation de clients d'une cellule" à la page 211.

Systèmes HP-UX

Pour supprimer manuellement les fichiers d'un système HP-UX, procédez comme suit :

1. Exécutez `/usr/sbin/swremove DATA-PROTECTOR` pour supprimer le logiciel Data Protector.
2. Supprimez les répertoires suivants à l'aide de la commande `rm` :

   ```
   rm -fr /var/opt/omni
   rm -fr /etc/opt/omni
   rm -fr /opt/omni
   ```

   A ce stade, les références Data Protector ne figurent plus sur votre système.

Systèmes Solaris

Pour supprimer manuellement les fichiers d'un système Solaris, supprimez-les des répertoires suivants, puis supprimez les répertoires à l'aide de la commande `rm` :

```
rm -fr /var/opt/omni
rm -fr /etc/opt/omni
rm -fr /opt/omni
```

Systèmes Linux

Pour supprimer manuellement les fichiers d'un système Linux, supprimez-les des répertoires suivants, puis supprimez les répertoires à l'aide de la commande `rm` :

```
rm -fr /var/opt/omni
rm -fr /etc/opt/omni
rm -fr /opt/omni
```

Autres systèmes UNIX

Supprimez les fichiers du répertoire suivant, puis supprimez le répertoire à l'aide de la commande `rm` :

```
rm -fr /usr/omni
```

Changement de composants logiciels Data Protector

Cette section décrit la procédure de suppression et d'ajout de composants logiciels Data Protector sur les systèmes Windows HP-UX, Solaris et Linux. Pour obtenir la liste des composants Data Protector pris en charge selon les systèmes d'exploitation, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.

Les composants logiciels Data Protector peuvent être ajoutés sur le Gestionnaire de cellule ou sur un client à l'aide de l'interface graphique utilisateur de Data Protector. L'installation à distance de composants sélectionnés s'effectue à l'aide de la fonctionnalité Serveur d'installation. Pour en connaître la procédure détaillée, reportez-vous à la section "Installation distante de clients Data Protector" à la page 78.

Les composants Data Protector peuvent être supprimés en local sur le Gestionnaire de cellule ou sur un client.

Sur les systèmes Windows

Pour ajouter ou supprimer des composants logiciels Data Protector sous Windows, procédez comme suit :

1. Dans le Panneau de configuration de Windows, cliquez sur Ajout/Suppression de programmes.
2. Sélectionnez HP Data Protector A.06.10 et cliquez sur Modifier.
3. Cliquez sur Suivant.
4. Dans la fenêtre Maintenance du programme, cliquez sur Modifier, puis sur Suivant.
5. Dans la fenêtre Installation personnalisée, sélectionnez les composants à ajouter et/ou désélectionnez les composants à supprimer. Cliquez sur Suivant.
6. Cliquez sur Installer pour lancer l'installation ou la suppression des composants logiciels.
7. Lorsque l'installation est terminée, cliquez sur Terminer.

Clients compatibles cluster

Si vous modifiez les composants logiciels de Data Protector sur les clients compatibles cluster, vous devez le faire localement, à partir du DVD-ROM, sur chaque nœud de cluster. Ensuite, vous devez importer manuellement le nom d'hôte du serveur virtuel dans la cellule Data Protector à l'aide de l'interface utilisateur.

Sur les systèmes HP-UX

Vous pouvez ajouter de nouveaux composants à l'aide de la fonctionnalité Serveur d'installation. Sur les systèmes HP-UX, certains composants Data Protector dépendent les uns des autres et ne pourront fonctionner correctement si vous supprimez l'un d'entre eux. Le tableau ci-dessous présente les composants et leurs interdépendances :

Tableau 8 - Dépendances de composants logiciels Data Protector sous HP-UX

Composants	dépendent de...
OMNI-CC, OMNI-CORE-IS	OMNI-CORE
OMNI-CS	OMNI-CORE, OMNI-CC
OMNI-INTEG , OMNI-DA, OMNI-MA, OMNI-VLSAM ou OMNI-NDMP	OMNI-CORE
OMNI-NDMP-P, OMNI-JGUI-P	OMNI-CORE-IS
OMNI-INF-P, OMNI-SYB-P, OMNI-ORA-P, OMNI-OR8-P, OMNI-SAP-P, OMNI-SAPDB-P, OMNI-DB2-P, OMNI-EMC-P, OMNI-SSEA-P, OMNI-SNAPA-P, OMNI-SMISA-P	OMNI-INTEG, OMNI-CORE-IS
OMNI-HPUX-P, OMNI-OTHUX-P, OMNI-OMNIST	OMNI-CORE-IS
OMNI-LOTUS-P, OMNI-OV-P	OMNI-CORE-IS

Procédure

Pour supprimer des composants logiciels Data Protector, procédez comme suit :

1. Connectez-vous en tant que `root`, puis exécutez la commande `swremove`.
2. Cliquez deux fois sur B6960MA, DATA-PROTECTOR, puis sur OB2-CM pour afficher une liste des composants Data Protector.
3. Sélectionnez les composants à supprimer.
4. Dans le menu Actions, cliquez sur Marquer pour suppression pour repérer les composants devant être supprimés.
5. Après avoir marqué les composants à supprimer, cliquez sur Supprimer dans le menu Actions, puis sur OK.

REMARQUE :

Lorsque vous marquez les composants Data Protector à supprimer et que la suppression de ceux-ci risque d'affecter le fonctionnement d'autres composants, la boîte Dépendances apparaît pour vous présenter la liste des composants dépendants.

Spécificités d'Oracle

Après la désinstallation de l'intégration Oracle Data Protector sur un système de serveur Oracle, le logiciel Oracle Server reste lié à la bibliothèque de base de données Data Protector. Vous devez supprimer ce lien, faute de quoi vous ne pourrez pas démarrer le serveur Oracle après suppression de l'intégration. Reportez-vous à la section "Utilisation d'Oracle après le retrait de l'intégration d'Oracle dans Data Protector" dans le *Guide d'intégration HP Data Protector*.

Sur les systèmes Solaris

Vous pouvez ajouter de nouveaux composants à l'aide de la fonctionnalité Serveur d'installation. Sur les systèmes Solaris, certains composants logiciels Data Protector dépendent les uns des autres et ne pourront fonctionner correctement si vous supprimez l'un d'entre eux. Le tableau ci-dessous présente les composants et leurs interdépendances:

Tableau 9 - Dépendances des composants logiciels Data Protector sous Solaris

Composants	dépendent de...
OB2-CC, OB2-C-IS	OB2-CORE
OB2-CS	OB2-CORE, OB2-CC
OB2-INTGP, OB2-DA, OB2-MA, OB2-VLSAM ou OB2-NDMPP	OB2-CORE
OB2-SOLUX, OB2-JGUI-P	OB2-C-IS
OB2-INFP, OB2-SYBP, OB2-OR8P, OB2-SAPP, OB2-SAPDP, OB2-DB2P, OB2-SSEAP, OB2-SMISP	OB2-INTGP, OB2-C-IS
OB2-OTHUX, OB2-OSTP, OB2-LOTP, OB2-OVP	OB2-C-IS

Procédure

Pour supprimer des composants logiciels Data Protector sur des systèmes Solaris, procédez comme suit :

1. Assurez-vous que toutes les sessions de Data Protector sont terminées et que vous avez quitté l'interface graphique utilisateur.
2. Entrez la commande `pkginfo | grep OB2` pour répertorier tous les packages Data Protector installés.
3. Supprimez dans l'ordre inverse de celui où ils ont été installés les packages mentionnés dans l'étape précédente par la commande `pkgrm` *`nom du package`* et suivez les instructions qui apparaissent sur la ligne de commande.

Autres systèmes UNIX

Lorsque vous supprimez manuellement des composants d'un client Data Protector sur un système UNIX autre que Solaris ou HP-UX, mettez à jour le fichier `omni_info` dans `/usr/omni/bin/install/omni_info`.

Pour chacun des composants désinstallés, supprimez la chaîne de version du composant associé dans le fichier `omni_info`.

Si vous supprimez simplement des composants d'un client Data Protector et que vous n'avez pas exporté le client à partir de la cellule, vous devrez mettre à jour la configuration de la cellule dans le fichier `cell_info` (sur le Gestionnaire de cellule). Pour ce faire, utilisez la commande suivante sur un système dans la cellule, avec la console de cellule installée :

```
/opt/omni/bin/omnicc -update_host nom_hôte
```

4 Mise à niveau vers Data Protector A.06.10

Description du chapitre

Ce chapitre décrit les procédures de mise à niveau et de migration de Data Protector.

Présentation de la mise à niveau

Avant de commencer

Avant de mettre à niveau une version de produit existante vers Data Protector A.06.10, tenez compte des éléments suivants :

- Pour en savoir plus sur les plates-formes et versions prises en charge ou non, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- Après la mise à niveau, le Gestionnaire de cellule et le Serveur d'installation doivent avoir la même version de Data Protector installée. Pour les clients, il est recommandé d'installer la même version. Les clients Agents de disque et Agents de support sont également pris en charge.
- Après la mise à niveau d'un environnement à plusieurs cellules (MoM), la même version de Data Protector doit être installée sur chaque Gestionnaire de cellule.
- Si vous avez une licence permanente pour Data Protector A.05.10, Data Protector A.05.50, ou Data Protector A.06.00, elle peut être utilisée avec Data Protector A.06.10.
  Dans le cas contraire, assurez-vous que vous disposez d'une licence temporaire valable pour une durée de 60 jours à partir de la date d'installation d'origine. Pour plus de détails sur la gestion des licences, reportez-vous au Chapitre 5 à la page 307.

Condition préalable

- Réalisez une sauvegarde du système de Gestionnaire de cellule existant et de la base de données interne (IDB).
- Lorsque vous mettez à niveau le Gestionnaire de cellule à partir d'un système à l'aide de Data Protector A.05.10, A.05.50, ou A.06.00 vers Data Protector A.06.10, vous devez d'abord mettre à jour le Gestionnaire de cellule existant vers Data Protector A.06.10.

- La mise à niveau de Data Protector A.06.10 est prise en charge uniquement pour Data Protector A.05.10, Data Protector A.05.50 et Data Protector A.06.00.
- Avec Data Protector A.06.10, vous ne pouvez pas restaurer une sauvegarde de la base de données interne créée avec des versions précédentes de Data Protector. Une fois le Gestionnaire de cellule mis à niveau, sauvegardez la base de données interne avant de continuer à utiliser Data Protector.
- Le changement de plate-forme du Gestionnaire de cellule n'est pas pris en charge dans la version A.06.10 de Data Protector. Les mises à niveau sont prises en charge uniquement sur une même plate-forme de Gestionnaire de cellule (de HP-UX à HP-UX, de Solaris à Solaris etde Windows à Windows).
- Si vous effectuez la mise à niveau vers Data Protector A.06.10 sous Windows et si votre version de Microsoft Installer est antérieure à 2.0, le programme d'installation de Data Protector met automatiquement cette dernière à niveau vers la version 2.0. Dans ce cas, Data Protector affichera une remarque à la fin de l'installation, indiquant que MSI a été mis à niveau. Si MSI a été mis à niveau, il est vivement recommandé de redémarrer le système. Consultez le support de Microsoft pour en savoir plus sur les prérequis de MSI 2.0 en fonction des différents systèmes d'exploitation Windows.
  Pour connaître la version de MSI installée sur votre système, cliquez avec le bouton droit sur `c:\winnt\system32\msi.dll` dans l'Explorateur et sélectionnez Propriétés. Dans la boîte de dialogue Propriétés, sélectionnez Version.

Séquence de mise à niveau

Pour mettre à niveau votre cellule des versions précédentes du produit vers Data Protector A.06.10, procédez comme suit :

1. Mettez à niveau le Gestionnaire de cellule et le Serveur d'installation vers Data Protector A.06.10. La procédure est différente pour les plates-formes UNIX et Windows.

   Notez que vous devez d'abord mettre à niveau le Gestionnaire de cellule dans la cellule actuelle avant de pouvoir mettre à niveau le Serveur d'installation.

   Pour certaines configurations de cellule spécifiques, les noms de fichiers de la base de données IDB doivent être convertis après la mise à niveau du Gestionnaire de cellule. Dans ce cas, un message vous y invitera. Reportez-vous au Tableau 11 à la page 278 et au Tableau 12 à la page 279.
2. Mettez à niveau les clients de l'interface graphique utilisateur.
3. Mettez à niveau les clients qui ont une intégration d'application en ligne installée, telles qu'Oracle, SAP R/3, Informix Server, Microsoft SQL Server, Microsoft Exchange Server et autres.

4. Mettez à niveau les clients sur lesquels un Agent de support (MA) est installé. Vous pouvez effectuer des sauvegardes dès que l'Agent de support (MA) est mis à niveau sur tous les clients MA de la même plate-forme que le Gestionnaire de cellule. Pour le client MA Data Protector A.05.10, certaines limites s'appliquent. Reportez-vous au Tableau 11 à la page 278 et au Tableau 12 à la page 279.
5. Il est recommandé de réaliser une mise à niveau des clients sur lesquels l'Agent de disque (DA) du système de fichiers est installé, dans un délai de quinze jours.

   Pour plus d'informations sur l'impact de la version de l'Agent de disque (DA) sur la sauvegarde et la restauration avant et après la conversion des noms de fichiers de la base de données IDB, reportez-vous à la section "Conversion des noms de fichiers de la base de données IDB" à la page 277.

Mise à niveau dans un environnement MoM

Pour mettre à niveau votre environnement MoM vers Data Protector A.06.10, vous devez dans un premier temps mettre à niveau le système du Gestionnaire MoM. Cela fait, chaque Gestionnaire de cellule des versions précédentes qui n'aurait pas encore été mis à niveau peut accéder à la MMDB centrale et à l'attribution centralisée des licences, et effectuer des sauvegardes, mais les autres fonctionnalités ne sont pas disponibles. Notez que le partage de périphériques entre la cellule MoM Data Protector A.06.10 et les cellules sur lesquelles d'anciennes versions du produit sont installées n'est pas assuré. Pendant la mise à niveau d'un environnement MoM, aucun des Gestionnaires de cellule de l'environnement MoM ne doit fonctionner.

Conversion nécessaire des noms de fichier de la base de données IDB

Dans les versions A.05.50, A.06.00 et A.06.10 de Data Protector, la gestion et l'affichage des noms de fichiers créés avec des paramètres régionaux différents sur des plates-formes différentes ont été améliorés. Ceci nécessite la conversion des noms de fichiers existants de la base de données IDB pour certaines configurations de cellule spécifiques si vous effectuez une mise à niveau à partir de Data Protector A.05.10.

La conversion est effectuée sur :

- le Gestionnaire de cellule UNIX dans le cadre de la sauvegarde post-mise à niveau des clients Windows ;
- le Gestionnaire de cellule Windows en processus d'arrière-plan après la mise à niveau du Gestionnaire de cellule.

Si nécessaire, un message vous invitera à effectuer la conversion de la base de données IDB.

UNIX

Sur un Gestionnaire de cellule UNIX, la conversion de la base de données IDB est réalisée dans le cadre des sauvegardes post-mise à niveau des clients Windows

- jusqu'à l'expiration de la période de conversion ou
- jusqu'à ce qu'une sauvegarde complète de tous les clients Windows de la cellule ait été réalisée. Cette étape est très importante et indispensable.

Pour obtenir des données chiffrées sur les performances de la conversion des noms de fichiers, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.

Windows

Sur un Gestionnaire de cellule Windows, la conversion de la base de données IDB peut être reportée à une date ultérieure. Toutefois, certaines limites s'appliquent jusqu'à ce qu'elle soit réalisée.

Vous trouverez des informations plus détaillées concernant la conversion des noms de fichier de la base de données IDB sur les Gestionnaires de cellule Windows et UNIX dans la section "Conversion des noms de fichiers de la base de données IDB" à la page 277.

Auto-migration des clés de cryptage

Après la mise à niveau du Gestionnaire de cellule, du Serveur d'installation et de tous les clients vers Data Protector A.06.10, la commande `omnikeymigrate` migre automatiquement tous les fichiers de `banque de clés` existants à partir de tous les systèmes client dans la cellule et les importe dans le fichier central de `banque de clés` dans le Gestionnaire de cellule Data Protector A.06.10. Si une clé de cryptage active est migrée du système client spécifié, toutes les spécifications de sauvegarde associées à ce système sont migrées automatiquement avec la clé. Une fois l'importation terminée, toutes les clés de cryptage migrées sont inactives.

Si, pour une raison quelconque, l'auto-migration ne fonctionne pas, vous pouvez migrer manuellement les clés de cryptage. Pour plus de détails, reportez-vous à la page `omnikeymigrate` du manuel ou au *Guide de rfrence de l'interface de ligne de commande HP Data Protector*.

Mise à niveau à partir de Data Protector A.05.10, A.05.50 et A.06.00

Les versions de Data Protector A.05.10, A.05.50 et A.06.00 peuvent être directement mises à niveau vers Data Protector A.06.10 pour les plates-formes UNIX et Windows.

Licences

Les licences existantes de Data Protector A.05.10, A.05.50 and A.06.00 sont totalement compatibles et valides pour une utilisation avec Data Protector A.06.10. Pour plus de détails sur la gestion des licences, reportez-vous au Chapitre 5 à la page 307.

Avant de commencer

Avant de commencer la mise à niveau, reportez-vous à la section "Présentation de la mise à niveau" à la page 247 pour plus d'informations sur les limites et la séquence de mise à niveau.

Mise à niveau du Gestionnaire de cellule et du Serveur d'installation UNIX

Configuration requise

- Arrêtez tous les services Data Protector en exécutant la commande `/opt/omni/sbin/omnisv -stop`.
- Sur Solaris, si des anciens correctifs sont installés, désinstallez-les avant la mise à niveau.
- Le shell POSIX (`sh`) doit être installé.
- Vous devez bénéficier des droits `root` pour effectuer la mise à niveau.

Si le Serveur d'installation HP-UX, Solaris ou Linux est installé conjointement avec le Gestionnaire de cellule, il est mis à niveau automatiquement lorsque la commande `omnisetup.sh` est exécutée.

Si le Serveur d'installation HP-UX, Solaris ou Linux est installé sur un système distinct, reportez-vous à la section "Mise à niveau d'un Serveur d'installation" à la page 254.

Mise à niveau d'un Gestionnaire de cellule

Le Gestionnaire de cellule HP-UX, Solaris ou Linux est mis à niveau automatiquement lorsque la commande `omnisetup.sh` est exécutée.

Sous HP-UX, cette commande met automatiquement à niveau le package existant à l'aide de l'utilitaire `swinstall`. Sous Solaris, cette commande supprime l'ensemble des packages existants à l'aide de l'utilitaire `pkgrm` et installe les nouveaux packages à l'aide de l'utilitaire `pkgadd`. Sous Linux, cette commande met automatiquement à niveau le package existant à l'aide de l'utilitaire `rpm`.

Si le Serveur d'installation est installé avec des composants client, il sera supprimé par la commande `omnisetup.sh`. Dans ce cas, installez un nouveau dépôt du Serveur d'installation au moyen de la commande `omnisetup.sh -IS`, puis réimportez le Serveur d'installation mis à niveau. Pour plus de détails, reportez-vous à la section "Importation d'un serveur d'installation dans une cellule" à la page 207.

MC/ServiceGuard

La procédure de mise à niveau du Gestionnaire de cellule configuré sur MC/SG est différente de celle effectuée sur un Gestionnaire de cellule ne fonctionnant pas dans l'environnement MC/SG. La procédure détaillée correspondante est décrite à la section

"Mise à niveau du Gestionnaire de cellule configuré sur MC/ServiceGuard" à la page 298.

Définition des paramètres de noyau

Sous HP-UX, il est recommandé de régler le paramètre de noyau `maxdsiz` (taille maximale des segments de données) ou `maxdsiz_64` (pour les systèmes 64 bits) sur au moins 134 217 728 octets (128 Mo), et le paramètre de noyau `semmnu` (nombre de structures Undo de sémaphore) sur au moins 256 Mo. Une fois ces modifications effectuées, recompilez le noyau et redémarrez la machine.

Sur les systèmes Solaris, il est recommandé de définir le paramètre de noyau `shmsys:shminfo_shmmax` (taille maximale des segments de la mémoire partagée (`SHMMAX`)) situé dans `/etc/system` sur au moins 67 108 864 octets (64 Mo). Une fois la modification effectuée, redémarrez la machine.

Procédure de mise à niveau

Procédez comme suit pour mettre à niveau le Gestionnaire de cellule HP-UX, Solaris ou Linux vers Data Protector A.06.10 :

1. Insérez et montez le DVD-ROM d'installation UNIX sur un point de montage.

   Par exemple :

   ```
   mkdir /dvdrom mount /dev/c0d0t0 /dvdrom
   ```

   Si vous souhaitez installer Data Protector depuis un dépôt sur le disque, procédez comme suit :

   - Copiez les répertoires `DP_DEPOT`, `LOCAL_INSTALL` et `AUTOPASS` (où se trouvent les fichiers d'installation) :
     `mkdir` *`répertoire`* `cp -r /dvdrom/`*`rép_plateforme`*`/DP_DEPOT` *`répertoire`* `cp -r /dvdrom/`*`rép_plateforme`*`/AUTOPASS` *`répertoire`* `cp -r /dvdrom/LOCAL_INSTALL` *`répertoire`*
     Où *`rép_plateforme`* est :

`hpux_ia`	HP-UX sur systèmes IA-64
`hpux_pa`	HP-UX sur systèmes PA-RISC
`solaris`	Systèmes Solaris
`linux`	Systèmes Linux

   - Copiez l'ensemble du DVD-ROM sur votre disque local :
     `cp -r /dvdrom` *`rép_image_dvd`*

2. Exécutez la commande `omnisetup.sh`.

   Pour lancer cette commande à partir du DVD-ROM, exécutez :

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

   Pour lancer l'installation à partir du disque :

   - Si vous avez copié les répertoires `DP_DEPOT`, `LOCAL_INSTALL` et `AUTOPASS` sur votre disque local sous *répertoire*, allez sur le répertoire qui contient le fichier `omnisetup.sh` et exécutez la commande suivante :
     ```
     cd répertoire/LOCAL_INSTALL
     ./omnisetup.sh
     ```
   - Si vous avez copié l'intégralité du DVD-ROM dans *rép_image_dvd*, exécutez la commande `omnisetup.sh` sans paramètres :
     ```
     cd rép_image_dvd/LOCAL_INSTALL
     ./omnisetup.sh
     ```

3. `omnisetup.sh` vous invite à installer ou à mettre à niveau l'utilitaire HP AutoPass si vous souhaitez télécharger et installer les mots de passe correspondant aux licences achetées directement via Internet à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus d'informations sur l'utilitaire AutoPass, reportez-vous à l'aide en ligne HP AutoPass. L'installation d'AutoPass est recommandée.

   Si AutoPass est installé sous MC/ServiceGuard, il doit être installé ou mis à niveau sur tous les nœuds.

   Lorsque vous y êtes invité, appuyez sur Entrée pour installer ou mettre à niveau AutoPass. Si vous ne souhaitez pas installer ou mettre à niveau AutoPass, entrez n.

   Lorsque la version A.05.10, A.05.50 ou A.06.00 de Data Protector est détectée, la procédure de mise à niveau démarre automatiquement. Si vous souhaitez effectuer une installation propre (la version précédente de la base de données sera effacée), désinstallez l'ancienne version puis redémarrez l'installation.

   Pour plus de détails sur la gestion des licences, reportez-vous aux sections "Installation d'un Gestionnaire de cellule UNIX" à la page 44 et "Installation des Serveurs d'installation pour UNIX" à la page 62.

4. Si vous réalisez une mise à niveau de Data Protector A.05.10 et que la cellule contient des clients Windows, un message vous informera que la conversion des noms de fichier de la base de données IDB va être réalisée. La conversion de la base de données IDB est nécessaire pour la gestion correcte des noms de fichiers comportant des caractères internationaux. Pour plus de détails, reportez-vous à la section "Conversion des noms de fichiers de la base de données IDB" à la page 277.

Dès que la procédure est terminée, vous pouvez utiliser les fonctionnalités de Data Protector.

Pour obtenir la description de la commande `omnisetup.sh`, consultez le fichier `LISEZMOI` se trouvant dans le répertoire *point_de_montage*`/LOCAL_INSTALL` sur le DVD-ROM ou la *Guide de rfrence de l'interface de ligne de commande HP*

Data Protector se trouvant dans le répertoire `point_de_montage/DOCS/C/MAN` sur le DVD-ROM.

Etape suivante

Une fois que les systèmes du Gestionnaire de cellule et du Serveur d'installation ont été mis à niveau, vérifiez si vous devez appliquer des modifications à vos fichiers de configuration. Reportez-vous à la section "Vérification des changements de configuration" à la page 261.

Sous HP-UX 11.23 et 11.31 (Itanium) et sous SuSE Linux (x86-64), la taille maximale des fichiers de base de données peut dépasser la taille maximale par défaut de 2 Go. Par conséquent, lors d'une mise à niveau vers Data Protector A.06.10, un message d'avertissement s'affiche pour inviter à régler la taille maximale des fichiers de base de données. Vous devez effectuer cette opération après la mise à niveau, car elle peut prendre beaucoup de temps, selon la taille de la base de données. Reportez-vous à la section "La taille maximale des fichiers de base de données dépasse 2 Go" à la page .

Mise à niveau d'un Serveur d'installation

Le Serveur d'installation HP-UX, Solaris ou Linux est mis à niveau automatiquement lorsque la commande `omnisetup.sh` est exécutée.

Sous HP-UX, cette commande met automatiquement à niveau le package existant à l'aide de l'utilitaire `swinstall`. Sous Solaris, cette commande supprime l'ensemble des packages existants à l'aide de l'utilitaire `pkgrm` et installe les nouveaux packages à l'aide de l'utilitaire `pkgadd`. Sous Linux, cette commande met automatiquement à niveau le package existant à l'aide de l'utilitaire `rpm`.

Si le Serveur d'installation est installé avec des composants client, il sera supprimé par la commande `omnisetup.sh`. Dans ce cas, installez un nouveau dépôt du Serveur d'installation au moyen de la commande `omnisetup.sh -IS`, puis réimportez le Serveur d'installation mis à niveau. Pour plus de détails, reportez-vous à la section "Importation d'un serveur d'installation dans une cellule" à la page 207.

IMPORTANT :

Vous ne pouvez pas mettre à niveau le Serveur d'installation si vous n'avez pas au préalable mis à niveau le Gestionnaire de cellule.

Procédure de mise à niveau

Procédez comme suit pour mettre à niveau le Serveur d'installation HP-UX, Solaris ou Linux vers Data Protector A.06.10 :

1. Insérez et montez le DVD-ROM d'installation UNIX sur un point de montage.

   Par exemple :

   ```
   mkdir /dvdrom mount /dev/c0d0t0 /dvdrom
   ```

   Si vous souhaitez installer Data Protector depuis un dépôt sur le disque, procédez comme suit :

   - Pour copier les répertoires `DP_DEPOT` et `LOCAL_INSTALL` (où se trouvent les fichiers d'installation) sur votre disque local, procédez comme suit :
     `mkdir répertoire`
     `cp -r /dvdrom/rép_plateforme/DP_DEPOT répertoire`
     `cp -r /dvdrom/rép_plateforme/AUTOPASS répertoire`
     `cp -r /dvdrom/LOCAL_INSTALL répertoire`
     Où *`rép_platform`* dépend du système d'exploitation et de la plate-forme du processeur sur lesquels vous mettez à niveau Data Protector:

`hpux_ia`	HP-UX sur systèmes IA-64
`hpux_pa`	HP-UX sur systèmes PA-RISC
`solaris`	Systèmes Solaris
`linux`	Systèmes Linux

   - Pour copier l'ensemble du DVD-ROM sur votre disque local, exécutez la commande :
     `cp -r /dvdrom rép_image_dvd`

2. Exécutez la commande `omnisetup.sh`.

   Pour lancer cette commande à partir du DVD-ROM, exécutez :

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

   Pour lancer l'installation à partir du disque, effectuez l'une des étapes suivantes :

   - Si vous avez copié les répertoires `DP_DEPOT` et `LOCAL_INSTALL` sur votre disque local sous *`répertoire`*, allez sur le répertoire qui contient le fichier `omnisetup.sh` et exécutez la commande suivante :
     `cd répertoire/LOCAL_INSTALL ./omnisetup.sh`
   - Si vous avez copié l'intégralité du DVD-ROM dans *`rép_image_dvd`*, exécutez la commande `omnisetup.sh` sans paramètres :
     `cd rép_dvd_image/LOCAL_INSTALL ./omnisetup.sh`

Dès que la procédure est terminée, vous pouvez utiliser les fonctionnalités de Data Protector.

Pour obtenir la description de la commande `omnisetup.sh`, consultez le fichier `LISEZMOI` se trouvant dans le répertoire *`point_de_montage`*`/LOCAL_INSTALL` sur le DVD-ROM ou la *Guide de rfrence de l'interface de ligne de commande HP Data Protector* se trouvant dans le répertoire *`point_de_montage`*`/DOCS/C/MAN` sur le DVD-ROM.

Etape suivante

Une fois que le système du Serveur d'installation a été mis à niveau, vérifiez si vous devez appliquer des modifications à vos fichiers de configuration. Reportez-vous à la section "Vérification des changements de configuration" à la page 261.

Mise à niveau du Gestionnaire de cellule et du Serveur d'installation Windows

Lorsque la version précédente de Data Protector est détectée, le jeu de composants pris en compte par le système d'exploitation est le même que celui qui est installé (sans les composants obsolètes). Le jeu de packages existant est supprimé et le nouveau jeu de packages est installé comme s'il s'agissait d'une nouvelle installation (propre).

Le Serveur d'installation Windows est mis à niveau automatiquement pendant la procédure de mise à niveau s'il est installé sur le même système que le Gestionnaire de cellule. L'ancien dépôt du Serveur d'installation est supprimé et, si le composant `Serveur d'installation` est sélectionné pendant l'installation, le nouveau dépôt du Serveur d'installation est copié à sa place.

Si le Serveur d'installation est installé parallèlement au client Data Protector, et si ce client est mis à niveau à distance (à l'aide de l'interface graphique utilisateur Data Protector), le Serveur d'installation est lui aussi mis à niveau.

IMPORTANT :

Réimportez le Serveur d'installation mis à niveau une fois la procédure d'installation terminée. Pour plus de détails, reportez-vous à la section "Importation d'un serveur d'installation dans une cellule" à la page 207.

REMARQUE :

Si vous souhaitez mettre à niveau votre système d'exploitation de Windows NT vers une nouvelle version de Windows, vous devez dans un premier temps mettre à niveau le système d'exploitation, puis la version précédente du produit vers Data Protector A.06.10. Pour plus de détails, reportez-vous à la section "Mise à niveau de Windows NT vers une nouvelle version de Windows" à la page 288.

Microsoft Cluster Server

La procédure de mise à niveau du Gestionnaire de cellule fonctionnant dans un environnement Microsoft Cluster Server est différente de celle d'un Gestionnaire de cellule non configuré pour être utilisé avec Microsoft Cluster Server. La procédure détaillée correspondante est décrite à la section "Mise à niveau du Gestionnaire de cellule configuré sur Microsoft Cluster Server" à la page 302.

Procédure de mise à niveau

Procédez comme suit pour mettre à niveau le Gestionnaire de cellule et le Serveur d'installation Windows vers Data Protector A.06.10 :

1. Insérez le DVD-ROM d'installation Windows et exécutez la commande `Windows_other`. Le processus d'installation détecte l'ancienne installation de Data Protector. Cliquez sur Suivant pour démarrer la mise à niveau.
2. Dans la page Sélection des composants, les composants précédemment installés sur le système sont sélectionnés. Notez que vous pouvez modifier le jeu de composants en sélectionnant ou en désélectionnant des composants supplémentaires. Pour obtenir une description des composants sélectionnés, reportez-vous à l'étape suivante de l'assistant. Cliquez sur Suivant.
3. *Windows XP et Windows Server 2003 SP1 uniquement* : si Data Protector détecte le pare-feu Windows sur votre système, la page Configuration du pare-feu Windows est affichée. Le programme d'installation de Data Protector enregistrera tous les exécutables Data Protector nécessaires. Par défaut, l'option `Permettre initialement aux nouveaux fichiers binaires Data Protector enregistrés d'ouvrir des ports le cas échéant` est sélectionnée. Si vous ne souhaitez pas activer Data Protector pour les ports ouverts, désélectionnez l'option. Toutefois, notez que les exécutables doivent être activés pour que Data Protector fonctionne correctement.

   Cliquez sur Suivant.
4. La liste des composants sélectionnés s'affiche. Cliquez sur Installer pour effectuer la mise à niveau.

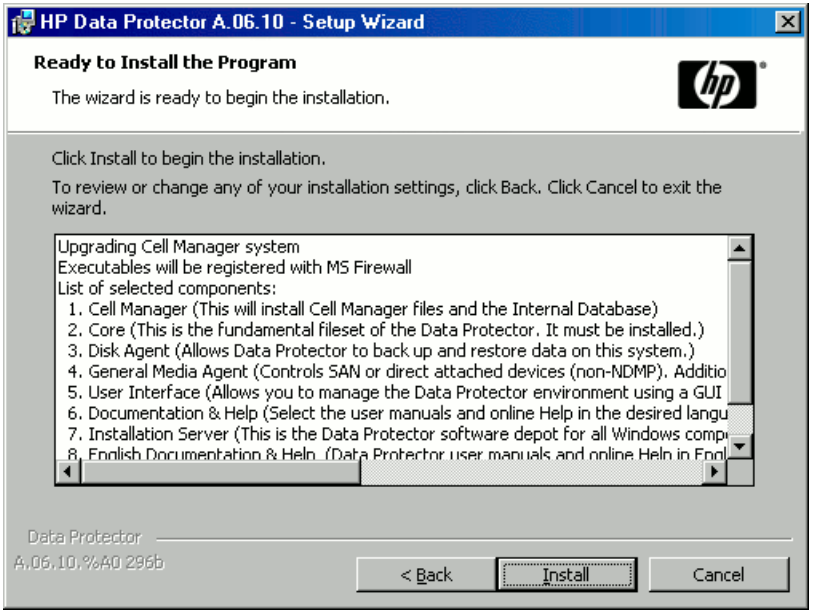

Figure 43 - Page de résumé des composants sélectionnés

5. La page d'état de l'installation s'affiche. Cliquez sur Suivant.

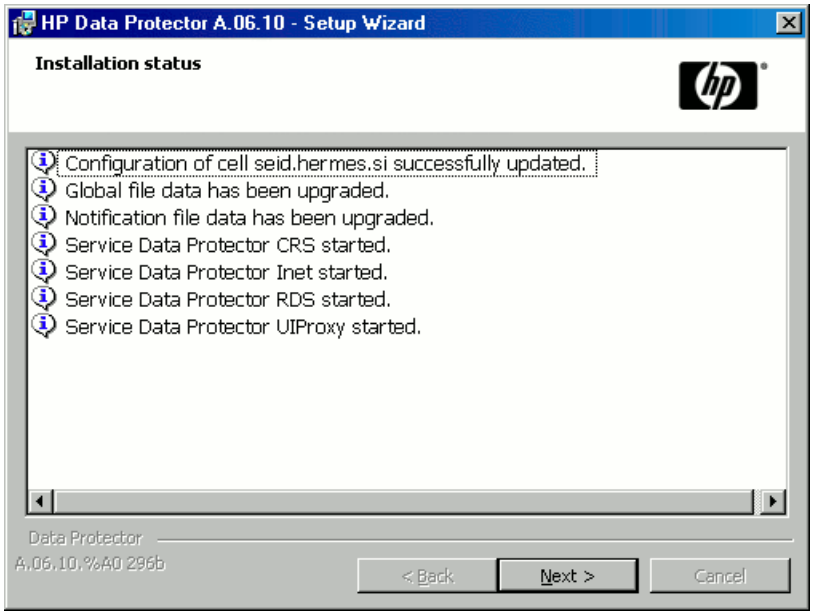

Figure 44 - Page d'état de l'installation

6. Si des clients UNIX sont présents dans la cellule, la page Conversion de l'IDB s'affiche. Reportez-vous à la section "Conversion des noms de fichiers de la base de données IDB" à la page 277.

7. Cette étape est effectuée uniquement pour une mise à niveau du Gestionnaire de cellule. Si le Serveur d'installation est installé sur un client autre que le Gestionnaire de cellule mis à niveau, cette étape n'apparaît pas.

   L'assistant d'installation vous permet d'installer ou de mettre à niveau l'utilitaire HP Auto Pass si vous souhaitez télécharger et installer les mots de passe correspondant aux licences achetées directement via Internet à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus d'informations sur l'utilitaire AutoPass, reportez-vous à la section "Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP AutoPass" à la page 322.

   Par défaut, l'option Start AutoPass installation (Démarrer l'installation d'AutoPass) ou Upgrade AutoPass installation (Mettre à niveau l'installation d'AutoPass) est sélectionnée. L'installation de l'utilitaire HP AutoPass est recommandée. Si vous ne souhaitez pas installer ou mettre à niveau AutoPass, désélectionnez cette option.

   Pour commencer à utiliser Data Protector immédiatement après son installation, sélectionnez Start the Data Protector Manager GUI (Lancer l'interface graphique du gestionnaire Data Protector).

   Pour consulter les *Références, notes de publication et annonces produits HP Data Protector*, sélectionnez Ouvrir les annonces sur les produits.

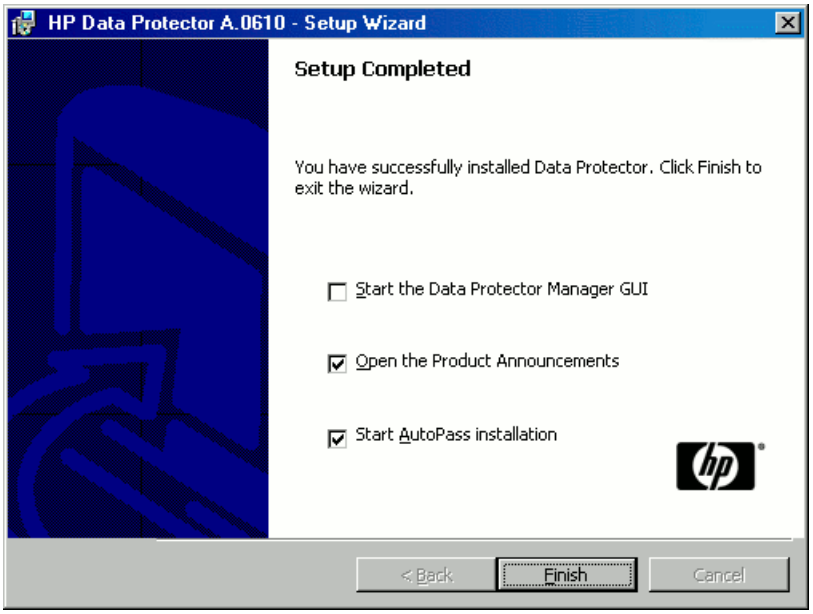

Figure 45 - Sélection d'AutoPass pour l'installation

8. Cliquez sur Terminer.

Dès que la procédure est terminée, vous pouvez utiliser les fonctionnalités de Data Protector.

Etape suivante

Après la mise à niveau des systèmes du Gestionnaire de cellule et du Serveur d'installation :

- La base de données IDB Data Protector sera convertie si des clients UNIX se trouvent dans la cellule, afin de permettre la gestion correcte des caractères non-ASCII dans les noms de fichiers de Data Protector. Pour plus d'informations sur la conversion de l'IDB, reportez-vous à la section "Conversion des noms de fichiers de la base de données IDB" à la page 277.
- Vérifiez si vous devez appliquer des modifications à vos fichiers de configuration. Reportez-vous à la section "Vérification des changements de configuration" à la page 261.

Vérification des changements de configuration

Fichier d'options globales

Pendant la mise à niveau, le contenu de l'*ancien* fichier d'options globales, qui se trouve dans le répertoire `/etc/opt/omni/server/options` sur le Gestionnaire de cellule UNIX ou dans le répertoire *`répertoire_Data_Protector`*`\Config\server\Options` sous directory sur le Gestionnaire de cellule Windows, est fusionné avec le contenu du *nouveau* fichier d'options globales (par défaut) sur le Gestionnaire de cellule :

- `/opt/omni/newconfig/etc/opt/omni/server/options` - Gestionnaire de cellule UNIX
- *`répertoire_Data_Protector`*`\NewConfig\Server\Options` - Gestionnaire de cellule Windows

Le fichier *fusionné*, nommé `global`, se trouve dans le même répertoire que l'ancien, dans le répertoire `/etc/opt/omni/server/options` sur le Gestionnaire de cellule UNIX, ou dans le répertoire *`répertoire_Data_Protector`*`\Config\server\Options` sur le Gestionnaire de cellule Windows, et est utilisé par la version mise à niveau du produit. L'*ancien* fichier d'options globales est renommé en `global.1`, `global.2`, etc., selon le nombre de mises à niveau réalisées.

Les faits suivants s'appliquent après la création du fichier fusionné :

- Les variables du fichier d'options globales qui étaient actives (non mises en commentaires) dans l'ancien fichier restent actives dans le fichier fusionné. Le commentaire suivant, indiquant que la valeur de la variable a été copiée à partir de l'ancien fichier, est ajouté au fichier fusionné :

```
variable=value # Data Protector A.06.10 # This value was
automatically copied from previous version.
```

- Les variables du fichier d'options globale qui ne sont plus utilisées sont mises en commentaires (rendues inactives) dans le fichier fusionné ; le commentaire suivant, qui indique que la variable n'est plus utilisée, est ajouté :

  ```
  #variable=value # Data Protector A.06.10 # This value
  is no longer in use.
  ```

- Les variables dont les valeurs ne sont plus prises en charge sont mises en commentaire (rendues inactives) dans le fichier fusionné. Le commentaire suivant, contenant un modèle (*modèle_variable*) et indiquant la valeur précédente de la variable, est inséré :

  ```
  # variable=variable_template # Data Protector A.06.10 #
  This variable cannot be transferred automatically. # The
  previous setting was: # variable=valeur
  ```

- Les commentaires ne sont pas transférés dans le nouveau fichier fusionné.

Sur les systèmes Windows, le fichier d'options globales est au format UNICODE et peut être modifié avec le Bloc-notes, par exemple. Après avoir modifié ce fichier, veillez à l'enregistrer au format UNICODE.

La description des nouvelles options figure dans le fichier d'options globales fusionné : `/etc/opt/omni/server/options/global` sur un Gestionnaire de cellule UNIX et *répertoire_Data_Protector*`\Config\server\options\global` sur un Gestionnaire de cellule Windows. Pour plus d'informations sur les options globales, reportez-vous au *Guide de dépannage HP Data Protector*.

Procédure manuelle

La liste ci-dessous récapitule les étapes à réaliser manuellement une fois que la procédure de mise à niveau est terminée :

- `Omnirc` fichier
  Après la mise à niveau des systèmes du Gestionnaire de cellule et du Serveur d'installation, vous souhaitez peut-être modifier le fichier `omnirc`. Pour obtenir des informations sur la procédure à suivre, reportez-vous à la section relative à l'utilisation du fichier Omnirc dans le *Guide de dépannage HP Data Protector*.
- Ligne de commande
  Reportez-vous à la section "Modifications de la ligne de commande après la mise à niveau vers Data Protector A.06.10" à la page 445 pour obtenir une liste des commandes qui ont été modifiées ou fournies avec des fonctionnalités étendues. Vous devez vérifier et modifier les scripts utilisant les anciennes commandes. Reportez-vous aux pages correspondantes du manuel pour un synopsis d'utilisation.
- Taille maximale par défaut par répertoire DCBF
  Les paramètres par défaut des répertoires DCBF existants ne sont pas modifiés après une mise à niveau. Seuls les nouveaux répertoires créés auront une taille maximale par de défaut de 16 Go. Pour modifier manuellement la taille maximale du répertoire DC, exécutez la commande suivante :
  `omnidbutil –modify_dcdir` *répertoire* `-maxsize` *taille_en_Mo*

Vous devez modifier les paramètres lorsque vous utilisez des unités de grande capacité (de type LTO 4, par exemple) et que vous sauvegardez plus de 10 millions de fichiers sur bande. En outre, vérifiez que le système de fichiers où résident les répertoires DC prennent en charge les fichiers volumineux.

Etape suivante

Une fois que le Gestionnaire de cellule et le Serveur d'installation sont installés et que toutes les modifications requises ont été appliquées, il est recommandé de distribuer le logiciel aux clients. Reportez-vous à la section "Mise à niveau des clients" à la page 263.

Mise à niveau des clients

Séquence de mise à niveau

Pour plus d'informations sur l'ordre dans lequel la mise à niveau du client est effectuée, reportez-vous à la section "Présentation de la mise à niveau" à la page 247.

Mise à niveau des clients à distance

Pour connaître la procédure de mise à niveau des clients à l'aide du Serveur d'installation, reportez-vous à la section "Installation distante de clients Data Protector" à la page 78. Sur les systèmes UNIX, vous devez mettre à niveau les composants déjà installés avant d'ajouter de nouveaux composants. Après l'ajout de nouveaux composants, Data Protector n'affiche pas les composants des versions précédentes. Dans ce cas, vous devez les réinstaller.

Mise à niveau des clients en local

Si le Serveur d'installation n'est pas installé sur votre réseau ou si, pour une raison quelconque, vous ne pouvez pas distribuer le logiciel Data Protector à un système client, les clients Data Protector peuvent être mis à niveau en local.

Pour mettre à niveau les clients Windows en local, reportez-vous à la section "Installation de clients Windows" à la page 87. Pour mettre à niveau les clients UNIX en local, reportez-vous à la section "Installation locale de clients UNIX" à la page 142.

Novell NetWare

Après la mise à niveau d'un client Novell NetWare, vous devez effectuer quelques étapes supplémentaires qui vous permettront de réaliser toute sauvegarde ou restauration de la base de données NDS/eDirectory. Pour plus de détails, reportez-vous à la section "Installation locale de clients Novell NetWare" à la page 126.

Clients Linux

Lors de la mise à niveau de clients Linux A.05.10 et A.05.50, les fichiers binaires et de configuration Data Protector sont déplacés de `/usr/omni` vers `/opt/omni` (fichiers

binaires) ou `/etc/opt/omni` (fichiers de configuration). Les scripts de pré-exécution et de post-exécution ne sont pas déplacés dans `/opt/omni`, mais ils sont copiés dans `/tmp/usr_omni`. Vous devez les copier manuellement dans `/opt/omni/lbin`. Les clients A.06.00 ne sont pas concernés.

Si le service `xinetd` est utilisé au lieu de `inetd`, le fichier `/etc/xinetd.d/omni` *n'est pas* remplacé et les paramètres demeurent inchangés. Pour vérifier que le service `xinetd` est exécuté, tapez la commande suivante :

```
ps -e | grep xinetd
```

Pour remplacer vos paramètres par les paramètres par défaut de Data Protector ou pour remplacer un fichier endommagé, retirez le fichier et tout composant logiciel Data Protector de l'interface graphique utilisateur de Data Protector. Le fichier `/etc/xinetd.d/omni` est alors installé avec les paramètres par défaut.

IMPORTANT :

Le remplacement du fichier `/etc/xinetd.d/omni` entraîne la perte de vos modifications. Si vous souhaitez conserver vos modifications, créez une copie de sauvegarde et transférez les paramètres manuellement vers le nouveau fichier.

Mise à niveau du client configuré sur MC/ServiceGuard

Si vous mettez à niveau le client utilisant MC/ServiceGuard et que le composant d'intégration Data Protector à mettre à niveau est installé sur le même nœud que le Gestionnaire de cellule, mettez à niveau d'abord les nœuds physiques, puis procédez comme suit :

1. Exportez l'hôte virtuel par la commande :

   ```
   omnicc -import_host nom_hôte_virtuel
   ```

2. Réimportez l'hôte virtuel en exécutant la commande :

   ```
   omnicc -import_host nom_hôte_virtuel -virtual
   ```

Mise à niveau de clients avec des intégrations

Si vous mettez à niveau le client Data Protector sur lequel l'intégration (par exemple Oracle, SAP R/3, Informix Server, Sybase, Microsoft Exchange Server, HP StorageWorks Disk Array XP, EMC Symmetrix, etc.) est installée, suivez les procédures décrites aux paragraphes ci-dessous :

- Pour obtenir des instructions sur la procédure de mise à niveau de l'intégration Oracle, reportez-vous à la section "Mise à niveau de l'intégration Oracle" à la page 265.
- Pour obtenir des instructions sur la procédure de mise à niveau de l'intégration SAP R/3, reportez-vous à la section "Mise à niveau de l'intégration SAP R/3" à la page 267.

- Pour obtenir des instructions sur la procédure de mise à niveau de l'intégration Informix Server, reportez-vous aux sections "Mise à niveau de l'intégration du serveur Informix sur des systèmes UNIX" à la page 268 et "Mise à niveau de l'intégration du serveur Informix sur des systèmes Windows" à la page 269.
- Pour obtenir des instructions sur la procédure de mise à niveau de l'intégration Sybase, reportez-vous aux sections "Mise à niveau de l'intégration Sybase sur des systèmes UNIX" à la page 270 et "Mise à niveau de l'intégration Sybase sur des systèmes Windows" à la page 272.
- Pour obtenir des instructions sur les procédures de mise à niveau des intégrations Microsoft Exchange, Microsoft SQL, HP StorageWorks Disk Array XP, EMC Symmetrix, etc., reportez-vous à la section "Mise à niveau des autres intégrations" à la page 276.

Mise à niveau de l'intégration Oracle

Les clients sur lesquels l'intégration Oracle est installée sont mis à niveau soit localement par la commande `omnisetup.sh -install oracle8` sur les systèmes UNIX ou `setup.exe` sur les systèmes Windows, soit à distance en chargeant l'agent d'intégration Oracle sur le client à l'aide de l'interface graphique de Data Protector. Sous UNIX, notez que si vous mettez à niveau le client qui ne réside pas sur le Gestionnaire de cellule, il n'est pas nécessaire de spécifier l'option `-install oracle8`. Dans ce cas, le programme d'installation sélectionnera sans émettre d'invite les mêmes composants que ceux déjà installés sur le système.

MML Data Protector

Après avoir mis à niveau un client UNIX, supprimez le lien symbolique renvoyant à la MML Data Protector car il n'est plus utile :

1. Accédez au répertoire *ORACLE_HOME*`/lib`.
2. Si le fichier `libobk.sl.orig` (`libobk.so.orig`) existe dans le répertoire *ORACLE_HOME*`/lib`, exécutez :

   HP–UX : `mv libobk.sl.orig libobk.sl`

   Autre système UNIX : `mv libobk.so.orig libobk.so`

   où `libobk.sl.orig` (`libobk.so.orig`) est le lien programmable Oracle tel qu'il existait avant la configuration de l'intégration.

Nouveaux modèles après la mise à niveau

Si vous effectuez une mise à niveau à partir de Data Protector A.05.10, les modèles Oracle sont remplacés par des versions plus récentes. Les nouveaux modèles se trouvent dans le répertoire suivant :

`/opt/omni/newconfig/etc/opt/omni/server/dltemplates/lists/oracle8` (sur les systèmes UNIX) ou

`répertoire_Data_Protector\NewConfig\server\dltemplates\lists\oracle8` (sur les systèmes Windows).

Pour utiliser les nouveaux modèles, copiez-les après la mise à niveau vers Data Protector A.06.10 dans le répertoire `/etc/opt/omni/server/dltemplates/lists\oracle8` (sur les systèmes UNIX) ou `répertoire_Data_Protector\Config\server\dltemplates\lists\oracle8` (sur les systèmes Windows). Si vous souhaitez conserver les anciens modèles, enregistrez-les sous un autre nom.

Configuration de la méthode ZDB

Selon que le fichier de configuration de l'instance Oracle contient ou non le paramètre *`ORACLE_DBID`*, le fichier de configuration de méthode ZDB est défini pour Data Protector A.06.10 comme suit :

- Si le fichier de configuration de l'instance Oracle contient le paramètre *`ORACLE_DBID`* (dans Data Protector A.05.10 ou A.05.50), le fichier de configuration de méthode ZDB est créé pour chaque instance de la base de données *pendant la mise à niveau*.

La méthode ZDB Oracle n'est pas modifiée pendant la mise à niveau. Pour plus d'informations sur la commutation entre les méthodes ZDB de proxy-copy et de jeu de sauvegarde, reportez-vous au *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Mise à niveau ZDB Oracle

Si vous effectuez une mise à niveau à partir de Data Protector A.05.10, les spécifications de sauvegarde ZDB Oracle sont automatiquement mises à niveau à la fin d'une procédure standard de mise à niveau de l'intégration Oracle.

Les opérations suivantes sont effectuées au cours d'une mise à niveau des spécifications de sauvegarde :

- Les paramètres `OB2DMAP` et `OB2SMB` sont ajoutés à la *première* commande RMAN `ALLOCATE CHANNEL`. Le paramètre `OB2DMAP` est configuré en fonction du nombre de canaux alloués avant la mise à niveau. Par exemple, dans le cas d'un script RMAN comprenant 4 canaux alloués, le paramètre `OB2DMAP` est défini sur 4.
- Toutes les commandes `ALLOCATE CHANNEL`, excepté la première, sont supprimées des scripts.
- Si la restauration instantanée est activée, les objets sauvegarde `TABLESPACE` ou `DATAFILES` sont changés en `DATABASE` pour permettre des sauvegardes uniquement de l'intégralité de la base de données.
- Si la méthode de sauvegarde proxy-copy a été utilisée, toutes les commandes `RELEASE CHANNEL` sont supprimées à l'exception de celle qui fait référence à la première commande `ALOCATE CHANNEL`.

Pour plus de détails, reportez-vous au *Guide d'intégration HP Data Protector pour Oracle et SAP* ou au *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Configuration d'une instance d'Oracle pour la restauration instantanée

Si les fichiers de contrôle, les catalogues de récupération ou les journaux de rétablissement archivés se trouvent dans le même groupe de volumes (si LVM est utilisé) ou dans le même volume source que les fichiers de base de données, vous devez reconfigurer l'instance d'Oracle ou définir les variables `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF et ZDB_ORA_NO_CHECKCONF_IR de la commande omnirc`. Reportez-vous au *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Mise à niveau de l'intégration SAP R/3

Les clients sur lesquels l'intégration SAP R/3 est installée sont mis à niveau soit localement par la commande `omnisetup.sh -install sap` sur les systèmes UNIX ou `setup.exe` sur les systèmes Windows, soit à distance en chargeant l'agent d'intégration SAP R/3 sur le client à l'aide de l'interface graphique de Data Protector. Sous UNIX, notez que si vous mettez à niveau le client qui ne réside pas sur le Gestionnaire de cellule, il n'est pas nécessaire de spécifier l'option `-install sap`. Dans ce cas, le programme d'installation sélectionnera sans émettre d'invite les mêmes composants que ceux déjà installés sur le système.

MML Data Protector

Après avoir mis à niveau un client UNIX SAP R/3, supprimez le lien symbolique renvoyant à la MML Data Protector car il n'est plus utile. Pour plus de détails, reportez-vous à la section "MML Data Protector" à la page 265.

Paramètre de configuration ORA_NLS_CHARACTERSET

Si vous mettez à niveau un client SAP R/3 Data Protector A.05.10 ou A.05.50 vers Data Protector A.06.10, définissez le paramètre `ORA_NLS_CHARACTERSET` Data Protector avec le codage utilisé par la base de données Oracle, pour chaque instance SAP R/3 configurée sur ce client. Procédez de l'une des manières suivantes :

- Au moyen de l'interface graphique ou de l'interface de ligne de commande de Data Protector, reconfigurez l'instance SAP R/3 en indiquant les mêmes paramètres de configuration. La reconfiguration met automatiquement à jour le fichier de configuration SAP R/3 avec le paramètre requis.
  Pour plus d'informations, reportez-vous au *Guide d'intégration HP Data Protector pour Oracle et SAP*.
- Au moyen de la commande `util_cmd` de Data Protector, ajoutez manuellement le paramètre au fichier de configuration :
  `util_cmd -putopt SAP` *`instance_SAP`* `ORA_NLS_CHARACTERSET '`*`codage_Oracle`*`'`

Exemple :
```
util_cmd -putopt SAP ICE ORA_NLS_CHARACTERSET 'US7ASCII'
```

Sessions ZDB compatibles SAP

Selon les normes SAP, il est recommandé, lors des sessions ZDB, de démarrer BRBACKUP sur le système de sauvegarde (sessions ZDB compatibles SAP). Data Protector A.06.10 permet de respecter ces normes. Configurez d'abord le système de sauvegarde selon les instructions fournies dans le guide SAP pour Oracle (sauvegarde split mirror, configuration du logiciel), puis installez le composant Data Protector `SAP R/3 Integration` sur le système de sauvegarde. Pour finir, configurez Data Protector pour des sessions ZDB compatibles SAP comme décrit dans le *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Configuration d'une instance d'Oracle pour la restauration instantanée

Si les fichiers de contrôle, les catalogues de récupération ou les journaux de rétablissement archivés se trouvent dans le même groupe de volumes (si LVM est utilisé) ou dans le même volume source que les fichiers de base de données, vous pouvez :

- Reconfigurer l'instance Oracle.
- Définir les variables `omnirc ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF et ZDB_ORA_NO_CHECKCONF_IR`.
- Configurer Data Protector pour démarrer BRBACKUP sur le système de sauvegarde (sessions ZDB compatibles SAP).

Pour plus d'informations, reportez-vous au *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Mise à niveau de l'intégration du serveur Informix sur des systèmes UNIX

Lorsque vous mettez à niveau l'intégration du serveur Informix de Data Protector A.05.10 vers Data Protector A.06.10, il existe trois procédures de mise à niveau, en fonction de l'environnement :

Procédure 1

Si le client du serveur Informix *ne se trouve pas* sur le même système que le Gestionnaire de cellule et s'il *n'est pas configuré* comme client Data Protector compatible cluster, les paramètres de configuration du serveur Informix Data Protector sont automatiquement déplacés d'un client du serveur Informix Data Protector vers le Gestionnaire de cellule au cours de la mise à niveau. Aucune reconfiguration des bases de données du serveur Informix n'est nécessaire après la mise à niveau.

Mettez le client à niveau, soit localement par la commande `omnisetup.sh`, soit à distance en chargeant l'agent d'intégration du serveur Informix sur le client avec l'interface graphique de Data Protector.

Procédure 2

Si le client du serveur Informix *ne se trouve pas* sur le même système que le Gestionnaire de cellule et s'il *est configuré* comme client Data Protector compatible cluster, les paramètres de configuration du serveur Informix Data Protector sont automatiquement déplacés du client du serveur Informix Data Protector vers le Gestionnaire de cellule au cours de la mise à niveau. Après la mise à niveau, les bases de données du serveur Informix doivent être reconfigurées.

1. Mettez le client à niveau, soit localement par la commande `omnisetup.sh`, soit à distance en chargeant l'agent d'intégration du serveur Informix sur le client avec l'interface graphique de Data Protector.
2. Configurez les bases de données du serveur Informix à l'aide de l'interface graphique ou de l'interface de ligne de commande Data Protector selon les indications du *Guide d'intégration HP Data Protector*.

   Configurez les bases de données du serveur Informix à l'aide du nom d'hôte virtuel du serveur Informix.

Procédure 3

Si le client du serveur Informix *se trouve* sur le même système qu'un *Gestionnaire de cellule compatible cluster et s'il est configuré ou non* comme client Data Protector compatible cluster, les paramètres de configuration du serveur Informix Data Protector ne sont pas automatiquement déplacés du client du serveur Informix Data Protector vers le Gestionnaire de cellule pendant la mise à niveau. Après la mise à niveau, les bases de données du serveur Informix doivent être reconfigurées.

1. Mettez le client à niveau, soit localement par la commande `omnisetup.sh`, soit à distance en chargeant l'agent d'intégration du serveur Informix sur le client avec l'interface graphique de Data Protector.
2. Configurez les bases de données du serveur Informix à l'aide de l'interface graphique ou de l'interface de ligne de commande Data Protector selon les indications du *Guide d'intégration HP Data Protector*.

Mise à niveau de l'intégration du serveur Informix sur des systèmes Windows

Lorsque vous mettez à niveau l'intégration du serveur Informix de Data Protector A.05.10 vers Data Protector A.06.10, il existe trois procédures de mise à niveau, en fonction de l'environnement :

Procédure 1

Si le client du serveur Informix *ne se trouve pas* sur le même système que le Gestionnaire de cellule et s'il *n'est pas configuré* comme client Data Protector compatible cluster, les paramètres de configuration du serveur Informix Data Protector sont automatiquement déplacés du client du serveur Informix Data Protector vers le Gestionnaire de cellule au

cours de la mise à niveau. Aucune reconfiguration des bases de données du serveur Informix n'est nécessaire après la mise à niveau.

Mettez le client à niveau, soit localement par la commande setup.exe, soit à distance en chargeant l'agent d'intégration du serveur Informix sur le client avec l'interface graphique de Data Protector.

Procédure 2

Si le client du serveur Informix *ne se trouve pas* sur le même système que le Gestionnaire de cellule et s'il *est configuré* comme client Data Protector compatible cluster, les paramètres de configuration du serveur Informix Data Protector sont automatiquement déplacés du client du serveur Informix Data Protector vers le Gestionnaire de cellule au cours de la mise à niveau. Après la mise à niveau, les bases de données du serveur Informix doivent être reconfigurées.

1. Mettez le client à niveau, soit localement par la commande setup.exe, soit à distance en chargeant l'agent d'intégration du serveur Informix sur le client avec l'interface graphique de Data Protector.
2. Configurez les bases de données du serveur Informix à l'aide de l'interface graphique ou de l'interface de ligne de commande Data Protector selon les indications du *Guide d'intégration HP Data Protector*.

   Configurez les bases de données du serveur Informix à l'aide du nom d'hôte virtuel du serveur Informix.

Procédure 3

Si le client du serveur Informix *se trouve* sur le même système qu'un *Gestionnaire de cellule compatible cluster et s'il est configuré ou non* comme client Data Protector compatible cluster, les paramètres de configuration du serveur Informix Data Protector ne sont pas automatiquement déplacés du client du serveur Informix Data Protector vers le Gestionnaire de cellule pendant la mise à niveau. Après la mise à niveau, les bases de données du serveur Informix doivent être reconfigurées.

1. Mettez le client à niveau, soit localement par la commande setup.exe, soit à distance en chargeant l'agent d'intégration du serveur Informix sur le client avec l'interface graphique de Data Protector.
2. Configurez les bases de données du serveur Informix à l'aide de l'interface graphique ou de l'interface de ligne de commande Data Protector selon les indications du *Guide d'intégration HP Data Protector*.

Mise à niveau de l'intégration Sybase sur des systèmes UNIX

Lorsque vous mettez à niveau l'intégration Sybase de Data Protector A.05.10 vers Data Protector A.06.10, il existe trois procédures de mise à niveau, en fonction de l'environnement :

Procédure 1

Si le client Sybase *ne se trouve pas* sur le même système que le Gestionnaire de cellule et qu'il *n'est pas configuré* comme client Data Protector compatible cluster, les paramètres de configuration Sybase Data Protector sont automatiquement déplacés du client Sybase Data Protector vers le Gestionnaire de cellule au cours de la mise à niveau. Aucune reconfiguration du serveur Sybase n'est nécessaire après la mise à niveau.

Mettez le client à niveau, soit localement par la commande `omnisetup.sh`, soit à distance en chargeant l'agent d'intégration Sybase sur le client avec l'interface graphique de Data Protector.

Procédure 2

Si le client Sybase *ne se trouve pas* sur le même système que le Gestionnaire de cellule et qu'il *est configuré* comme client Data Protector compatible cluster, les paramètres de configuration Sybase Data Protector sont automatiquement déplacés du client Sybase Data Protector vers le Gestionnaire de cellule au cours de la mise à niveau. Après la mise à niveau, le serveur Sybase doit être reconfiguré.

1. Mettez le client à niveau, soit localement par la commande omnisetup.sh, soit à distance en chargeant l'agent d'intégration Sybase sur le client avec l'interface graphique de Data Protector.
2. Configurez le client Sybase au moyen de l'interface graphique ou de l'interface de ligne de commande de Data Protector comme expliqué dans le *Guide d'intégration HP Data Protector*.

   Configurez le serveur Sybase à l'aide du nom d'hôte virtuel du serveur Sybase.

Procédure 3

Si le client Sybase *se trouve* sur le même système qu'un *Gestionnaire de cellule compatible cluster et s'il est configuré ou non* comme client Data Protector compatible cluster, les paramètres de configuration du serveur Sybase Data Protector ne sont pas automatiquement déplacés du client Sybase Data Protector vers le Gestionnaire de cellule pendant la mise à niveau. Après la mise à niveau, le serveur Sybase doit être reconfiguré.

1. Mettez le client à niveau, soit localement par la commande omnisetup.sh, soit à distance en chargeant l'agent d'intégration Sybase sur le client avec l'interface graphique de Data Protector.
2. Configurez le serveur Sybase au moyen de l'interface graphique ou de l'interface de ligne de commande de Data Protector comme expliqué dans le *Guide d'intégration HP Data Protector*.

   Si le serveur Sybase est configuré comme client Data Protector compatible cluster, configurez-le en utilisant le nom d'hôte virtuel du serveur en ligne.

   Si le serveur Sybase n'est pas configuré comme client Data Protector compatible cluster, configurez-le en utilisant le nom d'hôte du serveur Sybase.

Mise à niveau de l'intégration Sybase sur des systèmes Windows

Lorsque vous mettez à niveau l'intégration Sybase de Data Protector A.05.10 vers Data Protector A.06.10, il existe trois procédures de mise à niveau, en fonction de l'environnement :

Procédure 1

Si le client Sybase *ne se trouve pas* sur le même système que le Gestionnaire de cellule et qu'il *n'est pas configuré* comme client Data Protector compatible cluster, les paramètres de configuration Sybase Data Protector sont automatiquement déplacés du client Sybase Data Protector vers le Gestionnaire de cellule au cours de la mise à niveau. Aucune reconfiguration du serveur Sybase n'est nécessaire après la mise à niveau.

Mettez le client à niveau, soit localement par la commande setup.exe, soit à distance en chargeant l'agent d'intégration Sybase sur le client avec l'interface graphique de Data Protector.

Procédure 2

Si le client Sybase *ne se trouve pas* sur le même système que le Gestionnaire de cellule et qu'il *est configuré* comme client Data Protector compatible cluster, les paramètres de configuration Sybase Data Protector sont automatiquement déplacés du client Sybase Data Protector vers le Gestionnaire de cellule au cours de la mise à niveau. Après la mise à niveau, le serveur Sybase doit être reconfiguré.

1. Mettez le client à niveau, soit localement par la commande setup.exe, soit à distance en chargeant l'agent d'intégration Sybase sur le client avec l'interface graphique de Data Protector.
2. Configurez le client Sybase au moyen de l'interface graphique ou de l'interface de ligne de commande de Data Protector comme expliqué dans le *Guide d'intégration HP Data Protector*.

   Configurez le serveur Sybase à l'aide du nom d'hôte virtuel du serveur SQL Sybase.

Procédure 3

Si le client Sybase *se trouve* sur le même système qu'un *Gestionnaire de cellule compatible cluster et s'il est configuré ou non* comme client Data Protector compatible cluster, les paramètres de configuration du serveur Sybase Data Protector ne sont pas automatiquement déplacés du client Sybase Data Protector vers le Gestionnaire de cellule pendant la mise à niveau. Après la mise à niveau, le serveur Sybase doit être reconfiguré.

1. Mettez le client à niveau, soit localement par la commande `setup.exe`, soit à distance en chargeant l'agent d'intégration Sybase sur le client avec l'interface graphique de Data Protector.

2. Configurez le client Sybase au moyen de l'interface graphique ou de l'interface de ligne de commande de Data Protector comme expliqué dans le *Guide d'intégration HP Data Protector*.

   Si le serveur Sybase est configuré comme client Data Protector compatible cluster, configurez-le en utilisant le nom d'hôte virtuel du serveur en ligne.

   Si le serveur Sybase n'est pas configuré comme client Data Protector compatible cluster, configurez-le en utilisant le nom d'hôte du serveur Sybase.

Mise à niveau de l'intégration de HP StorageWorks EVA

La mise à niveau de l'intégration de HP StorageWorks EVA s'effectue à partir de l'Agent HP StorageWorks EVA (hérité) vers l'Agent HP StorageWorks EVA SMI-S. Cette mise à niveau est nécessaire en raison du caractère obsolète de l'agent EVA (hérité).

Si la procédure de mise à niveau s'est déroulée correctement, les résultats sont les suivants :

- Mise à niveau des spécifications de sauvegarde créées par l'Agent EVA (hérité)
- Transfert des informations sur les sessions de sauvegarde de l'EVADB vers la SMISDB afin de permettre leur restauration par l'Agent SMI-S
- Transfert des règles de groupes de disques et de connexion définies pour l'Agent EVA (existant) vers la SMISDB

Pour obtenir des informations détaillées sur les versions des produits associés prises en charge, ainsi qu'une liste des plates-formes sur lesquelles l'Agent SMI-S est pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.

Configuration requise

- Veillez à satisfaire les conditions minimales requises pour les systèmes d'exploitation sur lesquels l'agent SMI-S est pris en charge.
- Aucune sauvegarde EVA ne doit être en cours d'exécution. La procédure de mise à niveau peut faire échouer la sauvegarde ; dans ce cas, aucune information de session ne s'affichera dans la SMIDB et il sera impossible d'effectuer une restauration à partir de cette session.
- Ne lancez la mise à niveau d'un agent qu'une fois la mise à niveau du Gestionnaire de cellule terminée.

Procédure de mise à niveau

Pour effectuer une mise à niveau de l'Agent HP StorageWorks EVA (hérité) vers l'Agent HP StorageWorks EVA SMI-S, suivez les étapes décrites ci-dessous :

1. Sur le Gestionnaire de cellule, exécutez la commande `upgrade_cm_from_evaa` afin de mettre à niveau toutes les entrées EVADB vers les entrées SMISDB. Exécutez cette commande seulement lorsque la mise à niveau du Gestionnaire de cellule est terminée.

   Les informations suivantes sont transférées :

   - Spécifications de sauvegarde et sessions de sauvegarde (répliques) créées par l'Agent EVA (hérité)
   - Entrées de connexion associées au système de gestion EVA

   Prenez en compte les points suivants :

Connexion

- Si une entrée de connexion est déjà présente dans la SMISDB, aucune nouvelle entrée n'est créée pour ce système de gestion.
- Les nom d'utilisateur et mot de passe de connexion sont supposés être les mêmes pour CV EVA et un fournisseur SMI-S.
- L'entrée de connexion SMISDB utilisera toujours le port 5988.

Règles de groupes de disques

- S'il existe déjà une règle pour un groupe de disques donné dans la SMISDB, aucune mise à jour n'est effectuée.
- Toutes les règles de groupes de disques définies pour l'Agent EVA (hérité) sont ajoutées à la suite des règles de groupes de disques SMISDB existantes.

Pour plus d'informations su la commande `upgrade_cm_from_evaa`, reportez-vous au *Guide de rfrence de l'interface de ligne de commande HP Data Protector*.

2. Sur le système d'application, exécutez la commande `omnisetup.sh -install smisa` sur les systèmes UNIX ou la commande `setup.exe` sur les systèmes Windows si vous effectuez une mise à niveau locale. Si vous effectuez une mise à niveau à distance, chargez (push) l'Agent EVA SMI-S sur le client à l'aide de l'assistant `Ajouter composants` de l'interface graphique et sélectionnez `Agent HP StorageWorks EVA SMI-S`.

   Ce script de pré-exécution vérifie si le package EVAA se trouve sur le système. Si le package est détecté, les informations relatives à ce dernier sont supprimées du Gestionnaire de cellule.

   Parallèlement à la désinstallation du package EVAA, les informations relatives aux sessions de sauvegarde EVA (répliques) créées par l'Agent EVA (hérité) sont transférées de l'EVADB à la SMISDB. Cela signifie qu'après la mise à niveau, vous serez en mesure de restaurer les sessions de sauvegarde créées par l'Agent EVA (hérité) à l'aide de l'Agent SMI-S.

3. Une fois le système d'application mis à niveau, vous devez également mettre à niveau le système de sauvegarde. Les spécifications de sauvegardes planifiées ne fonctionneront pas tant que les systèmes d'application et les systèmes de sauvegarde n'auront pas été mis à niveau.
4. Vérifiez manuellement le fichier `omnirc` afin de vous assurer que les variables `omnirc` ont été correctement mises à niveau.

Mise à niveau du module de récupération automatique après sinistre

Le module de récupération automatique après sinistre (récupération après sinistre automatisée avancée et récupération automatique après sinistre) de Data Protector A.06.10 n'est pas entièrement compatible avec les anciennes versions du module (A.05.10, A.05.50 ou A.06.00 sans l'installation du correctif DPWIN_002700) :

- Sur des systèmes Windows 2000, les sauvegardes créées avant la mise à niveau ne peuvent pas servir à créer des images de récupération après sinistre sur des clients mis à niveau.
- L'interface graphique de Data Protector est compatible avec l'ancien module de récupération après sinistre et permet de créer des images de récupération après sinistre sur des clients Windows 2000 avec l'ancien module. Par exemple, vous pouvez gérer à l'aide de la nouvelle interface graphique un système Windows 2000 avec l'ancien module de récupération après sinistre. Dans un tel cas, l'interface crée une image de récupération après sinistre à partir d'une sauvegarde créée avec l'ancien module.
- Sur les systèmes Windows 2000, vous devez ajouter le compte `DRM$ADMIN` au groupe d'utilisateurs Admin de Data Protector au lieu du compte administrateur local du client (utilisé dans Data Protector A.05.10, A.05.50 ou A.06.00 sans le correctif).

Le Tableau 10 à la page 276 répertorie toutes les combinaisons et les problèmes de compatibilité.

Tableau 10 - Compatibilité EADR et OBDR après une mise à niveau

Version du client Data Protector		Résultat
Sauvegarde	Création d'image	
A.05.10, A.05.50 ou A.06.00 (sans le correctif DPWIN_002700)	A.05.10, A.05.50 ou A.06.00 (sans le correctif DPWIN_002700)	Création d'une image
A.05.10, A.05.50 ou A.06.00 (sans le correctif DPWIN_002700)	A.06.00 (avec le correctif DPWIN_002700) ou A.06.10	Erreur
A.06.00 (avec le correctif DPWIN_002700) ou A.06.10	A.05.10, A.05.50 ou A.06.00 (sans le correctif DPWIN_002700)	Erreur
A.06.00 (avec le correctif DPWIN_002700) ou A.06.10	A.06.00 (avec le correctif DPWIN_002700) ou A.06.10	Création d'une image

Pour plus d'informations sur les modifications des procédures EADR et OBDR, voir le *Guide de récupération aprs sinistre HP Data Protector*.

Mise à niveau des autres intégrations

Si une intégration Microsoft Exchange, Microsoft SQL, HP StorageWorks Disk Array XP, EMC Symmetrix, etc. est installée sur le client Data Protector, mettez ce dernier à niveau, soit localement via la commande `omnisetup.sh -install` *`liste_composants`* sur les systèmes UNIX ou `setup.exe` sur les systèmes Windows, soit à distance avec l'interface graphique de Data Protector. Pour obtenir une liste des codes des composants Data Protector, reportez-vous à la section "Installation locale de clients UNIX" à la page 142. Notez que si vous mettez à niveau le client qui ne réside pas sur le Gestionnaire de cellule, il n'est pas nécessaire de spécifier l'option `-install` *`liste_composants`*. Dans ce cas, le programme d'installation sélectionnera sans émettre d'invite les mêmes composants que ceux déjà installés sur le système.

Mise à niveau dans un environnement MoM

Vous pouvez mettre à niveau un environnement MoM de manière séquentielle. Toutefois, gardez à l'esprit les limites suivantes :

Limites

- Après avoir effectué une mise à niveau du Gestionnaire MoM/serveur CMMDB, il n'est pas possible de procéder à la *restauration* d'un système de fichiers ou d'une intégration Data Protector A.05.10 ou A.05.50 via l'interface graphique utilisateur MoMData Protector A.06.10. Par conséquent, utilisez l'ancienne

interface graphique utilisateur MoM pour la restauration ou mettez à niveau les clients.
Vous pouvez effectuer une *sauvegarde* de systèmes de fichiers et d'intégrations de clients Data Protector A.05.10 ou A.05.50 via l'interface graphique utilisateur MoM Data Protector A.06.10.

- Vous ne pouvez pas utiliser un format de support de fichier distribué avec vos bibliothèques de fichiers tant que tous les Gestionnaires de cellule n'ont pas été mis à niveau vers Data Protector A.06.10.

Pour mettre à niveau votre environnement MoM vers Data Protector A.06.10, procédez comme suit :

1. Mettez à niveau le Gestionnaire MoM/serveur CMMDB vers Data Protector A.06.10.

   Aucun Gestionnaire de cellule de l'environnement MoM ne doit fonctionner pendant la mise à niveau. Après la mise à niveau, le Gestionnaire MoM peut toujours fonctionner avec les anciens Gestionnaires de cellule.

2. Mettez à niveau chaque Gestionnaire de cellule client dans un environnement MoM.

   Pour connaître la procédure de mise à niveau à suivre, reportez-vous aux sections "Mise à niveau du Gestionnaire de cellule et du Serveur d'installation UNIX" à la page 251 et "Mise à niveau du Gestionnaire de cellule et du Serveur d'installation Windows" à la page 256.

3. Mettez à niveau les clients avec des périphériques configurés.

4. Mettez à niveau les clients avec des intégrations d'applications.

   Une fois que cette partie de la mise à niveau est effectuée, vous pouvez sauvegarder et restaurer les systèmes de fichiers et les intégrations via l'interface graphique utilisateur MoM Data Protector A.06.10.

Conversion des noms de fichiers de la base de données IDB

Data Protector A.05.50 et versions ultérieures présentent une amélioration dans la gestion et l'affichage des noms de fichiers créés avec des paramètres régionaux différents sur des plates-formes différentes. Ceci nécessite la conversion des noms de fichiers existants de la base de données IDB pour certaines configurations de cellule spécifiques si vous effectuez une mise à niveau à partir de Data Protector A.05.10.

La conversion des noms de fichiers de la base de données IDB doit être effectuée. Dans le cas contraire, la navigation et la sélection pour restauration des noms de fichiers contenant des caractères non-ASCII dépend de nombreux facteurs. La probabilité d'obtenir des résultats indésirables est élevée.

La conversion est réalisée :

- sur le Gestionnaire de cellule UNIX dans le cadre de la sauvegarde post-mise à niveau des clients Windows ;
- sur le Gestionnaire de cellule Windows en processus d'arrière-plan après la mise à niveau du Gestionnaire de cellule.

Si nécessaire, un message vous invitera à effectuer la conversion de la base de données IDB.

Le Tableau 11 à la page 278 (pour le Gestionnaire de cellule Windows) et le Tableau 12 à la page 279 décrivent l'impact de la conversion de noms de fichier sur le Gestionnaire de cellule si vous effectuez une mise à niveau à partir de Data Protector A.05.10.

Tableau 11 - Impact de la conversion de noms de fichier sur un Gestionnaire de cellule Windows

	Clients UNIX et autres	Clients Windows
Requiert une conversion de l'IDB	Oui[1]	Non
Sauvegarde avant la conversion, pas de mise à niveau du client	Problématique[2] Tout client comportant des caractères non ASCII dans ses spécifications de sauvegarde (arborescences, listes d'exclusion, etc.) doit être mis à niveau vers Data Protector A.06.10. Data Protector consigne tous ces clients dans le Journal d'événements Data Protector pendant la mise à niveau pour vous aider à organiser vos tâches de mise à niveau en fonction de leur priorité.	Aucun problème
Sauvegarde avant la conversion, mise à niveau du client vers la version A.06.10	Aucun problème Si un client est sauvegardé alors que la conversion est en cours et si des données IDB de ce client sont converties, la sauvegarde bascule en mode `Pas de journalisation` pour la session concernée.	Aucun problème
Affichage des fichiers à restaurer avant la conversion, sélection des noms de fichier/arborescences non ASCII à restaurer	Problématique[3] L'affichage correct (et la sélection destinée à la restauration) de caractères non ASCII dans l'interface graphique utilisateur de Data Protector est impossible tant que les noms de fichier dans l'IDB du client concerné ne sont pas convertis.	Aucun problème

	Clients UNIX et autres	Clients Windows
Sauvegarde après la conversion	Aucun problème Le client doit être mis à niveau vers Data Protector A.06.10.	Aucun problème
Affichage et restauration des fichiers après la conversion	Aucun problème Le client doit être mis à niveau vers Data Protector A.06.10.	Aucun problème
Compatibilité de l'Agent de disque (versions antérieures)[4]	Data Protector A.05.10 = Non, A.05.50 = OUI[4] .	Data ProtectorA.05.10 = OUI [4,] , A.05.50.= OUI[4]

Tableau 12 - Impact de la conversion de noms de fichier sur un Gestionnaire de cellule UNIX

	Clients UNIX et autres	Clients Windows
Requiert une conversion de l'IDB	Non	Oui[1]
Sauvegarde pendant la période de conversion, pas de mise à niveau du client	Aucun problème	Problématique[2] Tout client comportant des caractères non ASCII dans ses spécifications de sauvegarde (arborescences, listes d'exclusion, etc.) doit être mis à niveau vers Data Protector A.06.10. Data Protector consigne tous ces clients dans le Journal d'événements Data Protector pour vous aider à organiser vos tâches de mise à niveau en fonction de leur priorité.
Sauvegarde pendant la période de conversion, mise à niveau du client vers la version A.06.10	Aucun problème	Aucun problème Notez que la sauvegarde des clients Windows pendant la période de conversion est nécessaire. Les données de l'IDB de chaque client sont automatiquement converties pendant la sauvegarde du client. Vous devez réaliser une sauvegarde complète pour convertir tous les noms de fichier stockés dans l'IDB du client concerné.
Affichage des fichiers à restaurer avant la conversion, sélection des noms de fichier/arborescences non ASCII à restaurer	Aucun problème	Problématique[3] L'affichage correct (et la sélection destinée à la restauration) de caractères non ASCII dans l'interface graphique utilisateur de Data Protector est impossible tant qu'une sauvegarde complète n'aura pas été réalisée après la mise à niveau du Gestionnaire de cellule.

	Clients UNIX et autres	Clients Windows
Sauvegarde après la période de conversion	Aucun problème	Aucun problème Le client doit être mis à niveau vers Data Protector A.06.10.
Affichage et restauration des fichiers après la conversion	Aucun problème	Aucun problème Le client doit être mis à niveau vers Data Protector A.06.10.
Compatibilité de l'Agent de disque (versions antérieures)[4]	[4], A.05.10 = OUI[4], , A.05.50.= OUI[4]	Data Protector A.05.10 = Non, A.05.50 = OUI[4]

[1]Si la conversion de noms de fichier n'est pas réalisée, le nombre de noms de fichier de la partie base de données catalogue (CDB) de l'IDB augmente conformément au nombre de noms de fichier contenant des caractères non ASCII dans les fichiers sauvegardés. Les fichiers et répertoires qui requièrent d'être convertis mais qui ne l'ont pas encore été ne peuvent pas être sélectionnés pour la restauration. Le seul moyen de les restaurer consiste à restaurer une arborescence parente contenant uniquement des caractères ASCII dans un emplacement temporaire.
[2]Les restrictions ne s'appliquent pas si les noms de fichier (arborescences) de la spécification de sauvegarde ne contiennent que des caractères ASCII. Si tel est le cas, tous les fichiers et répertoires d'une arborescence sont sauvegardés et leurs noms stockés correctement dans l'IDB même si les noms de fichier (arborescences) contiennent des caractères non ASCII.
[3]Les restrictions ne s'appliquent pas si le nom de fichier (arborescence) que vous restaurez ne contient que des caractères ASCII. Dans le cas contraire, vous pouvez le restaurer en restaurant une arborescence parente contenant uniquement des caractères ASCII dans un emplacement temporaire. Tous les fichiers et répertoires de cette arborescence parente seront sauvegardés avec leurs noms de fichier d'origine (même s'ils ne s'affichent pas correctement dans l'interface graphique utilisateur de Data Protector GUI), à condition qu'ils soient restaurés sur leur plate-forme initiale.
[4]Compatibilité de l'Agent de disque du système de fichiers avec le Gestionnaire de cellule Data Protector A.06.10. La prise en charge de l'Agent de disque émanant de versions antérieures est limitée à deux semaines. Pendant ce délai, vous devez mettre à niveau tous les clients de la cellule.

Remarques

- Indépendamment des problèmes de gestion de noms de fichiers, lorsqu'un fichier est sauvegardé et restauré, la séquence d'octets d'origine composant le corps du fichier est conservée.
- Seuls les noms de fichier composés de caractères ASCII 7 bits sont entièrement pris en charge sur toutes les combinaisons de plates-formes et pour tous les composants (Gestionnaire de cellule, client, interface graphique utilisateur). Pour les noms de fichiers comportant des caractères non-ASCII, une configuration et un paramétrage spécifiques sont requis pour que les noms de fichiers soient correctement gérés.

La conversion de la base de données IDB peut demander un certain temps et monopoliser des ressources système, en fonction de la taille de la partie de l'IDB consacrée aux noms de fichier et de la configuration de la cellule. Toutefois, cela n'affecte pas la réussite de vos opérations de sauvegarde ou de restauration.

Conversion de l'IDB dans un Gestionnaire de cellule sous Windows

Introduction

Cette section s'applique aux Gestionnaires de cellule sous Windows dont la cellule contient des clients non-Windows et qui font l'objet d'une mise à niveau à partir de Data Protector A.05.10. Si vous effectuez une mise à niveau à partir de A.05.50, aucune conversion n'est requise.

La conversion de l'IDB demande un certain temps, selon sa taille et la configuration de votre cellule ; toutefois, cela n'affecte pas la réussite de vos opérations de sauvegarde ou de restauration. La conversion est effectuée en arrière-plan en une seule passe pour tous les clients non-Windows de la cellule, tandis que Data Protector reste totalement opérationnel. L'intégralité des données d'un client est convertie avant le passage aux données du client suivant. Une fois terminée, la conversion de l'IDB est complète et ne doit pas être répétée.

Si les noms de fichier ne comprennent pas de caractères non-ASCII, la conversion de l'IDB s'effectue malgré tout, mais rien ne change dans l'IDB.

La conversion de l'IDB n'affecte pas la taille de la base IDB.

Comment est effectuée la conversion de l'IDB ?

Une fois la mise à niveau de Data Protector terminée, l'assistant d'installation de Data Protector vous propose de convertir les noms de fichier dans l'IDB.

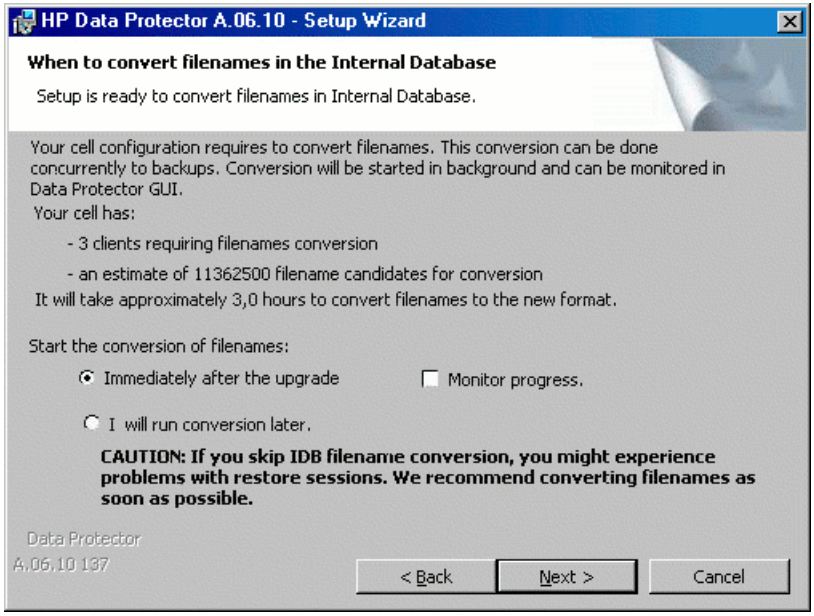

Figure 46 - Conversion de l'IDB après mise à niveau

Vous obtenez une estimation approximative de la durée de la conversion de l'IDB. Cette estimation est basée sur le nombre de clients non-Windows présents dans la cellule et sur le nombre de fichiers de ces clients qui sont stockés dans l'IDB.

Si vous remettez la conversion à une date ultérieure, vous devrez effectuer manuellement la conversion de l'IDB à l'aide de la commande `omnidbupgrade`. Pour plus de détails, reportez-vous au *Guide de rfrence de l'interface de ligne de commande HP Data Protector*.

REMARQUE :

Il est recommandé de procéder dès que possible à la conversion de l'IDB et à la mise à niveau des Agents de disque sur les clients.

Vous pouvez contrôler l'état de la conversion de l'IDB (savoir quels sont les clients dont les données ont déjà été converties) dans le menu contextuel Moniteur de l'interface utilisateur de Data Protector.

Sauvegarde pendant la conversion

Les sauvegardes pendant la conversion des noms de fichiers de l'IDB sont possibles, car la conversion s'effectue en arrière-plan, et Data Protector reste totalement opérationnel.

Si les données du client dans l'IDB sont converties pendant la sauvegarde de ce client, la sauvegarde est réalisée avec l'option `Pas de journalisation` (par conséquent,

aucune information relative aux fichiers et répertoires sauvegardés n'est consignée dans l'IDB pour ce client et cette session).

Restauration pendant la conversion

La restauration *pendant* la conversion des noms de fichiers est possible. Toutefois, seules les restaurations d'objets entiers ou de sélections de répertoires/fichiers de systèmes non-Windows, composés de caractères ASCII 7 bits, sont fiables.

Si des fichiers ou des répertoires sélectionnés pour la restauration d'un client spécifique contiennent des caractères non-ASCII (et proviennent d'une plate-forme non Windows), attendez que la conversion IDB des données de ce client soit terminée. L'Agent de disque de ce client doit être mis à niveau avant la restauration.

Sauvegarde et restauration après la conversion de l'IDB

Une fois toute la base IDB convertie et tous les Agents de disque sur tous les clients de la cellule mis à niveau vers la version A.06.10, l'opération de sauvegarde et de restauration se déroule normalement.

Conversion de l'IDB dans un Gestionnaire de cellule sous UNIX

Introduction

Cette section s'applique aux Gestionnaires de cellule sous UNIX dont la cellule contient des clients Windows et qui font l'objet d'une mise à niveau à partir de Data Protector A.05.10. Si vous effectuez une mise à niveau à partir de A.05.50, aucune conversion n'est requise.

La conversion de l'IDB demande un certain temps, selon sa taille et la configuration de votre cellule ; toutefois, cela n'affecte pas la réussite de vos opérations de sauvegarde ou de restauration. La conversion est réalisée en arrière-plan pendant les sauvegardes des clients Windows de la cellule, pendant une période spécifique. Après une sauvegarde complète de tous les objets sauvegarde de systèmes de fichiers de l'ensemble des clients Windows de la cellule, la conversion IDB est terminée et ne doit pas être effectuée à nouveau.

Par défaut, la conversion des noms de fichier dans l'IDB pendant les sauvegardes s'exécute pendant un mois, cette durée étant définie par l'option globale `ConvertFilenamesInIDBDuringBackup`. Pour plus de détails sur la modification du fichier d'options globales, consultez le *Guide de dépannage HP Data Protector*.

Impact sur les performances

La conversion des noms de fichiers de l'IDB a un impact sur les performances. Pendant la conversion (l'option globale `ConvertFilenamesInIDBDuringBackup` est activée), une sauvegarde d'un client Windows est ralentie jusqu'à ce que la première sauvegarde complète du client soit réalisée. Reportez-vous au document *Références, notes de*

publication et annonces produits HP Data Protector pour obtenir des informations détaillées.

Limites

Tenez compte des limites suivantes :

- Il est possible qu'un fichier, sauvegardé avec la version précédente de Data Protector et stocké dans l'IDB à l'aide de l'ancien codage, ait été supprimé du client avant la conversion de l'IDB. Dans ce cas, le nom de fichier n'est pas converti dans l'IDB. La même situation se produit si aucune sauvegarde n'a été effectuée au cours de la période de conversion (définie par l'option globale `ConvertFilenamesInIDBDuringBackup`). Cela rend la restauration d'un tel fichier plus difficile si des caractères non-ASCII sont utilisés dans le nom de fichier. Pour régler ce problème, reportez-vous au *Guide de dépannage HP Data Protector*.
- Pour connaître les autres restrictions, reportez-vous au Tableau 12 à la page 279.

Mise à niveau à partir de l'Edition serveur unique

La mise à niveau peut être effectuée à partir des versions suivantes :

- Des versions antérieures de l'Edition serveur unique (SSE) vers Data Protector A.06.10 Edition serveur unique. Pour plus de détails, reportez-vous à la section "Mise à niveau des versions antérieures de l'Edition serveur unique (SSE) vers Data Protector A.06.10 Edition serveur unique (SSE)" à la page 284.
- De Data Protector A.06.10 Edition serveur unique vers Data Protector A.06.10. Pour plus de détails, reportez-vous à la section "Mise à niveau de Data Protector A.06.10 Edition serveur unique (SSE) vers Data Protector A.06.10" à la page 285.

Mise à niveau des versions antérieures de l'Edition serveur unique (SSE) vers Data Protector A.06.10 Edition serveur unique (SSE)

La procédure de mise à niveau des versions antérieures de SSE vers Data Protector SSE est identique à celle des versions précédentes de Data Protector vers Data Protector A.06.10. Pour plus d'informations, reportez-vous à la section "Mise à niveau à partir de Data Protector A.05.10, A.05.50 et A.06.00" à la page 250.

Mise à niveau de Data Protector A.06.10 Edition serveur unique (SSE) vers Data Protector A.06.10

Licences

Vous devez posséder une licence pour effectuer la mise à niveau à partir de Data Protector A.06.10 Edition serveur unique vers Data Protector A.06.10. Pour plus de détails sur la gestion des licences, reportez-vous au Chapitre 5 à la page 307.

La mise à niveau de l'Edition serveur unique de Data Protector A.06.10 vers Data Protector A.06.10 est proposée dans les deux cas de figure suivants :

- L'Edition serveur unique Data Protector est installée sur un système (Gestionnaire de cellule) uniquement. Reportez-vous à la section "Mise à niveau du Gestionnaire de cellule" à la page 285.
- L'Edition serveur unique Data Protector est installée sur plusieurs systèmes et vous souhaitez fusionner ces cellules. Reportez-vous à la section "Mise à niveau de plusieurs installations" à la page 285.

REMARQUE :

Si vous souhaitez effectuer la mise à niveau d'une version précédente de l'Edition serveur unique vers une installation complète de Data Protector, commencez par mettre à niveau votre Edition serveur unique avec l'installation complète du même niveau de version. Ensuite, pour mettre à niveau cette installation complète vers Data Protector A.06.10, reportez-vous à la section "Mise à niveau à partir de Data Protector A.05.10, A.05.50 et A.06.00" à la page 250.

Mise à niveau du Gestionnaire de cellule

Pour mettre à niveau le Gestionnaire de cellule Edition serveur unique, procédez comme suit :

1. Supprimez la licence Edition serveur unique :
   - sous Windows : `del` *`répertoire_Data_Protector`*`\Config\server\Cell\lic.dat`
   - sous UNIX : `rm /etc/opt/omni/server/cell/lic.dat`
2. Démarrez l'interface graphique utilisateur de Data Protector et ajoutez un mot de passe permanent.

Mise à niveau de plusieurs installations

Pour mettre à niveau l'Edition serveur unique de Data Protector installée sur plusieurs systèmes, procédez comme suit :

1. Désignez parmi les systèmes où l'Edition serveur unique est installée celui qui doit devenir le nouveau Gestionnaire de cellule. Reportez-vous à la section "Choix du système Gestionnaire de cellule" à la page 35.
2. Mettez à niveau le Gestionnaire de cellule sélectionné comme suit :
   a. Supprimez la licence Edition serveur unique :

      `del` *`répertoire_Data_Protector`*`\Config\server\Cell\lic.dat` (sur les systèmes Windows) ou

      `rm /etc/opt/omni/server/cell/lic.dat` (sur les systèmes UNIX)

   b. Démarrez l'interface graphique utilisateur de Data Protector et ajoutez un mot de passe permanent.
3. Dans l'interface graphique, importez comme clients les autres systèmes Edition serveur unique dans le système Gestionnaire de cellule nouvellement créé.
4. Désinstallez l'Edition serveur unique Data Protector des autres systèmes. Reportez-vous à la section "Désinstallation du logiciel Data Protector" à la page 230.
5. Si nécessaire, importez les supports vers le nouveau Gestionnaire de cellule.

   Réalisez cette étape si vous envisagez de fréquentes restaurations de supports créés sur les autres systèmes Edition serveur unique. Si ces restaurations sont peu probables, vous pouvez utiliser l'option `Lister depuis support`. Dans *l'index de l'aide en ligne, recherchez : "importation, supports"* pour obtenir des informations sur l'importation de supports et sur la restauration à l'aide de l'option `Lister depuis support`.

Mise à niveau à partir de HP StorageWorks Application Recovery Manager A.06.00

Présentation

Application Recovery Manager est une solution de récupération de logiciels évolutive qui fournit des sauvegardes et des restaurations automatisées de données d'applications Exchange et SQL et qui a été conçue pour améliorer la disponibilité des applications grâce à une restauration très rapide des données.

Data Protector A.06.10 prend en charge la mise à niveau à partir de Application Recovery Manager A.06.00 et prend en charge toutes les fonctionnalités de Application Recovery Manager A.06.00. La configuration et la base de données internes sont conservées après la mise à niveau.

Limites

- Le changement de plate-forme du Gestionnaire de cellule n'est pas pris en charge dans la version A.06.10 de Data Protector. Les mises à niveau sont prises en charge uniquement sur une même plate-forme de Gestionnaire de cellule (Windows 32 bits à Windows 32 bits, ou Windows 64 bits à Windows 64 bits).

Procédure de mise à niveau

Les procédures de mise à niveau à partir de Application Recovery Manager A.06.00 et d'anciennes versions de Data Protector vers Data Protector A.06.10 sont identiques. Reportez-vous aux sections Mise à niveau du Gestionnaire de cellule et Mise à niveau des clients.

Sauvegarde de la base de données interne après la mise à niveau

Les anciennes sauvegardes de la base de données internes créées avec `dbtool.pl` ne sont pas utilisables avec Data Protector. Vous devez configurer une nouvelle spécification de sauvegarde pour sauvegarder la base de données interne et la configuration. Dans l'index de l'aide en ligne, recherchez : "IDB, configuration de sauvegardes".

Contrairement à Application Recovery Manager, la sauvegarde de la base IDB dans Data Protector utilise un lecteur de bande et se différencie par les opérations suivantes :

- les services Data Protector ne sont pas arrêtés lors de la sauvegarde comme avec `dbtool.pl`,
- la base de données VSS n'est pas sauvegardée.

Mise à niveau de spécifications de sauvegarde

Dans Application Recovery Manager, une spécification de sauvegarde ne contient aucun lecteur de bande. Une fois la mise à niveau vers Data Protector effectuée, les spécifications de sauvegarde peuvent être utilisées uniquement pour des sauvegardes ZDB sur disque. Pour utiliser la fonctionnalité de bande (ZDB sur disque + bande, ZDB sur bande), vous devez reconfigurer les spécifications de sauvegarde, en indiquant le lecteur de bande.

Changements dans l'utilisation de la commande omnib

Si aucune option n'est spécifiée, Data Protector utilise l'option ZDB sur disque + bande par défaut. Les sessions de sauvegarde Application Recovery Manager lancées à partir de l'interface de ligne de commande, à l'aide de la commande `omnib`, échoueront donc du fait de l'absence de lecteurs de bande. Pour conserver vos spécifications de sauvegarde existantes sans les reconfigurer pour des sauvegardes ZDB sur disque + bande, utilisez l'option `-disk_only` pour exécuter une sauvegarde ZDB sur disque.

Mise à niveau de Windows NT vers une nouvelle version de Windows

Si votre Gestionnaire de cellule est installé sur un système Windows NT, vous devez mettre à niveau le système d'exploitation vers une nouvelle version car Windows NT n'est pas pris en charge par Data Protector A.06.10 en tant que plate-forme de Gestionnaire de cellule.

Si vous souhaitez mettre à niveau votre système d'exploitation de Windows NT vers une nouvelle version de Windows, vous devez prendre en compte l'impact de cette mise à niveau sur Data Protector.

Si le Gestionnaire de cellule Data Protector A.05.10 est installé sous Windows NT, et si vous souhaitez le mettre à niveau vers Data Protector A.06.10, procédez comme suit :

1. Mettez à niveau le système d'exploitation de Windows NT vers la nouvelle version de Windows. Pour plus d'informations, reportez-vous à la documentation Windows.
2. Mettez à niveau le Gestionnaire de cellule Data Protector A.05.10 vers Data Protector A.06.10. Pour connaître la procédure à suivre, reportez-vous à la section "Mise à niveau à partir de Data Protector A.05.10, A.05.50 et A.06.00" à la page 250.

Mise à niveau de Solaris 8 vers Solaris 9

Si l'Agent de disque (DA) Data Protector est installé sous Solaris 8 et si vous voulez mettre à niveau le système d'exploitation vers Solaris 9, prenez en compte l'impact de cette mise à niveau sur Data Protector. Il est recommandé de remplacer l'Agent de disque générique Solaris installé sur le système par l'Agent de disque Solaris 9 pour garantir le bon fonctionnement de Data Protector et activer les options de sauvegarde avancées pour Solaris 9, comme par exemple la sauvegarde d'attributs étendus.

Réalisez la mise à niveau comme suit :

1. Mettez à niveau le système d'exploitation de Solaris 8 vers Solaris 9. Pour plus d'informations, reportez-vous à la documentation Solaris.
2. Installez l'Agent de disque à distance sur le système mis à niveau à l'aide d'un Serveur d'installation. L'Agent de disque générique Solaris sera ainsi remplacé par l'Agent de disque Solaris 9. Reportez-vous à la section "Installation distante de clients Data Protector" à la page 78 ou à la page man de `ob2install`.

Migration de HP-UX 11.x (PA-RISC) vers HP-UX 11.23/11.31 (IA-64)

Cette section décrit la procédure à suivre pour faire migrer votre Gestionnaire de cellule d'un système HP-UX 11.x basé sur une architecture PA-RISC vers un système HP-UX 11.23/11.31 pour l'architecture Intel Itanium 2 (IA-64).

Limites

Pour plus d'informations sur les versions des systèmes d'exploitation, les plates-formes, les architectures de processeurs et les composantsData Protector pris en charge et pour connaître les correctifs requis, les limites générales et les conditions requises pour l'installation, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.

- La migration est uniquement prise en charge à partir du Gestionnaire de cellule Data Protector A.06.10 sur un système HP-UX 11.x basé sur PA-RISC.
- Pour connaître les combinaisons de configurations MoM prises en charge, reportez-vous à la section "Informations spécifiques à MoM" à la page 292.

Condition préalable

- Avant la migration, le Gestionnaire de cellule Data Protector sur un système HP-UX 11.x basé sur une architecture PA-RISC doit être mis à niveau vers Data Protector A.06.10.

Recommandation

- Il est recommandé de convertir les noms de fichier dans la base IDB avant la migration. Reportez-vous à la section "Conversion des noms de fichiers de la base de données IDB" à la page 277.

Licences

Le nouveau Gestionnaire de cellule (système IA-64) aura une adresse IP différente de celle de l'ancien Gestionnaire de cellule; par conséquent, vous devriez demander la migration des licences avant de procéder à la migration du système. Pendant une période limitée, les licences des deux systèmes seront opérationnelles. Si les licences sont basées sur une plage IP et si l'adresse IP du nouveau Gestionnaire de cellule se situe dans cette plage, aucune reconfiguration de licence n'est nécessaire. Pour plus de détails, reportez-vous à la section "Migration de licence vers Data Protector A.06.10" à la page 364.

REMARQUE :

Sur les plates-formes Gestionnaire de cellule qui ne prennent pas en charge l'interface utilisateur graphique d'origine de Data Protector, vous pouvez utiliser l'interface utilisateur graphique Java de Data Protector ou installer l'interface utilisateur graphique d'origine de Data Protector sur un système qui la prend en charge. Utilisez la commande `omniusers` pour créer un compte utilisateur distant sur le nouveau Gestionnaire de cellule. Vous pouvez alors utiliser ce compte utilisateur avec l'interface graphique utilisateur de Data Protector installée pour lancer l'interface et vous connecter au nouveau Gestionnaire de cellule. Reportez-vous à la page `omniusers` du manuel.

Procédure de migration

Réalisez la procédure de migration comme suit :

1. Installez un client Data Protector sur le système IA-64 et importez-le dans la cellule de l'ancien Gestionnaire de cellule. Si vous avez l'intention de configurer Data Protector dans un cluster, installez le client sur le noeud principal. Reportez-vous à la section "Installation de clients HP-UX" à la page 94.
2. Exécutez la commande suivante sur l'*ancien* Gestionnaire de cellule pour ajouter le nom d'hôte du système IA-64 à la liste des hôtes approuvés sur les clients sécurisés :

   omnimigrate.pl -prepare_clients *`Nom_nouveau_GC`*, où *`Nom_nouveau_GC`* correspond au nom de client du système IA-64 de l'étape précédente.

   Pour plus d'informations sur les groupes d'hôtes approuvés et la sécurisation des clients Data Protector, reportez-vous aux sections "Sécurisation de clients" à la page 217 et "Groupement d'hôtes approuvés" à la page 226.
3. Sauvegardez la base de données IDB. Vérifiez que le support utilisé sera accessible par la suite sur le nouveau système du Gestionnaire de cellule. Reportez-vous au mot clé "Sauvegarde IDB" dans l'index de l'aide en ligne.
4. Restaurez la base IDB dans un emplacement temporaire sur le système IA-64. Reportez-vous au mot clé "Restauration IDB" dans l'index de l'aide en ligne.
5. Désinstallez le client Data Protector du nouveau système IA-64. Reportez-vous à la section "Désinstallation d'un client Data Protector" à la page 231.
6. Installez le Gestionnaire de cellule Data Protector sur le système IA-64. Si vous avez l'intention de configurer Data Protector dans un cluster, installez le Gestionnaire de cellule sur le noeud principal en tant que Gestionnaire de cellule *autonome* (non compatible avec les clusters). Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 42.

7. Si vous avez modifié le port Inet Data Protector par défaut sur l'ancien Gestionnaire de cellule, définissez le même port Inet sur le nouveau Gestionnaire de cellule. Reportez-vous à la section "Modification du numéro de port par défaut de Data Protector" à la page 398.

8. Déplacez la base de données IDB restaurée (résidant dans un emplacement temporaire sur le nouveau Gestionnaire de cellule) et les données de configuration dans le même emplacement sur le nouveau Gestionnaire de cellule que celui qu'elles occupaient sur l'ancien Gestionnaire de cellule. Reportez-vous au mot clé "Restauration IDB" dans l'index de l'aide en ligne.

   Si l'ancien Gestionnaire de cellule était compatible avec les clusters, commentez les variables `SHARED_DISK_ROOT` et `CS_SERVICE_HOSTNAME` dans le fichier `/etc/opt/omni/server/sg/sg.conf` . Cela est nécessaire même si le nouveau Gestionnaire de cellule est compatible avec les clusters.

9. Pour faire migrer l'IDB et les clients vers le nouveau Gestionnaire de cellule et pour reconfigurer les paramètres du Gestionnaire de cellule, procédez comme suit sur le *nouveau* Gestionnaire de cellule :

   - Si vous souhaitez configurer un Gestionnaire de cellule IA-64 autonome, exécutez la commande `omnimigrate.pl -configure`. Reportez-vous à la page man `omnimigrate.pl`.
   - Si vous souhaitez configurer un Gestionnaire de cellule IA-64 compatible cluster :

     a. Exécutez la commande `omnimigrate -configure_idb` pour configurer l'IDB de l'ancien Gestionnaire de cellule pour une utilisation avec le nouveau Gestionnaire de cellule. Reportez-vous à la page man `omnimigrate.pl`.

     b. Exécutez la commande `omnimigrate -configure_cm` pour reconfigurer les données de configuration de l'ancien Gestionnaire de cellule pour une utilisation avec le nouveau Gestionnaire de cellule. Reportez-vous à la page man `omnimigrate.pl`.

     c. Exportez l'ancien serveur virtuel de la cellule en exécutant la commande `omnicc -export_host` *`Nom_ancien_GC`*.

     d. Configurez le Gestionnaire de cellule principal et secondaire. Reportez-vous au mot clé "Configuration de l'intégration de MC/ServiceGuard" dans l'index de l'aide en ligne.

     e. Exécutez la commande `omnimigrate -configure_clients` pour faire migrer les clients de l'ancien Gestionnaire de cellule vers le nouveau Gestionnaire de cellule. Notez que l'ancien Gestionnaire de cellule conserve les clients dans les fichiers de configuration, mais il ne sera plus leur Gestionnaire de cellule.

REMARQUE :

Si le répertoire `/etc/opt/omni/server` est situé sur le volume de cluster partagé, les changements de configuration effectués par le script `omnimigrate.pl` affecteront tous les noeuds du cluster.

REMARQUE :

L'ancien Gestionnaire de cellule deviendra automatiquement un client dans la nouvelle cellule. Vous pouvez désinstaller le composant Gestionnaire de cellule de l'ancien Gestionnaire de cellule car il n'est plus nécessaire. Reportez-vous à la section "Changement de composants logiciels Data Protector" à la page 242.

10. Configurez les licences sur le nouveau Gestionnaire de cellule. Reportez-vous à la section "Structure de produit et licences de Data Protector A.06.10" à la page 349.
11. Créez un compte utilisateur distant sur le nouveau Gestionnaire de cellule et utilisez-le sur n'importe quel autre système équipé de l'interface graphique utilisateur de Data Protector afin de lancer cette dernière et de vous connecter au Gestionnaire de cellule. Pour plus de détails, reportez-vous à la page `omniusers` du manuel.
12. Des étapes supplémentaires sont requises dans les situations suivantes :
    - Votre cellule fait partie d'un environnement MoM. Reportez-vous à la section "Informations spécifiques à MoM" à la page 292.
    - Votre cellule fonctionne de part et d'autre d'un pare-feu. Reconfigurez tous les paramètres liés au pare-feu sur le nouveau Gestionnaire de cellule. Reportez-vous au mot clé "Environnements pare-feu" dans l'index de l'aide en ligne.
    - Vous souhaitez disposer d'un Serveur d'installation sur votre nouveau Gestionnaire de cellule. Reportez-vous à la section "Détails relatifs au Serveur d'installation" à la page 293.

Informations spécifiques à MoM

Si le nouveau Gestionnaire de cellule doit être configuré dans le MoM, des étapes supplémentaires sont requises une fois la procédure de migration de base terminée. Les étapes requises dépendent de la configuration du MoM pour l'ancien et le nouveau Gestionnaire de cellule dans votre environnement. Les combinaisons prises en charge sont les suivantes :

- L'ancien Gestionnaire de cellule était un client MoM ; le nouveau Gestionnaire de cellule sera un client MoM du même Gestionnaire MoM.
  Effectuez les opérations suivantes :

1. Dans le Gestionnaire MoM, exportez l'ancien Gestionnaire de cellule de la cellule du Gestionnaire MoM et importez le nouveau Gestionnaire de cellule. Reportez-vous au mot clé "Exportation de systèmes client" dans l'index de l'aide en ligne.
2. Ajoutez l'administrateur MoM à la liste des utilisateurs sur le nouveau Gestionnaire de cellule. Reportez-vous au mot clé "Administrateur MoM, ajout", dans l'index de l'aide en ligne.

- L'ancien Gestionnaire de cellule était un Gestionnaire MoM ; le nouveau Gestionnaire de cellule sera un Gestionnaire MoM.
  Si l'ancien Gestionnaire MoM était le seul client sur le MoM, aucune action n'est nécessaire. Dans le cas contraire, effectuez les opérations suivantes :
  1. Dans l'ancien Gestionnaire MoM (l'ancien Gestionnaire de cellule), exportez tous les clients MoM.
  2. Dans le nouveau Gestionnaire MoM (le nouveau Gestionnaire de cellule), importez tous les clients MoM.
  3. Ajoutez l'administrateur MoM à la liste des utilisateurs sur tous les nouveaux clients MoM.

REMARQUE :

Sur les plates-formes Gestionnaire de cellule qui ne prennent pas en charge l'interface utilisateur graphique d'origine de Data Protector, vous pouvez utiliser l'interface utilisateur graphique Java de Data Protector ou installer l'interface utilisateur graphique d'origine de Data Protector sur un système qui la prend en charge. Utilisez la commande `omniusers` pour créer un compte utilisateur distant sur le nouveau Gestionnaire de cellule. Vous pouvez alors utiliser ce compte utilisateur avec l'interface graphique utilisateur de Data Protector installée pour lancer l'interface et vous connecter au nouveau Gestionnaire de cellule. Reportez-vous à la page `omniusers` du manuel.

Détails relatifs au Serveur d'installation

La migration du Serveur d'installation ne s'effectue pas dans le cadre de la migration du Gestionnaire de cellule. Si un Serveur d'installation est installé sur votre ancien Gestionnaire de cellule, il ne migrera pas vers le nouveau Gestionnaire de cellule et restera le Serveur d'installation de votre cellule.

Si vous souhaitez également utiliser le nouveau Gestionnaire de cellule en tant que Serveur d'installation, installez le composant Serveur d'installation sur le nouveau Gestionnaire de cellule après la migration et importez-le dans la cellule. Reportez-vous au mot clé "Serveur d'installation" dans l'index de l'aide en ligne.

Migration d'un système Windows 32 bits/64 bits vers un système Windows 64 bits/Windows Server 2008

Cette section décrit la procédure de migration de votre Gestionnaire de cellule existant d'un système Windows 32 bits vers un système Windows 64 bits ou d'un système Windows 64 bits vers un système Windows Server 2008 64 bits.

Limites

Pour plus d'informations sur les versions des systèmes d'exploitation, les plates-formes, les processeurs et les éléments Data Protector pris en charge et pour connaître les correctifs requis, les limites générales et les conditions requises pour l'installation, reportez-vous aux Références, notes de publication et annonces produits HP Data Protector.

Condition préalable

- Avant la migration, le Gestionnaire de cellule de Data Protector sur un système Windows 32 bits doit être mis à niveau vers Data Protector A.06.10.

Recommandation

- Dans le cas d'une mise à niveau à partir de Data Protector A.05.10, nous vous recommandons d'effectuer la conversion des noms de fichiers dans l'IDB avant la migration. Reportez-vous à la section "Conversion des noms de fichiers de la base de données IDB" à la page 277.

Licences

Le nouveau Gestionnaire de cellule aura une adresse IP différente de celle de l'ancien Gestionnaire de cellule ; par conséquent, vous devriez demander la migration des licences avant de procéder à la migration du système. Pendant une période limitée, les licences des deux systèmes seront opérationnelles. Si les licences sont basées sur une plage IP et si l'adresse IP du nouveau Gestionnaire de cellule se situe dans cette plage, aucune reconfiguration de licence n'est nécessaire. Reportez-vous à la section "Migration de licence vers Data Protector A.06.10" à la page 364 pour plus de détails.

Procédure de migration

Réalisez la migration comme suit :

1. Installez un client Data Protector sur le système Windows 64 bits ou sur le système Windows Server 2008 64 bits qui deviendra votre nouveau Gestionnaire de cellule. Pour plus de détails, reportez-vous à la section "Installation de clients Windows" à la page 87.
2. Importez le système dans la cellule de l'ancien Gestionnaire de cellule'.

3. Sur l'*ancien* Gestionnaire de cellule, ajoutez le nom d'hôte du nouveau Gestionnaire de cellule à la liste des hôtes approuvés sur les clients sécurisés. Dans le répertoire `répertoire_Data_Protector\bin`, exécutez :

   ```
   perl winomnimigrate.pl -prepare_clients
   Nom_nouveau_gestionnaire
   ```

   `Nom_nouveau_gestionnaire` est le nom de client du nouveau Gestionnaire de cellule de l'étape précédente. Pour plus d'informations sur `winomnimigrate.pl`, reportez-vous au document *Guide de rfrence de l'interface de ligne de commande HP Data Protector*.

   Pour plus d'informations sur les hôtes approuvés et la sécurisation des clients Data Protector, reportez-vous aux sections "Sécurisation de clients" à la page 217 et "Groupement d'hôtes approuvés" à la page 226.

4. Sauvegardez la base de données IDB. Vérifiez que le support utilisé sera accessible par la suite sur le nouveau système du Gestionnaire de cellule. Dans l'index de l'aide en ligne, recherchez : "sauvegarde de la base de données interne".

5. Restaurez la base IDB dans un emplacement temporaire sur le nouveau Gestionnaire de cellule. Selon l'option choisie pour la sauvegarde de la base IDB, vous devrez peut-être configurer le périphérique et importer le catalogue à partir du support approprié. Une fois l'objet de sauvegarde IDB dans la base IDB, vous pouvez restaurer l'IDB afin de déplacer les données de configuration vers le nouveau système. Dans l'index de l'aide en ligne, recherchez : "restauration de la base de données interne".

6. Désinstallez le client Data Protector du nouveau Gestionnaire de cellule. Reportez-vous à la section "Désinstallation d'un client Data Protector" à la page 231.

7. Installez le Gestionnaire de cellule Data Protector sur le nouveau Gestionnaire de cellule. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 42.

8. Si vous avez modifié le port Inet Data Protector par défaut sur l'ancien Gestionnaire de cellule, définissez le même port Inet sur le nouveau Gestionnaire de cellule. Reportez-vous à la section "Modification du numéro de port par défaut de Data Protector" à la page 398.

9. Déplacez la base de données IDB restaurée (résidant dans un emplacement temporaire sur le nouveau Gestionnaire de cellule) et les données de configuration sur le nouveau Gestionnaire de cellule, dans le même emplacement qu'elles occupaient sur l'ancien Gestionnaire de cellule. Ne redémarrez pas les services Data Protector. Dans l'index de l'aide en ligne, recherchez : "restauration de la base de données interne".

10. Pour faire migrer l'IDB et les clients vers le nouveau Gestionnaire de cellule et pour reconfigurer les paramètres du Gestionnaire de cellule, procédez comme suit sur le *nouveau* Gestionnaire de cellule :

- Configurez un Gestionnaire de cellule autonome. Dans le répertoire `répertoire_Data_Protector\bin`, exécutez :
  `perl winomnimigrate.pl -configure`
  Si vous migrez le Gestionnaire de cellule vers un système Windows Server 2008 64 bits, vous pouvez utiliser l'option `-keep_dcdirs` pour conserver sans condition les références à d'autres répertoires DCBF dans la base de données IDB migrée :
  `perl winomnimigrate.pl -configure -keep_dcdirs`
- Pour configurer un Gestionnaire de cellule compatible cluster :
  a. Dans le répertoire `répertoire_Data_Protector\bin`, exécutez `perl winomnimigrate.pl -configure_idb` afin de configurer la base de données IDB de l'ancien Gestionnaire de cellule en vue d'une utilisation sur le nouveau Gestionnaire de cellule.
     Si vous migrez le Gestionnaire de cellule vers un système Windows Server 2008 64 bits, vous pouvez utiliser l'option `-keep_dcdirs` pour conserver sans condition les références à d'autres répertoires DCBF dans l'IDB migrée : `perl winomnimigrate.pl -configure_idb -keep_dcdirs`
  b. Dans le répertoire `répertoire_Data_Protector\bin`, exécutez `perl winomnimigrate.pl -configure_cm` afin de reconfigurer les données de configuration transférées de l'ancien Gestionnaire de cellule en vue d'une utilisation sur le nouveau Gestionnaire de cellule.
  c. Exportez l'ancien serveur virtuel de la cellule en exécutant la commande `omnicc -export_host` *`Nom_ancien_gestionnaire`*.
  d. Dans le répertoire `répertoire_Data_Protector\bin`, exécutez `perl winomnimigrate.pl -configure_clients` pour migrer les clients de l'ancien Gestionnaire de cellule vers le nouveau Gestionnaire de cellule. Notez que l'ancien Gestionnaire de cellule conserve les clients dans les fichiers de configuration, mais il ne sera plus leur Gestionnaire de cellule.

REMARQUE :

L'ancien Gestionnaire de cellule deviendra automatiquement un client dans la nouvelle cellule. Vous pouvez désinstaller le composant Gestionnaire de cellule de l'ancien Gestionnaire de cellule car il n'est plus nécessaire. Reportez-vous à la section "Changement de composants logiciels Data Protector" à la page 242.

11. Si vous avez installé le nouveau Gestionnaire de cellule 64 bits dans un autre répertoire que celui où l'ancien Gestionnaire de cellule était installé, les liens internes dans la base IDB seront ajoutés dans les chemins de l'ancien Gestionnaire de cellule. Ajoutez manuellement les nouveaux chemins des répertoires du catalogue de détails sur le nouveau Gestionnaire de cellule à l'aide de l'interface graphique utilisateur de Data Protector. Dans l'index de l'aide en ligne, recherchez : "création de répertoires DC".

12. Configurez les licences sur le nouveau Gestionnaire de cellule. Reportez-vous à la section "Structure de produit et licences de Data Protector A.06.10" à la page 349.

13. Des étapes supplémentaires sont nécessaires dans les cas suivants :
    - Votre cellule fait partie d'un environnement MoM. Reportez-vous à la section "Informations spécifiques à MoM" à la page 297.
    - Votre cellule fonctionne de part et d'autre d'un pare-feu. Reconfigurez tous les paramètres liés au pare-feu sur le nouveau Gestionnaire de cellule. Dans l'index de l'aide en ligne, recherchez : "environnements pare-feu".
    - Vous souhaitez disposer d'un Serveur d'installation sur votre nouveau Gestionnaire de cellule. Reportez-vous à la section "Détails relatifs au Serveur d'installation" à la page 298.

Informations spécifiques à MoM

Si le nouveau Gestionnaire de cellule doit être configuré dans le MoM, des étapes supplémentaires sont requises une fois la procédure de migration de base terminée. Les étapes requises dépendent de la configuration du MoM pour l'ancien et le nouveau Gestionnaire de cellule dans votre environnement. Les combinaisons prises en charge sont les suivantes :

- L'ancien Gestionnaire de cellule était un client MoM ; le nouveau Gestionnaire de cellule sera un client MoM du même Gestionnaire MoM.
  Effectuez les opérations suivantes :
  1. Dans le Gestionnaire MoM, exportez l'ancien Gestionnaire de cellule de la cellule du Gestionnaire MoM et importez le nouveau Gestionnaire de cellule. Dans l'index de l'aide en ligne, recherchez : "systèmes clients, exportation".
  2. Ajoutez l'administrateur MoM à la liste des utilisateurs sur le nouveau Gestionnaire de cellule. Dans l'index de l'aide en ligne, recherchez : "administrateur MoM, ajout".
- L'ancien Gestionnaire de cellule était un Gestionnaire MoM ; le nouveau Gestionnaire de cellule sera un Gestionnaire MoM.
  Si l'ancien Gestionnaire MoM était le seul client sur le MoM, aucune action n'est nécessaire. Dans le cas contraire, effectuez les opérations suivantes :
  1. Dans l'ancien Gestionnaire MoM (l'ancien Gestionnaire de cellule), exportez tous les clients MoM.

2. Dans le nouveau Gestionnaire MoM (le nouveau Gestionnaire de cellule), importez tous les clients MoM.
3. Ajoutez l'administrateur MoM à la liste des utilisateurs sur tous les clients MoM.

Détails relatifs au Serveur d'installation

La migration du Serveur d'installation ne s'effectue pas dans le cadre de la migration du Gestionnaire de cellule. Si un Serveur d'installation est installé sur votre ancien Gestionnaire de cellule, il ne fera pas l'objet d'une migration vers le nouveau Gestionnaire de cellule.

Si vous souhaitez également utiliser le nouveau Gestionnaire de cellule en tant que Serveur d'installation, installez le composant Serveur d'installation sur le nouveau Gestionnaire de cellule après la migration et importez-le dans la cellule. Dans l'index de l'aide en ligne, recherchez : "Serveur d'installation".

Mise à niveau du Gestionnaire de cellule configuré sur MC/ServiceGuard

Lors d'une mise à niveau, seule la base de données est mise à niveau : l'ancienne version du produit est supprimée. Data Protector A.06.10 est installé avec la sélection d'agents par défaut et les autres agents sont supprimés. Pour obtenir une configuration dont l'état est équivalent à l'état antérieur à la mise à niveau, vous devez sélectionner manuellement les autres agents souhaités pendant la procédure de mise à niveau, ou les réinstaller ensuite sur chacun des nœuds physiques.

La procédure de mise à niveau de Data Protector A.05.10, Data Protector A.05.50 ou Data ProtectorA.06.00 consiste à mettre à niveau le nœud principal et les nœuds secondaires. Pour cela, procédez comme suit :

Nœud principal

Connectez-vous au nœud principal et procédez comme suit :

1. Arrêtez l'ancien package OmniBack/Data Protector en exécutant la commande `cmhaltpkg` *`nom_pkg`* (où *`nom_pkg`* correspond au nom du package de clusters). Par exemple :

   ```
   cmhaltpkg ob2cl
   ```

2. Activez le groupe de volumes en mode exclusif :

   ```
   vgchange -a e -q y nom_gv
   ```

   Par exemple :

   ```
   vgchange -a e -q y /dev/vg_ob2cm
   ```

3. Montez le volume logique sur le disque partagé :

   `mount chemin_vl disque_partagé`

   Le paramètre *chemin_vl* correspond au nom de chemin du volume logique et le paramètre *disque_partagé* au point de montage ou répertoire partagé. Par exemple :

   `mount /dev/vg_ob2cm/lv_ob2cm /omni_shared`

4. Mettez à niveau le Gestionnaire de cellule en suivant la procédure décrite dans les paragraphes qui suivent. Notez que certaines étapes sont différentes selon la version du produit que vous mettez à niveau vers Data Protector A.06.10. Reportez-vous à la section "Mise à niveau du Gestionnaire de cellule et du Serveur d'installation UNIX" à la page 251.

5. Arrêtez les services Data Protector s'ils sont en cours d'exécution :

   `/opt/omni/sbin/omnisv -stop`

6. Démontez le disque partagé :

   `umount disque_partagé`

   Par exemple :

   `umount /omni_shared`

7. Désactivez le groupe de volumes :

   `vgchange -a n nom_gv`

   Par exemple :

   `vgchange -a n /dev/vg_ob2cm`

Nœud secondaire

Connectez-vous au nœud secondaire et procédez comme suit :

1. Activez le groupe de volumes en mode exclusif :

   `vgchange -a e -q y nom_gv`

2. Montez le volume logique sur le disque partagé :

   `mount chemin_vl disque_partagé`

3. Mettez à niveau le Gestionnaire de cellule. Les étapes sont différentes selon la version du produit que vous mettez à niveau vers Data Protector A.06.10. Suivez les étapes de la procédure décrite à la section "Mise à niveau du Gestionnaire de cellule et du Serveur d'installation UNIX" à la page 251.

4. Renommez les scripts de démarrage `csfailover.sh` et `mafailover.ksh` dans le répertoire `/etc/opt/omni/server/sg` (en leur donnant par exemple les noms `csfailover_DP51.sh` et `mafailover_DP51.ksh`) et copiez les nouveaux scripts `csfailover.sh` et `mafailover.ksh` du répertoire `/opt/omni/newconfig/etc/opt/omni/server/sg` vers le répertoire `/etc/opt/omni/server/sg`.

   Si vous avez personnalisé vos anciens scripts de démarrage, implémentez à nouveau les modifications dans les nouveaux scripts de démarrage.

REMARQUE :

En cas de mise à niveau de Data Protector A.05.10, les chemins par défaut de certains fichiers de configuration, fichiers journaux et de base de données (sous UNIX) ont été modifiés dans Data Protector A.05.50 et versions ultérieures. Certains fichiers figurant dans les répertoires server et client sont désormais divisés. Reportez-vous à la section "Fichiers de configuration sous UNIX" à la page 442.

5. Arrêtez les services Data Protector s'ils sont en cours d'exécution :

   ```
   /opt/omni/sbin/omnisv -stop
   ```

6. Démontez le disque partagé :

   ```
   umount disque_partagé
   ```

7. Désactivez le groupe de volumes :

   ```
   vgchange -a n nom_gv
   ```

Nœud principal

Reconnectez-vous au nœud principal et procédez comme suit :

1. Redémarrez le package Data Protector :

   ```
   cmrunpkg nom_pkg
   ```

   Assurez-vous que le basculement du package et les options de basculement des nœuds sont activés.

2. Configurez le Gestionnaire de cellule. Veillez à ne pas vous placer dans les répertoires `/etc/opt/omni` ou `/var/opt/omni` ou dans leurs sous-répertoires lorsque vous exécutez ce script. Assurez-vous également qu'il n'existe aucun sous-répertoire monté dans `/etc/opt/omni` ou `/var/opt/omni`. Exécutez :

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

3. Arrêtez les services Data Protector s'ils sont en cours d'exécution :

   ```
   /opt/omni/sbin/omnisv -stop
   ```

4. Démontez le disque partagé :

   `umount disque_partagé`

5. Désactivez le groupe de volumes :

   `vgchange -a n nom_gv`

Nœud secondaire

Connectez-vous à nouveau au nœud secondaire et procédez comme suit :

1. Redémarrez le package Data Protector :

   `cmrunpkg nom_pkg`

   Assurez-vous que le basculement du package et les options de basculement des nœuds sont activés.

2. Configurez le Gestionnaire de cellule. Veillez à ne pas vous placer dans les répertoires `/etc/opt/omni` ou `/var/opt/omni` ou dans leurs sous-répertoires lorsque vous exécutez ce script. Assurez-vous également qu'il n'existe aucun sous-répertoire monté dans `/etc/opt/omni` ou `/var/opt/omni`. Exécutez :

   ```
   /opt/omni/sbin/install/omniforsg.ksh -secondary /share
   -upgrade
   ```

3. Arrêtez les services Data Protector s'ils sont en cours d'exécution :

   `/opt/omni/sbin/omnisv -stop`

4. Démontez le disque partagé :

   `umount disque_partagé`

5. Désactivez le groupe de volumes :

   `vgchange -a n nom_gv`

Nœud principal

Reconnectez-vous au nœud principal et procédez comme suit :

1. Redémarrez le package Data Protector :

   `cmrunpkg nom_pkg`

   Assurez-vous que le basculement du package et les options de basculement des nœuds sont activés.

2. Réimportez l'hôte virtuel :

   `omnicc -import_host nom_hôte_virtuel -virtual`

3. Changez le nom du Gestionnaire de cellule dans la base de données IDB :

   `omnidbutil -change_cell_name`

4. Si le Serveur d'installation se trouve dans le même package que le Gestionnaire de cellule, importez le nom d'hôte virtuel du serveur d'installation :

   `omnicc -import_is` *`nom_hôte_virtuel`*

REMARQUE :

Toutes les demandes provenant des Gestionnaires de cellule sont enregistrées dans le fichier `/var/opt/omni/log/inet.log` sur les clients. Pour empêcher l'écriture d'entrées inutiles dans le journal, sécurisez les clients. Pour plus d'informations sur la procédure de sécurisation d'une cellule, reportez-vous à la section "Considérations sur la sécurité" à la page 214.

Mise à niveau du Gestionnaire de cellule configuré sur Microsoft Cluster Server

La mise à niveau de Data Protector A.05.10, A.05.50 ou A.06.00 Gestionnaire de cellule vers Data Protector A.06.10 sur Microsoft Cluster Server (MSCS) se fait en local, à partir du DVD-ROM d'installation Windows.

REMARQUE :

Il est recommandé d'installer MSI 2.0 sur tous les nœuds de clusters .

Pour effectuer la mise à niveau, procédez comme suit :

1. Insérez le DVD-ROM d'installation Windows et exécutez la commande `\Windows_other\\i386\setup.exe`. Il est recommandé de lancer l'installation sur le noeud de serveur virtuel actuellement actif.

   Le programme d'installation détecte automatiquement l'ancienne version du produit et vous invite à la mettre à niveau vers Data Protector A.06.10.

   Cliquez sur Suivant pour continuer.

2. Data Protector sélectionne automatiquement les composants qui ont été installés.

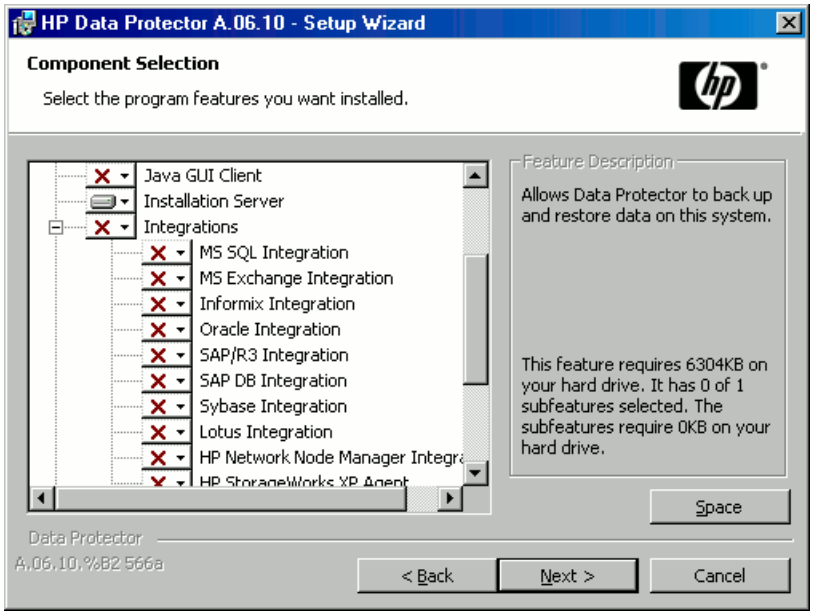

Figure 47 - Sélection des composants

3. La liste récapitulative des composants sélectionnés s'affiche. Cliquez sur Installer pour effectuer la mise à niveau.

   Notez qu'à l'issue de la mise à niveau, tous les nœuds disposent du même jeu de composants.

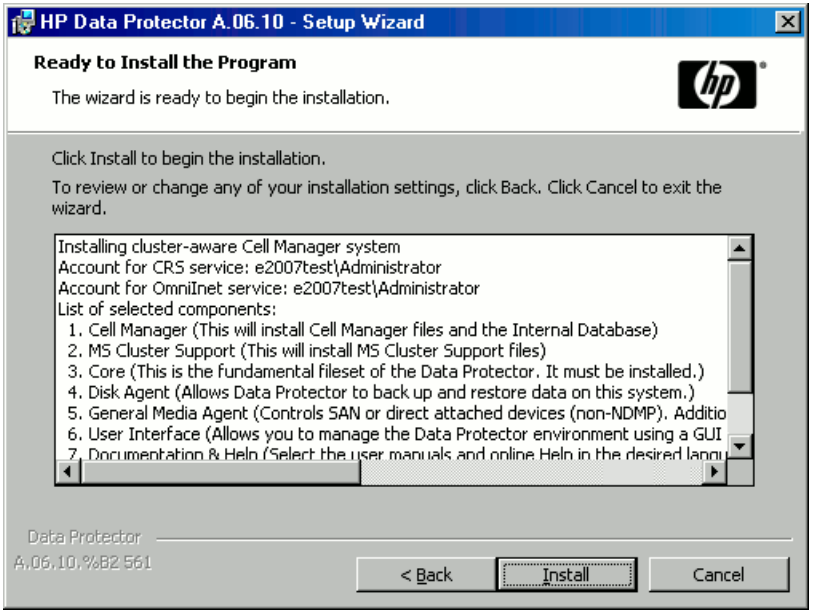

Figure 48 - Page de résumé des composants sélectionnés

4. La page d'état de l'installation s'affiche. Cliquez sur Suivant.

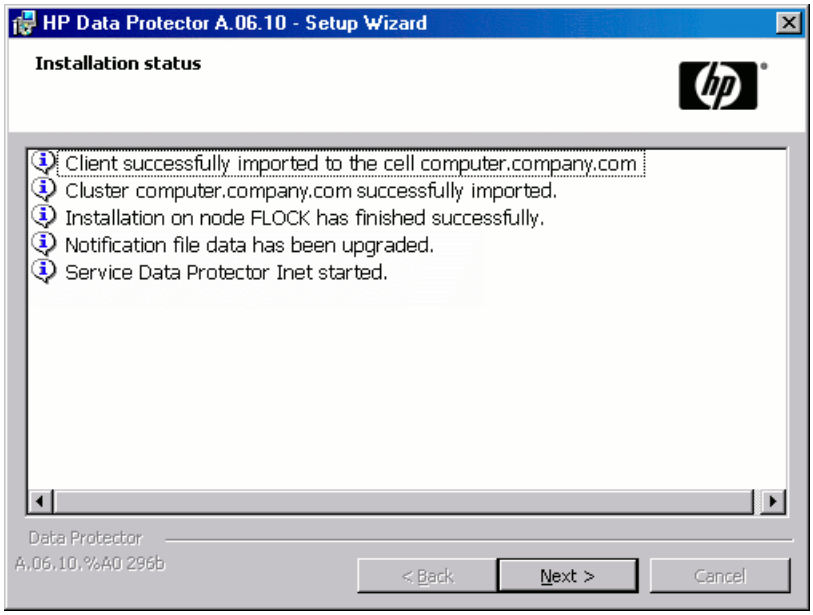

Figure 49 - Page d'état de l'installation

5. Si des clients UNIX sont présents dans la cellule, la page Conversion de l'IDB s'affiche. Reportez-vous à la section "Conversion des noms de fichiers de la base de données IDB" à la page 277.

6. Pour commencer à utiliser Data Protector immédiatement après son installation, sélectionnez Start the Data Protector Manager GUI (Lancer l'interface graphique du gestionnaire Data Protector).

   Pour consulter les *Références, notes de publication et annonces produits HP Data Protector*, sélectionnez Ouvrir les annonces sur les produits.

   Il n'est *pas* recommandé d'installer l'utilitaire HP AutoPass sur Microsoft Cluster Server, car il ne serait installé que sur un seul noeud et non sur tous. Toutefois, si vous installez AutoPass, vous devez désinstaller Data Protector du même noeud sur lequel il était installé, une fois que vous décidez de supprimer Data Protector du système.

   Cliquez sur Terminer.

REMARQUE :

Si vous mettez à niveau des clients compatibles cluster, commencez par mettre à niveau séparément chaque nœud de cluster, puis réimportez le serveur virtuel. La mise à niveau à distance n'est pas prise en charge.

5 Attribution de licences Data Protector

Description du chapitre

Ce chapitre contient des informations sur la vérification et le signalement des licences Data Protector ainsi que sur l'obtention et l'installation de mots de passe Data Protector.

Introduction

La structure Data Protector A.06.10 et de son système d'attribution de licences comprend trois catégories principales :

1. Packs Starter
2. Extensions de lecteur et extensions de bibliothèque
3. Extensions fonctionnelles

REMARQUE :

Les licences UNIX du produit fonctionnent sur toutes les plates-formes, avec le même niveau de fonctionnalité quelle que soit la plate-forme, tandis que les licences Windows fonctionnent uniquement sur les plates-formes Windows, NetWare et Linux.

Liés au Gestionnaire de cellule, les mots de passe sont valides pour l'intégralité de la cellule Data Protector. Les clients ne requièrent aucune licence pour les sauvegardes de système de fichiers ou d'image disque.

Vérification et signalement des licences manquantes

La présence des licences Data Protector est vérifiée et leur absence éventuelle est signalée lors de diverses opérations de Data Protector, par exemple :

- Dans le cadre du mécanisme de vérification et de maintenance de Data Protector, la présence des licences est vérifiée et leur absence éventuelle est consignée dans le journal d'événements de Data Protector. Le journal d'événements de Data Protector se trouve sur le Gestionnaire de cellule dans *donnes_programme_Data_Protector*`\log\server\Ob2EventLog.txt` (Windows Server 2008) ou dans *répertoire_Data_Protec-*

tor\log\server\Ob2EventLog.txt (autres systèmes Windows). Pour plus d'informations sur le mécanisme de vérification et de maintenance de Data Protector, recherchez l'entrée suivante dans l'index de l'aide en ligne : "journal d'événements, Data Protector".

- Si des licences manquantes sont signalées dans le journal des événements de Data Protector au démarrage de l'interface utilisateur de Data Protector, une notification du journal des événements s'affiche. Pour plus d'informations sur le journal d'événements de Data Protector, recherchez l'entrée suivante dans l'index de l'aide en ligne : "journal d'événements, Data Protector".
- Au démarrage d'une session Data Protector, la présence des licences est vérifiée et leur absence éventuelle est signalée.

Les licences Data Protector sont regroupées comme suit selon leurs caractéristiques :

- Licences liées au Gestionnaire de cellule
- Licences basées sur les entités
- Licences basées sur la capacité

Licences liées au Gestionnaire de cellule

Les licences liées au Gestionnaire de cellule Data Protector sont :

- Packs Starter
- Extension Manager-of-Managers
- Edition serveur unique

Lorsqu'un composant Data Protector donné, tel que le Gestionnaire de cellule (inclus dans le Pack Starter) ou le Manager-of-Managers, est présent dans la cellule, seule la présence des licences de base et spéciales est vérifiée.

Licences basées sur les entités

Les licences basées sur les entités Data Protector sont :

- Extension de bibliothèque pour une bibliothèque de 61 à 250 emplacements et pour une bibliothèque avec un nombre illimité d'emplacements
- Extension de lecteur pour UNIX / NAS / SAN et extension de lecteur pour Windows / NetWare / Linux (Intel)
- Extension pour sauvegarde en ligne d'un seul système UNIX et extension pour sauvegarde en ligne d'un seul système Windows / Linux
- Extension de cryptage Data Protector

Lorsque l'un des éléments soumis aux licences basées sur la source est configuré dans la cellule, la présence et le nombre des licences requises basées sur les entités sont vérifiés.

Data Protector compare le nombre d'éléments configurés basés sur les entités et le nombre de licences basées sur les entités. S'il y a moins de licences que d'éléments configurés, Data Protector émet une notification.

Dans le cas des deux premières licences de la liste ci-dessus, il convient de respecter la règle suivante :

Lorsqu'un périphérique de sauvegarde est configuré dans un environnement SAN pour plusieurs clients Data Protector, la fonctionnalité multi-chemins doit être utilisée pour que Data Protector le reconnaisse comme un périphérique de sauvegarde unique.

Licences basées sur la capacité

Les licences Data Protector basées sur la capacité sont les suivantes :

- Sauvegarde avec temps d'indisponibilité nul (ZDB) pour HP StorageWorks XP pour 1 To et 10 To
- Sauvegarde avec temps d'indisponibilité nul pour HP StorageWorks Enterprise Virtual Array pour 1 To et 10 To
- Sauvegarde avec temps d'indisponibilité nul pour EMC Symmetrix DMX 1 To et 10 To
- Restauration instantanée pour HP StorageWorks Enterprise Virtual Array pour 1To et 10 To
- Sauvegarde directe pour HP StorageWorks Disk Array XP pour 1 To et 10 To
- Sauvegarde directe pour HP StorageWorks Enterprise Virtual Array pour 1 To et 10 To
- Sauvegarde directe via NDMP pour 1 To et 10 To
- Sauvegarde avancée sur disque pour 1 To, 10 To et 100 To
- Extension de sauvegarde sur HP IAP pour 1 To

Lorsqu'une licence basée sur la capacité (autre que celle de sauvegarde avancée sur disque) est vérifiée, la quantité *totale* de l'espace disque des unités logiques sauvegardées est comparée au nombre de licences installées.

La vérification des licences est effectuée de façon à vous permettre de réaliser une restauration instantanée ou une sauvegarde même si vous avez atteint la capacité autorisée par la licence. Dans ce cas, un message d'avertissement apparaît au cours de la session de sauvegarde vous informant que vous avez dépassé la capacité autorisée par la licence.

La capacité de disque utilisée est calculée d'après les informations d'historique collectées au cours de chaque session de sauvegarde avec temps d'indisponibilité nul ou de sauvegarde directe. L'intervalle de temps retenu est vingt-quatre heures. Data Protector calcule la capacité de disque utilisée en tenant compte des disques ayant été utilisés pendant toutes les sessions au cours des dernières vingt-quatre heures et compare la capacité ainsi obtenue à la capacité autorisée par la licence.

En cas de violation de licence, un message d'avertissement est émis au cours de la sauvegarde. En outre, l'outil de génération de rapports sur les licences est exécuté quotidiennement et il inscrit une notification dans le journal des événements de Data Protector en cas de dépassement de la capacité autorisée par la licence.

Calcul de la capacité utilisée

La fonction de calcul de la capacité utilisée évalue la capacité autorisée par la licence pour chaque type de baie de disques ayant été utilisé au cours des dernières vingt-quatre heures. Les disques utilisés deux fois ou plus au cours de l'intervalle de temps spécifié ne sont comptabilisés qu'une seule fois. Chaque baie de disques est identifiée par son numéro d'identification. L'utilisation des numéros d'identification des baies indique si une baie a déjà été comptabilisée.

Si une session de sauvegarde avec temps d'indisponibilité nul incluant une restauration instantanée ou une sauvegarde directe a été exécutée, la capacité totale de l'unité d'origine est calculée pour inclure d'une part la capacité utilisée pour la sauvegarde avec temps d'indisponibilité nul par baie de disques et d'autre part la capacité utilisée pour la restauration instantanée ou la sauvegarde directe par baie de disques.

Prenons l'exemple d'un scénario avec deux baies de disques EVA. Une baie contient un seul disque (serveur 1) d'une capacité de 200 Go utilisée pour la protection des données. Les sessions de sauvegarde déclenchées trois fois par jourackup session incluent une option de restauration instantanée. Trois snapshots sont conservés simultanément ; ils sont utilisés tour à tour à des fins de restauration instantanée. La deuxième baie de disques comporte deux disques (serveur 2 et serveur 3) dont la capacité est de 150 Go et de 120 Go, respectivement). La sauvegarde est exécutée une fois par jour sur le disque du serveur 2 et le snapshot est supprimé une fois les données copiées sur la bande. Sur le serveur 3, la sauvegarde est exécutée trois fois par jour et cinq snapshots différents sont utilisés tour à tour à des fins de restauration instantanée. Reportez-vous à la Figure 50 à la page 311.

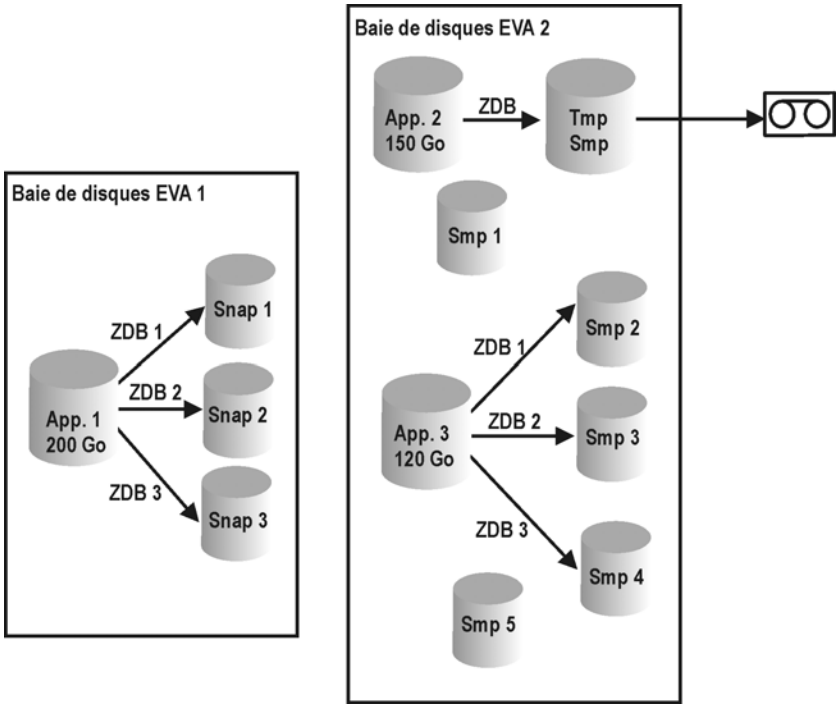

Figure 50 - Scénario de calcul de la capacité utilisée

Le calcul de la capacité utilisée pour la sauvegarde avec temps d'indisponibilité nul tient compte de tous les disques utilisés lors des sessions de sauvegarde au cours des dernières vingt-quatre heures 200 Go (Serveur 1) + 150 Go (Serveur 2) + 120 Go (Serveur 3) = 470 Go.

La fonction de calcul de la capacité utilisée pour la restauration instantanée évalue la capacité source pour les sessions de sauvegarde avec temps d'indisponibilité nul ayant laissé des données à des fins de restauration instantanée. Le même disque n'est pris comptabilisé qu'une fois : 200 Go (Serveur 1) + 120 Go (Serveur 3) = 320 Go.

Licence de sauvegarde avancée sur disque

La licence de sauvegarde avancée sur disque est requise pour pouvoir réaliser une sauvegarde sur une bibliothèque de fichiers Data Protector. Elle peut également être utilisée pour une bibliothèque de bandes virtuelle à la place des licences de lecteur ou de bibliothèque. Cette licence est requise par capacité native utilisable d'espace de sauvegarde sur disque en teraoctets (To).

CONSEIL :

Des licences supplémentaires pour 10 To et 100 To sont également disponibles. Elles sont plus économiques que 10 licences de 1 To ou 100 licences de 1 To.

- La capacité native utilisable d'une bibliothèque de fichiers Data Protector correspond à la taille sur disque de tous les fichiers utilisés pour la bibliothèque de fichiers, telle que l'indique le système de fichiers.
  - Sauvegarde complète virtuelle et sauvegarde complète synthétique Data Protector : les sauvegardes complètes virtuelles et les sauvegardes incrémentales à consolider en sauvegarde complète synthétique/virtuelle doivent être stockées dans la bibliothèque de fichiers Data Protector qui requiert cette licence.
- La capacité native utilisable d'une bibliothèque de bandes virtuelle correspond à la taille sur disque de la bibliothèque de bandes virtuelle utilisée par toutes les sauvegardes Data Protector protégées, telle que l'indique la bibliothèque.
  - Si la bibliothèque dispose de la fonction intégrée pour migrer des données de sauvegarde du cache de disque vers un disque ou une bande plus économique, la capacité de stockage migrée doit faire l'objet d'une licence complète. Aucune licence de lecteur et de bibliothèque n'est requise pour la bibliothèque de bandes contrôlée exclusivement par la bibliothèque de bandes virtuelle, mais la capacité utilisée de toutes les bandes de la bibliothèque physique doit faire l'objet d'une licence. Dans ces cas, il peut s'avérer plus économique d'adopter le modèle de licence de lecteur de bandes (références B6953AA et B6963AA). Ceci ne s'applique pas si la copie d'objet Data Protector a servi à migrer les données de sauvegarde vers un autre disque ou une autre bande.
  - Pour chaque bibliothèque de bandes virtuelle, vous pouvez choisir d'utiliser le modèle de licence de sauvegarde sur disque ou sur lecteur de bandes. Les deux modèles ne doivent pas être combinés dans une même bibliothèque.
  - Par défaut, Data Protector traite les bibliothèques de bandes virtuelles comme des bibliothèques ordinaires (comme les bibliothèques SCSI II par exemple). Pour pouvoir utiliser les licences de sauvegarde avancée sur disque, il faut que le périphérique soit identifié comme bibliothèque de bandes virtuelle lors de sa configuration. Dans l'index de l'aide en ligne, recherchez : "bibliothèque de bandes virtuelle".
  - Si la licence a été achetée avant le 1er juillet 2008, HP s'engage à une pleine protection des investissements. En d'autres termes, vous pouvez choisir d'utiliser la licence pour la bibliothèque de bandes virtuelle selon les anciennes conditions : la capacité native utilisable d'une bibliothèque de bandes virtuelle correspond à l'espace occupé par les sauvegardes protégées et les miroirs et copies de sauvegarde protégés selon la base de données interne de Data Protector. Pour que la gestion des licences des bibliothèques de bandes virtuelles reste simple, un taux de compression hypothétique de 2

pour 1 est appliqué pour les bibliothèques de ce type sans supplément de prix. Le maintien du modèle précédent n'a de sens que si vous n'utilisez pas une technologie de compression ou de déduplication. Sinon, vous obtenez une solution plus avantageuse en utilisant des licences achetées auparavant selon le nouveau modèle de licence.

  - Si Data Protector utilise exclusivement la bibliothèque de bandes virtuelle, il est conseillé d'acquérir une licence pour une quantité correspondant à la capacité physique de la bibliothèque de bandes virtuelle. HP parle de "capacité native utilisable" pour désigner la capacité physique de la bibliothèque de bandes virtuelle. D'autres fournisseurs parlent de "capacité brute".
  - Aucune licence Data Protector supplémentaire n'est requise pour la réplication de la bibliothèque de bandes virtuelle.

- Avec ce concept d'attribution de licences en fonction de la taille sur disque, il n'est pas nécessaire de prendre en compte les taux de compression et de déduplication, ni la configuration RAID.
- 1 To = 1024 Go, 1 Go = 1024 Mo, 1 Mo = 1024 Ko, 1 Ko = 1024 octets
- Dans le cas de la gestion centrale des licences avec le Gestionnaire MoM, au moins 1 To doit être affecté à chaque cellule via la fonctionnalité de sauvegarde avancée sur disque.

REMARQUE :

Data Protector n'est pas en mesure d'indiquer le nombre requis de licences car les bibliothèques de bandes virtuelles actuelles et certains serveurs de fichiers hébergeant la bibliothèque de fichiers Data Protector ne disposent pas des interfaces et des outils adéquats. L'utilisateur est responsable d'acquérir une licence couvrant la capacité en fonction des définitions de licence. Lorsque vous commandez une nouvelle capacité d'espace de sauvegarde, vérifiez toujours que les licences Data Protector disponibles couvrent la capacité de votre infrastructure de sauvegarde.

Exemples :

- Une baie de disques de sauvegarde avec une capacité native utilisable totale de 2,5 To, entièrement utilisée pour la sauvegarde avancée sur disque, requiert 3 licences B7038AA.
- Une baie de disques de sauvegarde avec une capacité brute totale de 2,5 To, entièrement configurée en RAID 1 (mise en miroir), a seulement une capacité native utilisable de 1,25 To et ne requiert que deux licences B7038AA si elle est entièrement utilisée pour la sauvegarde avancée sur disque.
- Deux baies de disques de sauvegarde avec une capacité native utilisable totale de 2,5 To chacune, entièrement utilisées pour la sauvegarde avancée sur disque, nécessitent 5 licences B7038AA.
- Dix serveurs lame avec une capacité native utilisable de 0,75 To chacun, entièrement utilisés pour la sauvegarde avancée sur disque, requièrent huit

licences B7038AA (en fait, il serait plus économique d'acquérir une licence B7038BA (10 To)).

- Une bibliothèque de bandes virtuelle avec une capacité de disque utilisable de 10 To et contrôlant 90 To de données de sauvegarde sur bandes requiert une licence B7038CA (100 To).

Extension de sauvegarde sur HP IAP

Comprend la licence d'utilisation pour 1 To d'espace d'archivage sur disque. Licence requise par capacité native utilisable d'espace d'archivage sur disque en teraoctets (To).

- La licence de sauvegarde sur HP IAP est requise pour pouvoir réaliser une sauvegarde sur HP Integrated Archive Platform (IAP).
- La capacité native utilisable correspond à l'espace utilisable du système de fichiers selon le système d'exploitation sous-jacent.
- La capacité utilisable se distingue de la capacité brute en ce qu'elle exclut le surdébit RAID. Cela signifie qu'il n'est pas nécessaire de prendre en compte la configuration RAID.
- Aucune licence d'utilisation de lecteur ou de bibliothèque n'est requise.
- Aucun supplément de prix n'est demandé pour la compression au niveau de la capacité native utilisable. La compression peut être assurée par le système d'exploitation sous-jacent. C'est également le cas pour l'instanciation unique.
- Aucune licence supplémentaire n'est requise pour la réplication vers une autre plate-forme HP IAP à l'aide de la technologie de réplication intégrée HP IAP.
- Dans le cas de la gestion centrale des licences avec le Gestionnaire MoM, au moins 1 To doit être affecté à chaque cellule via la fonctionnalité de sauvegarde sur HP IAP.

Exemple :

- Une plate-forme HP IAP avec une capacité native utilisable totale de 2,5 To, entièrement utilisée pour la sauvegarde sur HP IAP avec instanciation unique et offrant un stockage de 100 To de données non compressées, requiert trois licences TA030AA.

Exemples de licences basées sur la capacité

Ce paragraphe fournit des exemples illustrant la manière dont les licences basées sur la capacité sont attribuées.

Exemple 1

La Figure 51 à la page 315 montre une situation dans laquelle les données d'une unité logique de 800 Go sont sauvegardées trois fois par jour au cours d'une session de sauvegarde avec temps d'indisponibilité nul sur disque.

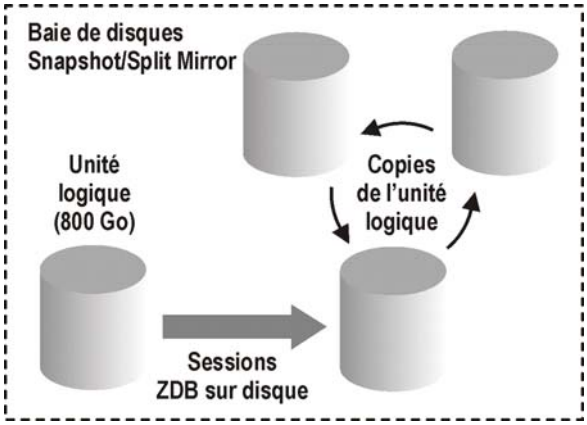

Figure 51 - Sessions de sauvegarde avec temps d'indisponibilité nul sur disque

Trois copies Split mirror ou snapshot (répliques) sont copiées en rotation et conservées à des fins de restauration instantanée. L'attribution de la licence basée sur la capacité est calculée de la manière suivante :

Une unité logique de 800 Go est utilisée pour les sessions de sauvegarde avec temps d'indisponibilité nul sur disque :

1 x 800 Go = 0,8 To pour la licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To".

Trois copies de la même unité logique de 800 Go sont conservées à des fins de restauration instantanée. Notez que la licence tient compte de la capacité de stockage des volumes source et non de la capacité des répliques :

1 x 800 Go = 0,8 To pour la licence "Restauration instantanée pour 1 To".

Une licence "Sauvegarde à temps d'indisponibilité nul pour 1 To" et une licence "Restauration instantanée pour 1 To" suffisent pour le cas illustré.

Exemple 2

La Figure 52 à la page 316 montre une situation dans laquelle les données d'une unité logique de 800 Go sont sauvegardées deux fois par jour au cours d'une session de sauvegarde avec temps d'indisponibilité nul sur bande. Par conséquent, les copies Split mirror ou snapshot (répliques) ne sont pas conservées à des fins de restauration instantanée. L'attribution de la licence basée sur la capacité est calculée de la manière suivante :

Une unité logique de 800 Go est utilisée pour les sessions de sauvegarde avec temps d'indisponibilité nul sur disque :

1 x 800 Go = 0,8 To pour la licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To".

La licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To" suffit.

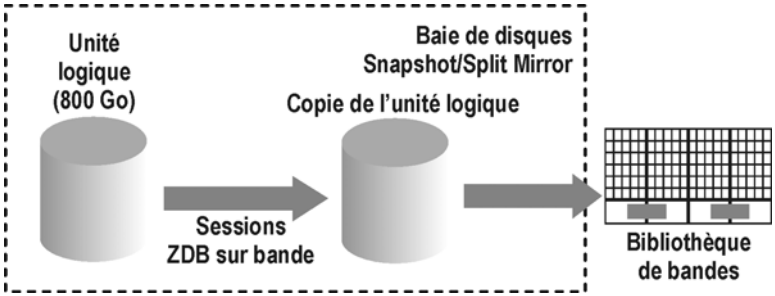

Figure 52 - Sessions de sauvegarde avec temps d'indisponibilité nul sur bande

Exemple 3

La Figure 53 à la page 317 montre une situation dans laquelle les données d'une unité logique de 800 Go sont sauvegardées trois fois par jour au cours d'une session de sauvegarde avec temps d'indisponibilité nul sur disque + bande. Cinq copies Split mirror ou snapshot (répliques) sont copiées en rotation et conservées à des fins de restauration instantanée. L'attribution de la licence basée sur la capacité est calculée de la manière suivante :

Une unité logique de 800 Go est utilisée pour les sessions avec temps d'indisponibilité nul sur disque + bande :

1 x 800 Go = 0,8 To pour la licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To".

Cinq copies de la même unité logique de 800 Go sont conservées à des fins de restauration instantanée. Notez que la licence tient compte de la capacité de stockage des volumes source et non de la capacité des répliques :

1 x 800 Go = 0,8 To pour la licence "Restauration instantanée pour 1 To".

Une licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To" et une licence "Restauration instantanée pour 1 To" suffisent.

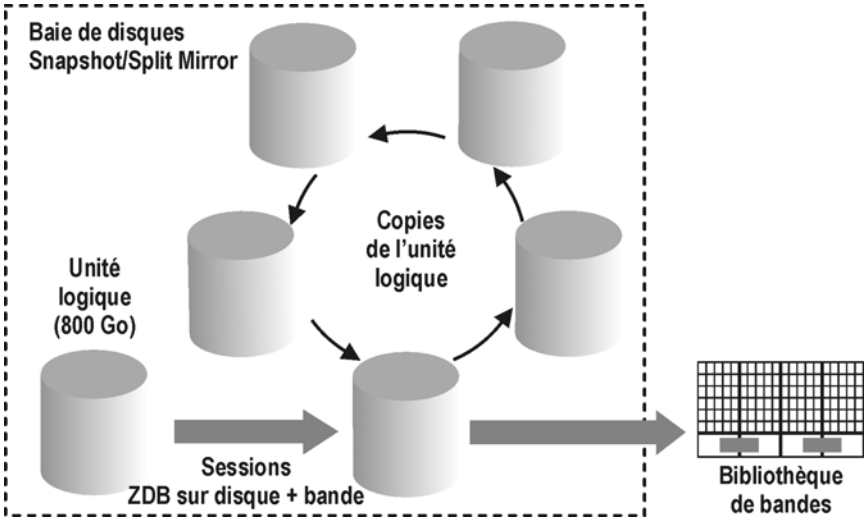

Figure 53 - Sessions avec temps d'indisponibilité nul sur disque + bande

Exemple 4

La Figure 54 à la page 318 montre une situation dans laquelle les données d'une unité logique de 800 Go sont sauvegardées quatre fois par jour au cours d'une session de sauvegarde directe. Trois copies Split mirror ou snapshot (répliques) créées lors de la session de sauvegarde directe sont copiées en rotation et conservées à des fins de restauration instantanée. L'attribution de la licence basée sur la capacité est calculée de la manière suivante :

Une unité logique de 800 Go est utilisée pour les sessions de sauvegarde directe :

1 x 800 Go = 0,8 To pour la licence "Sauvegarde directe pour 1 To".

La même unité logique de 800 Go est utilisée pour les sessions de sauvegarde avec temps d'indisponibilité nul sur disque + bande. Elle est donc soumise à une autre licence :

1 x 800 Go = 0,8 To pour la licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To".

Trois copies de la même unité logique de 800 Go sont conservées à des fins de restauration instantanée. Notez que la licence tient compte de la capacité de stockage des volumes source et non de la capacité des répliques :

1 x 800 Go = 0,8 To pour la licence "Restauration instantanée pour 1 To".

Une licence "Sauvegarde directe pour 1 To", une licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To" et une licence "Restauration instantanée pour 1 To" suffisent pour le cas illustré par la Figure 54 à la page 318.

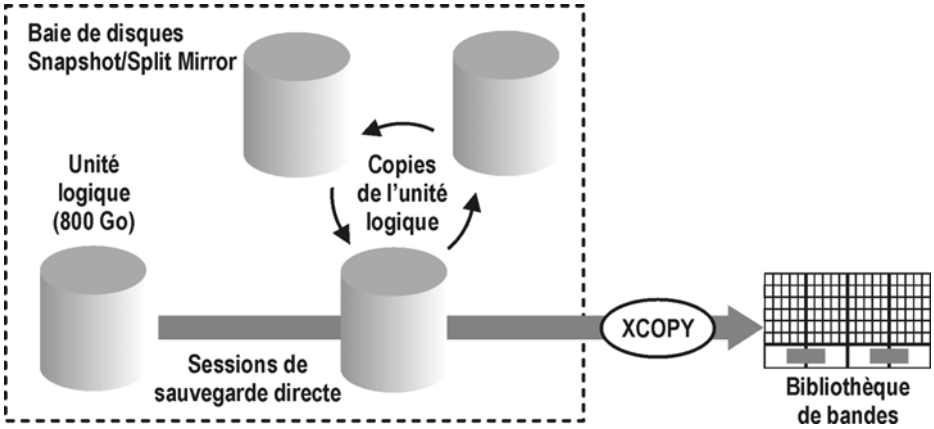

Figure 54 - Sessions de sauvegarde directe

Exemple 5

Une unité logique de 200 Go, une de 500 Go, une de 120 Go et une de 300 Go sont utilisées dans des sessions de sauvegarde avec temps d'indisponibilité nul :

1 x 200 Go + 1 x 500 Go + 1 x 120 Go + 1 x 300 Go = 1,12 To pour la licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To".

Des copies Split Mirror ou snapshot d'unités logiques de respectivement 200 Go, 120 Go et 300 Go sont conservées à des fins de restauration instantanée :

1 x 200 Go + 1 x 120 Go + 1 x 300 Go = 0,62 To pour la licence "Restauration instantanée pour 1 To".

Une unité logique de 300 Go est utilisée dans les sessions de sauvegarde directe :

1 x 300 Go = 0,3 To pour la licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To".

Une licence "Sauvegarde directe pour 1 To", deux licences "Sauvegarde avec temps d'indisponibilité nul pour 1 To" et une licence "Restauration instantanée pour 1 To" suffisent si les quatre exemples dans les figures Figure 51 à la page 315 à Figure 55 à la page 320 sont configurés dans une cellule.

Production d'un rapport de licences sur demande

Pour générer un rapport sur les licences, utilisez la commande `omnicc` de Data Protector. Saisissez la commande suivante :

```
omnicc -check_licenses [-detail]
```

Si l'option `-detail` n'est pas spécifiée, les informations renvoyées par la commande indiquent si l'attribution de licences Data Protector est possible ou non.

Si l'option `-detail` est spécifiée, un rapport détaillé est généré. Les informations renvoyées pour chaque licence de la cellule sont les suivantes : nom de licence, licences installées, licences utilisées et licences requises.

Pour plus d'informations, reportez-vous à la page `omnicc` du manuel. Notez que la commande n'indique pas les dates d'expiration des licences. Selon l'environnement et le nombre de licences installées, le rapport peut mettre un certain temps pour se générer. Pour obtenir les dates d'expiration des licences, saisissez la commande suivante :

```
omnicc -password_info
```

IMPORTANT :

Dans un environnement MoM dans lequel la base de données CMMDB est configurée, il convient d'exécuter la commande `omnicc` sur le Gestionnaire de cellule sur lequel la base de données CMMDB est installée lors de la génération d'un rapport sur les licences pour les éléments liés aux bibliothèques et aux lecteurs.

Quelles sont les licences disponibles ?

Le tableau suivant présente les licences disponibles avec ce produit. Pour obtenir des informations détaillées sur chaque référence produit, reportez-vous à l'Annexe A à la page 349 du présent manuel.

1. Packs Starter	(obligatoire)	ttes plates-formes	Windows	Linux	HP-UX	Solaris
licence et DVD	1 x cellule		B6961AA	B6961DA	B6951AA	B6951DA
manuels papier Pack Starter anglais US/japonais/français		B6960IA/J/F				
licence seule	1 x cellule		B6961BA	B6961CA	B6951BA	B6951CA
jeu de DVD	comprend 3 DVD	B6960MA				

2. extensions lecteurs et bibliothèques		ttes plates-formes	Windows, NetWare, Linux	SAN, UNIX, NAS
licence lecteur	1 x lecteur		B6963AA	B6953AA
licence bibliothèque	1 x 61-250/empl. illimités	B6957BA/B6958BA		
	1 x mise à niv. emp. illim.	B6958CA		

3. extensions fonctionnelles		ttes plates-formes	Windows et Linux		UNIX
manuels papier extensions fonctionnelles US/jap.		B6960EA/J			
licence sauv. en ligne	1 x système		B6965BA		B6955BA
licence cryptage	1 x 1/10 serveurs	BB618AA/BA			
licence MoM	1 x système		B6966AA		B6956AA
licence sauv. av. disque	1 x To/10 x To/100 x To	B7038AA/BA/CA			
licence sauv. sur IAP	1 x To	TA030AA			
licence sauv. fich. ouv.	1 x serveur d'entreprise	BA155AA			
	1 x 1 serv./1 x 10 serv.	BA153AA/BA			
lic. opérations supports	1 x 2 000/10 000 supp.	B7100AA/B7101AA			
	1 x nbre illim. supports	B7102AA			
	CD uniq./manuels uniq.	B7129AA/B7128AA			
		NDMP	HP XP	HP EVA	EMC
licence ZDB	1 x To /10 x To		B7023CA/DA	B7025CA/DA	B6959CA/DA
licence restaur. instant.	1 x To /10 x To		B7026CA/DA	B7028AA/DA	
licence sauv. directe	1 x To /10 x To	B7022BA/DA	B7027AA/DA		

édition serveur unique	Windows	HP-UX	Solaris
licence et supports / licence seule	B7030AA/BA	B7020AA/BA	B7020DA/CA
migration vers Pack Starter	B7031AA	B7021AA	B7021DA

Figure 55 - Structure du produit HP Data Protector

Les nouveaux numéros de produits dans le tableau ci-dessus sont indiqués en rouge.

Data Protector utilise les numéros de produits des versions précédentes de Data Protector. C'est la raison pour laquelle les licences Data Protector existantes restent valides après la migration. Pour plus d'informations sur les licences disponibles, reportez-vous à la section "Structure de produit et licences de Data Protector A.06.10" à la page 349.

A propos des mots de passe

Vous trouverez ci-après des éléments qui vous aideront à déterminer le nombre de mots de passe dont vous avez besoin.

- Les mots de passe temporaires sont utilisables sur tout candidat à un Gestionnaire de cellule. En revanche, pour tous les autres types de mots de passe, vous devez déterminer la plate-forme correspondante. Cela s'applique également au Gestionnaire de cellule, qui deviendra le système d'administration central de Data Protector. Il est important d'utiliser des mots de passe temporaires pour appréhender parfaitement les besoins de votre configuration de cellule avant de demander un mot de passe permanent.
- Les licences permanentes peuvent être déplacées vers un autre Gestionnaire de cellule. En revanche, vous devez utiliser le ou les formulaires de déplacement de licence et les envoyer au *Centre de remise de mots de passe HP (PDC)*.
- Les mots de passe sont installés sur le Gestionnaire de cellule et sont valides pour l'intégralité de la cellule.

- La gestion centralisée des licences est assurée par la fonctionnalité Manager-of-Managers (MoM). Si vous achetez plusieurs licences pour différentes cellules, vous pouvez les installer sur le système MoM.
- Vous devez disposer d'une licence de Gestionnaire de cellule pour chaque cellule.
- Le logiciel vérifie que les licences sont toujours valables chaque fois que vous effectuez une tâche de configuration Data Protector ou que vous démarrez une session de sauvegarde.
- Les mots de passe temporaires sont utilisables sur tout système, tandis que les mots de passe d'évaluation et permanents ne sont utilisables que sur le système du Gestionnaire de cellule pour lequel vous avez demandé les licences.
- Si le système sur lequel le Gestionnaire de cellule est installé dispose de plusieurs adresses IP (systèmes multirésidents, serveurs RAS, clusters), vous pouvez lier la licence à n'importe laquelle de ces adresses IP.

REMARQUE :

Si vous avez prévu de modifier l'adresse IP du Gestionnaire de cellule, de déplacer le Gestionnaire de cellule sur un autre système ou de déplacer les licences d'une cellule à une autre (et que vous n'utilisez pas la fonctionnalité MoM), vous devez contacter le *Centre de remise de mot de passe HP (PDC)* pour mettre vos licences à jour. Consultez la section "Autres moyens d'obtenir et d'installer des mots de passe permanents" à la page 325 pour connaître la procédure à suivre pour contacter le Centre de remise de mot de passe HP.

Mots de passe Data Protector

Une fois Data Protector installé sur votre réseau, vous pouvez l'utiliser pendant 60 jours. A l'issue de cette période, vous devez installer un mot de passe permanent sur le Gestionnaire de cellule afin d'activer le logiciel. Vous pouvez charger le logiciel sur le Gestionnaire de cellule Data Protector, mais vous ne pouvez pas effectuer de tâches de configuration sans mot de passe permanent, car les licences requises pour cette fonctionnalité Data Protector particulière requièrent ce type de mot de passe.

Les licences Data Protector requièrent l'un des mots de passe suivants :

- Mot de passe temporaire
  Un mot de passe temporaire est généré pour le produit lors de sa première installation. Vous pouvez utiliser le logiciel pendant 60 jours à compter de son installation sur tout système pris en charge par Data Protector. Au cours de cette période, vous devez demander un mot de passe permanent au *Centre de remise de mot de passe HP (PDC)* et l'installer.
- Mots de passe permanents
  Data Protector est livré avec une licence *Attestation de droit* qui vous donne le droit d'obtenir un mot de passe permanent. Ce mot de passe vous permet de configurer une cellule Data Protector en fonction de votre stratégie de

sauvegarde, à condition que vous ayez acheté les licences requises. Avant de demander un mot de passe permanent, vous devez déterminer quel système sera utilisé pour le Gestionnaire de cellule et définir la configuration nécessaire.

- Mot de passe d'urgence
  Les mots de passe d'urgence sont disponibles si les mots de passe installés ne correspondent pas à la configuration système en raison d'une urgence. Ils permettront à tout système de fonctionner pendant une période de 120 jours. Les mots de passe d'urgence sont délivrés par l'organisation de support. Ils doivent être demandés par les collaborateurs HP et ne sont remis qu'à ces derniers. Reportez-vous à votre centre de support ou à au centre HP d'attribution des licences à l'adresse : http://webware.hp.com.
  Les mots de passe d'urgence sont conçus pour permettre des opérations de sauvegarde tandis que la configuration système originale est reconstruite ou jusqu'à ce que l'installation soit déplacée vers un nouvel emplacement permanent. En cas de déplacement des licences, vous devez remplir un formulaire de déplacement de licence et l'adresser au *Centre de remise de mot de passe HP (PDC)* ou consulter la page Web http://webware.hp.com sur laquelle les mots de passe peuvent être générés, déplacés, etc.

Il est recommandé de demander les mots de passe à l'aide de l'utilitaire HP AutoPass, qui peut être installé pendant le processus d'installation du Gestionnaire de cellule. Reportez-vous à la section "Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP AutoPass" à la page 322 pour connaître les instructions sur l'obtention de mots de passe avec l'utilitaire HP AutoPass une fois ce dernier installé pendant le processus d'installation du Gestionnaire de cellule.

Reportez-vous à la section "Autres moyens d'obtenir et d'installer des mots de passe permanents" à la page 325 pour des instructions sur l'obtention et l'installation d'un mot de passe par un autre moyen que via l'utilitaire HP AutoPass.

Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP AutoPass

L'utilitaire HP AutoPass permet d'installer directement via Internet des mots de passe pour les licences achetées pour vos produits HP, à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus d'informations sur l'utilitaire HP AutoPass, reportez-vous à l'aide en ligne de HP AutoPass.

Configuration système requise

Pour obtenir et installer des mots de passe permanents à l'aide de l'utilitaire HP AutoPass, vous devez remplir les conditions suivantes :

- Installez l'utilitaire HP AutoPass avec le Gestionnaire de cellule. Si vous n'avez pas installé cet utilitaire sur votre système avant d'installer Data Protector, vous pouvez le faire à l'aide du script `omnisetup.sh` (systèmes UNIX) ou pendant l'installation du Gestionnaire de cellule (systèmes Windows).

- Installez Java Runtime Environment (JRE) 1.5.0_06 ou toute version supérieure sur le Gestionnaire de cellule.
- Sur MC/ServiceGuard, l'utilitaire HP AutoPass doit être installé sur tous les noeuds.
- Vous devez disposer d'une attestation de droit d'une licence permanente.
- Vous devez disposer du numéro de commande HP pour les licences achetées.
- Vous avez besoin de l'adresse IP du Gestionnaire de cellule du système Manager-of-Managers.
- Avant d'installer AutoPass sur HP-UX 11.23 (Itanium), vérifiez que les correctifs suivants sont installés :
  - PHSS_36343 1.0 aC++ Runtime (IA : A.06.15, PA : A.0376)
  - PHSS_37039 1.0 Integrity Unwind Library

Limites

Les limites suivantes s'appliquent à l'utilitaire HP AutoPass :

- L'utilitaire HP AutoPass n'est pas installé sur les systèmes d'exploitation Windows 2003 x64, Windows Vista x64, Windows Server 2008 x64 et Linux.
- Il *n'est pas* recommandé d'installer HP AutoPass sur Microsoft Cluster, car il ne serait installé que sur un seul noeud et non sur tous.
- La commande `omniinstlic` ne fonctionne que si JRE 1.5.0_06 (ou une version supérieure) est installé sur le Gestionnaire de cellule.

Pour plus d'informations sur les conditions requises et les limitations, reportez-vous à l'aide en ligne HP AutoPass.

Les mots de passe sont installés sur le Gestionnaire de cellule et sont valides pour l'intégralité de la cellule.

Procédure

Pour obtenir et installer un mot de passe permanent, procédez comme suit :

1. Rassemblez les informations nécessaires à l'obtention d'un mot de passe permanent. Consultez l'aide en ligne HP AutoPass pour connaître les informations requises.

2. Commandez le mot de passe en ligne à l'aide de l'*utilitaire HP AutoPass*. Pour lancer l'*utilitaire HP AutoPass*, exécutez la commande suivante sur le Gestionnaire de cellule :

REMARQUE :

Dans un environnement Manager-of-Managers (MoM), la commande `omniinstlic` doit être exécutée soit sur le système MoM (si vous *utilisez* une attribution centralisée des licences Data Protector), soit sur le Gestionnaire de cellule auquel les mots de passe commandés et installés sont destinés (si vous *n'utilisez pas* l'attribution centralisée des licences Data Protector).

`/opt/omni/sbin/omniinstlic` (Gestionnaire de cellule UNIX) ou

`répertoire_Data_Protector``\bin\omniinstlic` (Gestionnaire de cellule Windows)

Reportez-vous à la page man de `omniinstlic` pour plus d'informations.

3. Suivez les instructions de l'assistant de l'*utilitaire HP AutoPass* et saisissez les informations requises.

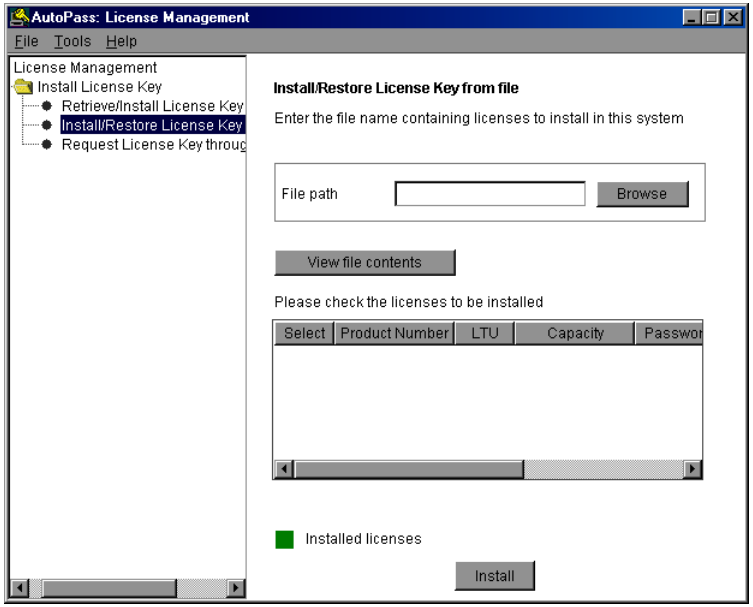

Figure 56 - Assistant HP AutoPass

A la dernière étape de l'assistant, cliquez sur Obtenir mot de passe pour transférer les mots de passe permanents des licences achetées du *Centre de remise de mot de passe HP* vers le Gestionnaire de cellule.

Cliquez sur Terminer pour installer les mots de passe permanents des licences achetées sur le Gestionnaire de cellule.

4. Pour plus d'informations sur la vérification des mots de passe installés, reportez-vous à la section "Vérification du mot de passe" à la page 328.

Autres moyens d'obtenir et d'installer des mots de passe permanents

Obtention

Pour obtenir des mots de passe permanents, procédez comme suit :

1. Regroupez les informations demandées dans le *Formulaire de demande* de mot de passe permanent. Reportez-vous à la section "Formulaires d'attribution de licences Data Protector" à la page 369 pour trouver l'emplacement des formulaires et obtenir des instructions pour les remplir.

2. Pour plus d'informations sur la structure des produits, reportez-vous à la section "Structure de produit et licences de Data Protector A.06.10" à la page 349. Le *Centre de remise de mot de passe HP* vous enverra un mot de passe permanent en utilisant la méthode dont vous vous êtes servi pour envoyer votre demande. Si vous avez fait votre demande par e-mail, par exemple, vous recevrez votre mot de passe permanent par e-mail.
3. Choisissez l'une des options suivantes :
   - Consultez le site Web du *Centre de remise de mot de passe* à l'adresse http://www.webware.hp.com.
   - Remplissez le *Formulaire de demande de mot de passe permanent* et adressez-le au *Centre de remise de mot de passe HP* à l'aide d'une des méthodes suivantes (reportez-vous à l'attestation de droit livrée avec le produit pour connaître les numéros de téléphone et de télécopie, les adresses e-mail et les horaires d'ouverture) :
     - En envoyant le formulaire par télécopie au *Centre de remise de mot de passe HP*
     - En envoyant un e-mail au *Centre de remise de mot de passe HP*
       Vous pouvez également utiliser la version électronique des formulaires de licence qui se trouve dans les fichiers suivants sur le Gestionnaire de cellule et les supports de distribution :
       - Avec le Gestionnaire de cellule Windows : `répertoire_Data_Protector\Docs\license_forms.txt`
       - Avec le Gestionnaire de cellule UNIX : `/opt/omni/doc/C/license_forms_UNIX`
       - Sur le DVD-ROM d'installation Windows : `Nom_disque:\Docs\license_forms.txt`

       pour "copier" et "coller" votre message au *Centre de remise de mot de passe HP (HP PDC)*.
       Votre mot de passe permanent vous sera envoyé dans les 24 heures suivant l'envoi du *Formulaire de demande de mot de passe permanent.*

Installation

Les paragraphes qui suivent indiquent la procédure à suivre pour installer un mot de passe permanent transmis par le *Centre de remise de mot de passe HP (HP PDC)* :

Condition préalable

Le *Centre de remise de mot de passe HP* doit vous avoir envoyé les mots de passe permanents et l'interface utilisateur Data Protector doit être installée sur le Gestionnaire de cellule. Les mots de passe sont installés sur le Gestionnaire de cellule et sont valides pour l'intégralité de la cellule.

Utilisation de l'interface graphique utilisateur

Pour installer le mot de passe permanent via l'interface graphique de Data Protector, procédez comme suit :

1. Dans le menu contextuel, cliquez sur Clients.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur Cellule Data Protector, puis sélectionnez Ajouter licence.
3. Vous devez saisir le mot de passe exactement tel qu'il figure dans le *Certificat de mot de passe*.

   Un mot de passe se compose de 8 groupes de 4 caractères chacun, séparés par un espace et suivis par une chaîne. Assurez-vous que cette séquence ne contient ni saut de ligne, ni retour chariot. Vous trouverez ci-après un exemple de mot de passe :

   `2VFF 9WZ2 C34W 43L7 RYY7 HBYZ S9MQ 1LZA JUUQ TA48 EPNB QFRN MR9F 2A2A 7UEG 9QR3 Y3QW LZA9 AZA9 EQ97 "Produit;` Gestionnaire de cellule UNIX"

   Après avoir saisi le mot de passe, effectuez les vérifications suivantes :

   - Assurez-vous que le mot de passe s'affiche correctement à l'écran.
   - Vérifiez qu'il n'y a pas d'espace en tête ou à la fin du mot de passe, ni de caractères en trop.
   - Vérifiez que vous n'avez pas confondu les caractères "1" (le chiffre) et "l" (la lettre).
   - Vérifiez que vous n'avez pas confondu les caractères "O" (lettre majuscule) et "0" (chiffre).
   - Vérifiez que vous avez utilisé la bonne casse. Le mot de passe tient compte de la casse.

   Cliquez sur OK.

Le mot de passe est enregistré dans le fichier suivant sur le Gestionnaire de cellule :

- Sous Windows Server 2008 : *donnes_programme_Data_Protector*`\Config\server\Cell\lic.dat`
- Sur les autres systèmes Windows : *répertoire_Data_Protector*`\Config\server\Cell\lic.dat`
- Sur les systèmes UNIX : `/etc/opt/omni/server/cell/lic.dat`

Utilisation de l'interface de ligne de commande

Pour installer le mot de passe permanent via l'interface de ligne de commande (CLI) de Data Protector, procédez comme suit :

1. Connectez-vous au Gestionnaire de cellule.

2. Exécutez la commande suivante :
   - Sous Windows : *répertoire_Data_Protector*\bin\omnicc -install_license *mot de passe*
   - Sous UNIX : /opt/omni/bin/omnicc -install_license *mot de passe*

   Le *mot de passe* doit être saisi tel qu'il apparaît dans le *Certificat de mot de passe*. Il doit figurer sur une seule ligne et ne contenir aucun caractère de retour chariot. Le mot de passe doit être placé entre apostrophes. Si le mot de passe comporte également une description entre apostrophes, ces dernières doivent être précédées d'une barre oblique inverse. Pour plus d'informations et consulter un exemple, reportez-vous à la page omnicc du manuel.

Vous pouvez également ajouter le mot de passe dans le fichier suivant sur le Gestionnaire de cellule :

- Sous Windows Server 2008 : *donnes_programme_Data_Protector*\config\server\cell\lic.dat
- Sur les autres systèmes Windows : *répertoire_Data_Protector*\config\server\cell\lic.dat
- Sur les systèmes UNIX : /etc/opt/omni/server/cell/lic.dat

Si ce fichier n'existe pas, créez-en un avec un éditeur tel que vi ou Bloc-notes. Vous trouverez un exemple de mot de passe à l'Étape 3 à la page 327 de la procédure faisant appel à l'interface graphique utilisateur.

Vérification du mot de passe

Utilisation de l'interface graphique utilisateur

Pour vérifier que le mot de passe pour la licence que vous avez installée est correct, procédez comme suit dans l'interface graphique utilisateur de Data Protector :

1. Dans le menu Aide, cliquez sur A propos de.
2. Cliquez sur l'onglet Licence. Toutes les licences installées s'affichent. Si le mot de passe que vous avez saisi n'est pas correct, il est accompagné de la remarque Impossible de décoder le mot de passe.

Utilisation de l'interface de ligne de commande

Pour vérifier que le mot de passe pour la licence que vous avez installée est correct, utilisez la commande suivante :

- Sous Windows : *répertoire_Data_Protector*\bin\omnicc -password_info
- Sous UNIX : /opt/omni/bin/omnicc -password_info

Cette commande affiche toutes les licences installées. Si le mot de passe que vous avez saisi n'est pas correct, il est accompagné de la remarque `Impossible de décoder le mot de passe.`

Recherche du nombre de licences installées

Utilisation de l'interface graphique utilisateur

Après avoir installé un mot de passe permanent, vous pouvez vérifier le nombre de licences actuellement installées sur le Gestionnaire de cellule :

1. Démarrez le gestionnaire Data Protector.
2. Dans la barre de menus, cliquez sur Aide, puis sur A propos. La fenêtre A propos du Gestionnaire affiche alors les licences installées.

Utilisation de l'interface de ligne de commande

Si vous utilisez la ligne de commande, procédez comme suit :

1. Connectez-vous au Gestionnaire de cellule.
2. Exécutez la commande suivante :
   - Sous Windows : *répertoire_Data_Protector*`\bin\omnicc -query`
   - Sous UNIX : `/opt/omni/bin/omnicc -query`

Un tableau contenant les licences installées s'affiche alors.

Déplacement des licences vers un autre système Gestionnaire de cellule

Vous devez contacter le *Centre de remise de mot de passe HP* dans les cas suivants :

- Lorsque vous souhaitez déplacer le Gestionnaire de cellule vers un autre système.
- Lorsque vous prévoyez de déplacer vers une autre cellule Data Protector une licence installée sur un Gestionnaire de cellule qui n'est pas utilisé dans la cellule.

REMARQUE :

Il est possible de déplacer une licence UNIX vers un autre Gestionnaire de cellule UNIX ou vers un Gestionnaire de cellule Windows ; en revanche, il est impossible de déplacer une licence Windows vers un Gestionnaire de cellule UNIX.

Procédez comme suit pour déplacer des licences d'un Gestionnaire de cellule vers un autre :

1. Remplissez un *Formulaire de déplacement de licence* pour chaque nouveau Gestionnaire de cellule et envoyez-le au *Centre de remise de mot de passe HP*. Si vous souhaitez déplacer des licences correspondant à des produits qui ne sont plus en vente, utilisez les *formulaires de déplacement de licence* fournis avec la version précédente du produit. Reportez-vous à la section "Formulaires d'attribution de licences Data Protector" à la page 369.

   Dans le formulaire, vous devez spécifier le nombre de licences à déplacer du Gestionnaire de cellule existant.

2. Supprimez le fichier suivant :
   - Sous Windows Server 2008 : `donnes_programme_Data_Protector\config\server\cell\lic.dat`
   - Sur les autres systèmes Windows : `répertoire_Data_Protector\config\server\cell\lic.dat`
   - Sur les systèmes UNIX : `/etc/opt/omni/server/cell/lic.dat`

3. Après avoir rempli le *formulaire de déplacement de licence*, envoyez-le au *Centre de remise de mot de passe HP*. Vous êtes dans l'obligation légale de supprimer tous les mots de passe Data Protector du Gestionnaire de cellule courant.

4. Installez les nouveaux mots de passe. Vous recevrez un mot de passe pour chaque nouveau Gestionnaire de cellule. Vous recevrez également un nouveau mot de passe pour le Gestionnaire de cellule courant si des licences sont conservées sur celui-ci. Le nouveau mot de passe remplace le mot de passe utilisé sur le Gestionnaire de cellule courant.

Gestion centralisée des licences

Data Protector vous permet de configurer la gestion centralisée des licences pour l'environnement multicellules dans son intégralité, ce qui simplifie considérablement la gestion des licences. Toutes les licences sont conservées sur le système Manager-of-Managers (MoM) Manager. Elles sont ensuite allouées aux cellules spécifiques tout en restant configurées sur le Gestionnaire MoM.

Pour plus d'informations sur la procédure de configuration des licences, reportez-vous à l'aide en ligne de Data Protector.

REMARQUE :

Il est possible d'affecter une licence UNIX à un autre Gestionnaire de cellule UNIX ou à un Gestionnaire de cellule Windows ; en revanche, il est impossible d'affecter une licence Windows à un Gestionnaire de cellule UNIX.

La fonction MoM vous permet de déplacer (réaffecter) les licences entre les cellules MoM. Pour plus d'informations, recherchez l'entrée suivante dans l'index de l'aide en ligne : "environnement MoM".

Si vous installez une nouvelle licence Data Protector, n'oubliez pas de vérifier la fonctionnalité MoM avant de demander des licences. Si vous décidez d'utiliser la gestion centralisée de licences par la suite, vous devrez appliquer la procédure de déplacement des licences dans son intégralité.

REMARQUE :

La fonction MoM permet de gérer les licences de manière centralisée. Cela signifie que vous pouvez installer toutes les licences sur le Gestionnaire MoM, puis les distribuer aux Gestionnaires de cellule qui appartiennent à la cellule du MoM. Par la suite, les licences peuvent être déplacées (redistribuées) entre les cellules du MoM. Pour plus d'informations, recherchez l'entrée suivante dans l'index de l'aide en ligne : "environnement MoM".

Outil de commande Data Protector

Data Protector comprend un outil simple permettant de générer automatiquement la liste des numéros de produits Data Protector requis pour votre environnement. Cet outil vous guide tout au long de la procédure : grâce à des questions simples concernant votre configuration système et l'utilisation envisagée, il est en mesure de déterminer la structure de votre cellule en fonction des réponses que vous lui avez données.

Une fois que vous avez répondu à toutes les questions, l'outil de commande affiche la liste complète des numéros de produits que vous devez commander pour l'environnement élaboré sur la base de vos réponses. Si vous souhaitez voir un exemple, reportez-vous à la Figure 57 à la page 332.

L'outil de commande est disponible sur les DVD Data Protector.

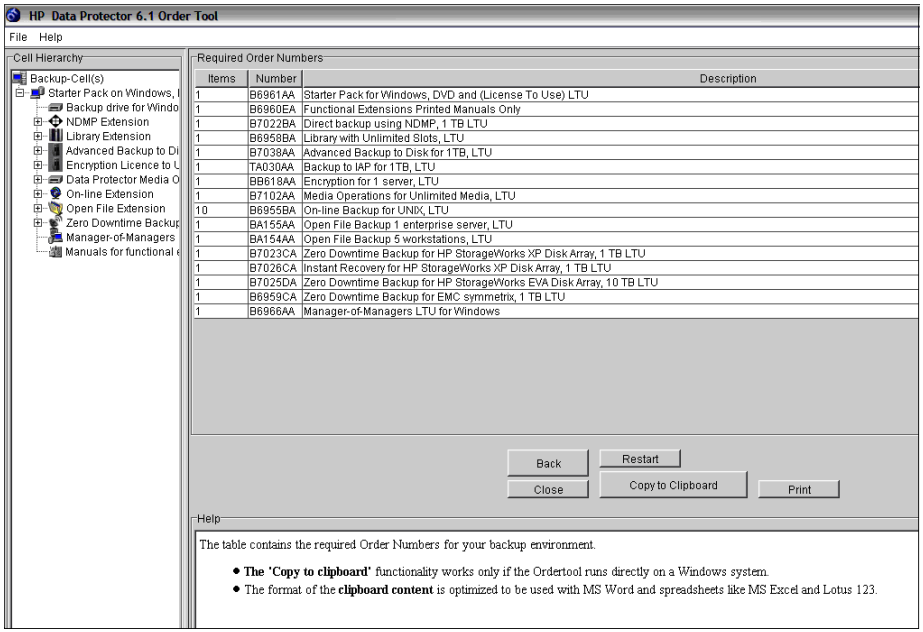

Figure 57 - Exemple de résultats fournis par l'outil de commande Data Protector

6 Résolution des problèmes d'installation

Description du chapitre

Ce chapitre contient des informations relatives aux problèmes d'installation. Vous trouverez des informations générales sur la résolution de problèmes dans *le Guide de dépannage HP Data Protector*.

Ce chapitre contient des informations sur les éléments suivants :

- "Problèmes de résolution de noms lors de l'installation du Gestionnaire de cellule Windows" à la page 333
- "Vérification des connexions DNS dans la cellule Data Protector" à la page 334
- "Résolution des problèmes d'installation et de mise à niveau de Data Protector" à la page 336
- "Résolution des problèmes d'installation du Gestionnaire de cellule Data Protector sous Solaris" à la page 338
- "Résolution des problèmes d'installation des clients UNIX" à la page 340
- "Vérification de l'installation du client Data Protector" à la page 342
- "Résolution des problèmes de la mise à niveau" à la page 343
- "Utilisation des fichiers journaux" à la page 345
- "Création de traces d'exécution de l'installation" à la page 347

Problèmes de résolution de noms lors de l'installation du Gestionnaire de cellule Windows

Au cours de l'installation du Gestionnaire de cellule Data Protector sous Windows, Data Protector détecte toute configuration erronée du DNS ou du fichier LMHOSTS et vous en avertit. De plus, Data Protector vous envoie une notification si le protocole TCP/IP n'est pas installé sur le système.

Problème

Echec de la résolution de noms avec le DNS ou le fichier LMHOSTS

Si la résolution de noms échoue, le message `"Erreur lors du développement du nom d'hôte"` s'affiche et l'installation est abandonnée.

- Si un problème de résolution survient lorsque vous utilisez le DNS, un message d'avertissement relatif à votre configuration DNS actuelle s'affiche.
- Si un problème de résolution survient lorsque vous utilisez le fichier LMHOSTS, un message d'avertissement s'affiche, vous invitant à vérifier le paramétrage de ce fichier.
- Si vous n'avez configuré ni l'un ni l'autre (DNS ou LMHOSTS), un message d'avertissement s'affiche pour activer le DNS ou la résolution LMHOSTS dans la boîte de dialogue des propriétés TCP/IP.

Action

Vérifiez la configuration du DNS ou du fichier LMHOSTS, ou activez-la. Reportez-vous à la section "Vérification des connexions DNS dans la cellule Data Protector" à la page 334.

Problème

Le protocole TCP/IP n'est pas installé et configuré sur votre système.

Data Protector utilise le protocole TCP/IP pour les communications réseau ; celui-ci doit donc être installé et configuré sur chaque client de la cellule. Dans le cas contraire, l'installation est abandonnée.

Action

Vérifiez la configuration TCP/IP. Pour plus d'informations, reportez-vous à la section "Modification du numéro de port par défaut de Data Protector" à la page 398.

Vérification des connexions DNS dans la cellule Data Protector

Le DNS (Domain Name System) est un service de noms pour les hôtes TCP/IP. Le DNS est configuré avec une liste de noms d'hôtes et d'adresses IP, ce qui permet aux utilisateurs de désigner les systèmes distants par des noms d'hôtes plutôt que par des adresses IP. Le DNS garantit le bon fonctionnement des communications entre membres de la cellule Data Protector.

Si le DNS n'est pas correctement configuré, des problèmes de résolution de noms peuvent survenir dans la cellule Data Protector et les membres ne seront pas en mesure de communiquer les uns avec les autres.

Data Protector fournit la commande `omnicheck` pour vérifier les connexions DNS entre membres de la cellule Data Protector. Même si cette commande permet de vérifier toutes les connexions possibles dans la cellule, il suffit de vérifier les connexions suivantes, essentielles à la cellule Data Protector :

- Du Gestionnaire de cellule vers tout autre membre de la cellule et vice versa

- De l'Agent de support vers tout autre membre de la cellule et vice versa

Utilisation de la commande omnicheck

Limites

- La commande vérifie uniquement les connexions entre membres de la cellule, et non les connexions DNS en général.
- Elle ne peut être utilisée que sur les clients Data Protector sur lesquels Data Protector A.05.10 (ou une version ultérieure) est installé. Si la commande rencontre un client disposant d'une version antérieure de Data Protector, elle envoie un message d'erreur et reprend au client suivant.

La commande `omnicheck` réside dans le répertoire suivant du Gestionnaire de cellule :

Windows : `répertoire_Data_Protector\bin`

UNIX : `/opt/omni/bin`

Le synopsis de la commande omnicheck est le suivant :

```
omnicheck -dns [-host Client | -full] [-verbose]
```

Les différentes options vous permettent de vérifier les connexions DNS suivantes dans la cellule de Data Protector :

- Pour vous assurer que le Gestionnaire de cellule et que chaque Agent de support présent dans la cellule résolve correctement les connexions DNS vers chaque client Data Protector de la cellule et vice versa, exécutez la commande suivante :
  `omnicheck -dns [-verbose]`
- Pour vérifier qu'un client Data Protector particulier résout correctement les connexions DNS avec chaque client Data Protector de la cellule, exécutez la commande suivante :
  `omnicheck -dns -host client [-verbose]`
  où *`client`* est le nom du client Data Protector vérifié.
- Pour vérifier toutes les connexions DNS possibles dans la cellule, exécutez la commande suivante :
  `omnicheck -dns -full [-verbose]`

Lorsque l'option `[-verbose]` est spécifiée, la commande retourne tous les messages. Si cette option n'est pas définie (réglage par défaut), seuls les messages résultant d'échecs de vérification sont retournés.

Pour plus d'informations, reportez-vous à la page `omnicheck` du manuel.

Le Tableau 13 à la page 336 répertorie les messages retournés pour la commande `omnicheck`. Si le message retourné indique un problème de résolution DNS, reportez-vous au chapitre "Dépannage du réseau et de la communication" dans le Guide de dépannage HP Data Protector.

Tableau 13 - Messages retournés

Message renvoyé	Signification
client_1 ne peut pas se connecter à *client_2*	Délai de connexion à *client_2* dépassé.
client_1 se connecte à *client_2*, mais le système connecté se présente comme *client_3*	Le fichier *%SystemRoot%*\Sys-tem32\drivers\etc\hosts/etc/hosts (systèmes UNIX) sur le *client_1* n'est pas correctement configuré ou le nom d'hôte du *client_2* ne correspond pas à son nom DNS.
client_1 n'a pas pu se connecter à *client_2*	*client_2* est inaccessible (c'est-à-dire déconnecté) ou le fichier *%SystemRoot%*\Sys-tem32\drivers\etc\hosts (systèmes Windows) ou /etc/hosts (systèmes UNIX) n'est pas correctement configuré sur *client_1*.
vérification de la connexion entre *client_1* et *client_2*	
toutes les vérifications se sont terminées correctement.	
nb_vérifications_non_réussies échecs de vérification.	
le client n'est pas membre de la cellule.	
le client a été contacté, mais il s'agit apparemment d'une version antérieure. Le nom d'hôte n'est pas vérifié.	

Résolution des problèmes d'installation et de mise à niveau de Data Protector

Problème

L'un des messages d'erreur suivants s'affiche :

- Le service Windows Installer est inaccessible.
- Cette application doit être installée pour que le programme s'exécute.
- Impossible d'ouvrir ce package de correctifs.

- `Impossible d'ouvrir le périphérique ou le fichier spécifié.`

Après l'installation ou la mise à niveau vers Data Protector A.06.10, Windows peut signaler que certaines applications ne sont pas installées ou qu'il est nécessaire de les réinstaller.

Ce problème est dû à une erreur de la procédure de mise à niveau de Microsoft Installer. Les données de la version 1.x de Microsoft Installer n'ont pas été transférées vers la version 2.x de Microsoft Installer que Data Protector installe sur l'ordinateur.

Action

Ce problème est décrit à l'article Q324906 de la base de connaissances Microsoft.

Problème

Gestionnaire de cellule Echec de l'installation d'un Gestionnaire de cellule sur un système Windows qui ne fait partie d'aucun domaine Windows

Le message d'erreur suivant s'affiche :

`Impossible de faire correspondre le mot de passe et le nom de compte spécifié.`

Actions

Deux solutions possibles :

- Associer le système Windows sur lequel vous installez le Gestionnaire de cellule à un domaine.
- Utiliser le compte administrateur local pour le service CRS.

Problème

Le message d'erreur suivant s'affiche :

`Fichier msvcr71.dll introuvable`

Impossible de trouver la bibliothèque `MSVCR71.dll` (en majuscules), car il n'y a que `msvcr71.dll` (en minuscules) sur le partage réseau. Comme `MSVCR71.dll` et `msvcr71.dll` sont traités comme des fichiers différents, `setup.exe` n'arrive pas à trouver la bonne `dll`.

Action

Renommez le fichier `msvcr71.dll` (minuscules) en `MSCVCR71.dll` (majuscules) ou reconfigurez le partage réseau de façon à ce qu'il ne soit plus sensible à la casse.

Problème

L'annulation de l'installation ne désinstalle pas des composants déjà installés

Si vous annulez l'installation de Data Protector alors que certains composants ont déjà été installés, Data Protector ne les désinstalle pas. L'installation se termine en affichant un message d'erreur.

Action

Désinstallez manuellement les composants déjà installés après avoir annulé l'installation.

Problèmes lors de l'installation à distance des clients Windows

Problème

Erreur lors du lancement du processus d'installation

Lorsque vous utilisez l'installation à distance Data Protector pour mettre à jour les clients Windows, le message d'erreur suivant s'affiche :

```
Erreur au démarrage du processus d'installation, err=[1326]
Accès réseau refusé : nom d'utilisateur inconnu ou mauvais mot
de passe.
```

Le problème est que le service `Inet Data Protector` fonctionne sur l'ordinateur distant sous un compte utilisateur qui ne dispose pas d'un accès au partage OmniBack sur l'ordinateur du Serveur d'installation. Il s'agit très probablement d'un utilisateur local.

Action

Remplacez l'utilisateur pour le service `Inet Data Protector` par un utilisateur qui puisse accéder au partage Data Protector.

Résolution des problèmes d'installation du Gestionnaire de cellule Data Protector sous Solaris

Problème

Impossible de créer un répertoire temporaire

Lors de l'installation de Gestionnaire de cellule sous Solaris, un répertoire temporaire ne peut être créé et l'installation échoue avec le message d'erreur suivant :

```
Processing package instance OB2-CORE from /tmp/
DP_A0510_158_SUN78.pkg
```

```
pkgadd : ERREUR : unable to make temporary directory
//tmp/old//installR.aOj3
```

Action

Créez manuellement le répertoire temporaire manquant à l'emplacement indiqué dans le message d'erreur et redémarrez la procédure d'installation.

Par exemple, si vous obtenez le message d'erreur ci-dessus, créez le répertoire suivant : `//tmp/old//installR.aOj3`.

Résolution des problèmes d'installation des clients UNIX

Problème

Echec de l'installation à distance de clients UNIX

L'installation ou la mise à niveau à distance d'un client UNIX échoue avec le message d'erreur suivant :

```
Installation/Upgrade session finished with errors.
```

Lors de l'installation ou de la mise à niveau à distance de clients UNIX, l'espace disque disponible sur un système client dans le dossier `/tmp` doit atteindre au moins la taille du plus gros package à installer. Sur les systèmes client Solaris, la même quantité d'espace disque doit également être disponible dans le répertoire `/var/tmp`.

Action

Vérifiez si vous disposez de suffisamment d'espace disque dans ces répertoires et redémarrez la procédure d'installation ou de mise à niveau.

Pour connaître l'espace disque nécessaire, reportez-vous au document *Références, notes de publication et annonces produits HP Data Protector*.

Problème

Problèmes d'installation d'un client HP-UX

Lorsque vous ajoutez un nouveau client HP-UX à une cellule Data Protector, le message d'erreur suivant s'affiche :

```
/tmp/omni_tmp/packet: vous ne disposez pas des autorisations
requises pour exécuter cette fonction SD...
```

```
Accès refusé à root pour démarrer l'agent sur le dépôt
enregistré /tmp/omni_tmp/packet. Insertion non autorisée sur
l'hôte.
```

Action

Arrêtez le démon `swagent` et relancez-le, soit en supprimant le processus, soit en le redémarrant à l'aide de la commande `/opt/omni/sbin/swagentd` ou `/opt/omni/sbin/swagentd -r`.

Vérifiez que vous disposez d'une entrée de bouclage local (localhost) dans le fichier hosts (`/etc/hosts`).

Problème

Impossible de démarrer Omniinet après l'installation du Gestionnaire de cellule UNIX

Au démarrage du Gestionnaire de cellule, le message d'erreur suivant s'affiche :

```
ERREUR : Impossible de démarrer le service "omniinet", erreur
système : [1053] erreur inconnue 1053.
```

Action

Vérifiez que le service `inetd` ou `xinetd` est en cours d'exécution :

HP-UX et Solaris: `ps -ef | grep inetd`

Linux : `ps -ef | grep xinetd`

Pour démarrer le service, exécutez :

HP-UX : `/usr/sbin/inetd`

Solaris : `/usr/sbin/inetd -s`

Linux : `rcxinetd start`

Résolution des problèmes d'installation des clients Windows XP

Problème

Echec de l'installation à distance de clients Windows

Lorsqu'un système Windows XP est membre d'un groupe de travail et que la stratégie de sécurité Partage de fichiers simple est activée, les utilisateurs qui tentent d'accéder au système par le réseau sont obligés d'utiliser le compte Invité. Lors d'une installation à distance d'un client Data Protector, Data Protector demande à plusieurs reprises un nom d'utilisateur et un mot de passe valides car les droits de l'administrateur sont nécessaires pour l'installation à distance.

Action

Désactivez le partage de fichiers simple comme suit : dans Windows XP, ouvrez l'Explorateur Windows ou Poste de travail, sélectionnez le menu Outils, cliquez sur l'option Options des dossiers, puis sur l'onglet Affichage et décochez l'option Utiliser le partage de fichiers simple (recommandé).

La stratégie Partage de fichiers simple est ignorée :

- lorsque l'ordinateur est membre d'un domaine,
- lorsque le paramètre de stratégie de sécurité `Accès réseau : modèle de partage et de sécurité pour les comptes locaux` a la valeur `Classique : les utilisateurs locaux s'identifient eux-mêmes`

Résolution des problèmes d'installation des clients Windows Vista et Windows Server 2008

Problème

Echec de l'installation à distance de clients Windows

Echec de l'installation à distance d'un client Data Protector sur un système Windows Vista ou Windows Server 2008 avec le message d'erreur suivant :

```
[Normal] Connexion au client ordinateur.société.com...
```

```
[Normal] Terminé.
```

```
[Normal] Installation du service d'amorçage Data Protector sur
le client ordinateur.société.com...
```

```
[Critique] Impossible de se connecter au Gestionnaire de
contrôle des services sur le client ordinateur.société.com: [5]
Accès refusé.
```

Action

1. Sur le Serveur d'installation, exécutez la commande suivante pour indiquer un compte utilisateur du groupe local Administrateurs du système d'exploitation que le Serveur d'installation doit utiliser lors de l'installation à distance :
   `omniinetpasswd -inst_srv_user` *`utilisateur@domaine`*
   Notez que le compte utilisateur doit déjà être ajouté à la configuration Inet locale. Pour plus d'informations, reportez-vous à la description de la commande `omniinetpasswd` dans le *Guide de rfrence de l'interface de ligne de commande HP Data Protector*.
2. Relancez l'installation à distance du client Data Protector.

Vérification de l'installation du client Data Protector

La vérification de l'installation du client Data Protector se divise en plusieurs étapes :

- Vérification de la configuration DNS des systèmes Gestionnaires de cellule et clients, puis vérification que les résultats de la commande `omnicheck -dns` du système Gestionnaire de cellule et client correspondent au système spécifié.
- Vérification des composants logiciels installés sur le client.
- Comparaison de la liste des fichiers requis pour un composant logiciel particulier à installer avec celle des fichiers présents sur le client.
- Vérification du total de contrôle pour chaque fichier en lecture seule requis pour un composant logiciel particulier.

Condition préalable

Un Serveur d'installation doit être disponible pour le type de système client (UNIX, Windows) sélectionné.

Limites

La procédure de vérification ne s'applique pas aux clients Novell NetWare et MPE.

Pour vérifier une installation Data Protector à l'aide de l'interface graphique utilisateur de Data Protector :

1. Dans le menu contextuel, cliquez sur Clients.
2. Dans la fenêtre de navigation, développez Clients, cliquez sur le système du Gestionnaire de cellule avec le bouton droit de la souris, puis cliquez sur Vérifier installation pour lancer l'assistant.
3. Suivez les instructions de l'assistant pour vérifier l'installation des systèmes dans la cellule. La fenêtre Vérifier installation s'affiche avec les résultats de l'installation.

   Reportez-vous à l'aide en ligne pour plus d'informations.

Si votre installation a échoué, reportez-vous à la section "Utilisation des fichiers journaux" à la page 345.

Pour plus d'informations sur la vérification de l'installation sur les systèmes UNIX à l'aide de l'interface en ligne de commande de Data Protector, reportez-vous à la page `ob2install` du manuel.

Résolution des problèmes de la mise à niveau

Problème

Les fichiers de la base de données IDB et de configuration ne sont plus disponibles après la mise à niveau

Après la mise à niveau du Gestionnaire de cellule à partir d'une version précédente, la base IDB ainsi que tous les fichiers de configuration ne sont pas disponibles. Ce problème survient en cas d'interruption de la procédure de mise à niveau, quelle qu'en soit la raison.

Action

Restaurez Data Protector à partir de la sauvegarde effectuée avant la mise à niveau, éliminez la raison de l'interruption et redémarrez la mise à niveau.

Problème

Les anciens correctifs Data Protector ne sont pas supprimés après la mise à niveau

Les anciens correctifs Data Protector sont répertoriés dans la liste des programmes installés si vous exécutez la commande `swlist` une fois la mise à niveau Data Protector terminée. Les correctifs ont été supprimés du système au cours de la mise à niveau, mais restent dans la base de données sw.

Pour savoir quels correctifs Data Protector sont installés, reportez-vous à la section "Contrôle des correctifs Data Protector installés" à la page 228.

Action

Pour supprimer les anciens correctifs de la base de données sw, exécutez la commande suivante :

```
swmodify -u correctif.\* correctif
```

Par exemple, pour supprimer le correctif "`PHSS_30143`" de la base de données sw, exécutez la commande suivante :

```
swmodify -u PHSS_30143.\* PHSS_30143
```

Problème

La taille maximale des fichiers de base de données dépasse 2 Go

Sous HP-UX 11.23 et 11.31 (Itanium) et sous SuSE Linux (x86-64), la taille maximale des fichiers de base de données (`dirs.dat`, `fnames.dat`, `fn?.ext` et leurs fichiers d'extension) peut dépasser la taille maximale par défaut de 2 Go. Par conséquent, lors d'une mise à niveau vers Data Protector A.06.10, un message d'avertissement s'affiche pour inviter à régler la taille maximale des fichiers de base de données :

```
Exécutez omnidbutil -modifytblspace pour régler la taille
maximale des fichiers de base de données.
```

Action

Vous devez effectuer cette opération après la mise à niveau, car la procédure de réglage de la taille maximale des fichiers de base de données peut s'avérer gourmande en temps et en espace, selon la taille de la base de données. Tant que le réglage n'est pas effectué, Data Protector A.06.10 signale des tailles d'espace de table incorrectes comme c'est le cas dans la version A.06.00. Toutefois, il reste possible d'exécuter une sauvegarde et une restauration.

REMARQUE :

Vérifiez que l'espace disque disponible est suffisant avant de lancer le réglage. Vous avez besoin d'un espace disponible supplémentaire au moins égal à la taille actuelle de la base de données que vous allez exporter.

Prévoyez un temps suffisant pour l'ensemble de l'opération. L'exportation et l'importation de la base de données peuvent prendre beaucoup de temps (jusqu'à plusieurs jours, selon la complexité et la taille de la base de données) et vous ne pouvez pas effectuer de sauvegarde ou de restauration pendant l'exportation et l'importation.

Pour résoudre le problème, procédez comme suit :

1. Effectuez une sauvegarde réussie de l'ensemble de l'IDB.
2. Exportez l'IDB dans un répertoire temporaire existant :
   `omnidbutil -writedb -mmdb` *`répertoireMMDB`* `-cdb` *`répertoireCDB`*
   où *`répertoireCDB`* et *`répertoireMMDB`* sont des répertoires temporaires vers lesquels les éléments CDB et MMDB sont exportés.
3. Initialisez l'IDB :
   `omnidbinit`
4. Ajoutez le nombre requis de fichiers d'extension pour le fichier d'espace de table :
   `omnidbutil -extendtblspace` *`nom_fichier_espace_table nom_chemin`* `-maxsize` *`taille_mo`*
   Par exemple, si la taille du fichier `fnames.dat` est de 7 Go, vous devez ajouter trois fichiers d'extension avec une taille maximale de 2047 Mo en exécutant la même commande trois fois :
   ```
   omnidbutil -extendtblspace fnames.dat /var/opt/omni/
   server/db40/datafiles/cdb -maxsize 2047
   omnidbutil -extendtblspace fnames.dat /var/opt/omni/
   server/db40/datafiles/cdb -maxsize 2047
   omnidbutil -extendtblspace fnames.dat /var/opt/omni/
   server/db40/datafiles/cdb -maxsize 2047
   ```

Ces commandes créent trois fichiers d'extension, `fnames.dat1`, `fnames.dat2` et `fnames.dat3`.

5. Réglez la taille maximale des fichiers de base de données existants :
   `omnidbutil –modifytblspace`
   Suivant l'exemple ci-dessus, `fnames.dat`, qui atteignait auparavant une taille de 7 Go, est maintenant limité à 2 Go.
6. Importez l'IDB :
   `omnidbutil -readdb -mmdb` *`répertoireMMDB`* `-cdb` *`répertoireCDB`*
   Si vous n'avez pas créé un nombre suffisant de fichiers d'extension, la commande `omnidbutil` se termine avec le message suivant :
   `Mémoire insuffisante pour l'espace de table` *`nom_espace_table`*.
   Ajoutez le nombre requis de fichiers d'extension et relancez l'opération d'importation.
7. Une fois le réglage réussi, supprimez les fichiers temporaires.

Procédure de mise à niveau manuelle

Normalement, vous mettez à niveau les Gestionnaire de cellule et Serveur d'installation Data Protector A.05.10, Data Protector A.05.50 ou Data Protector A.06.00 UNIX en exécutant la commande `omnisetup.sh`, qui effectue une procédure automatique de mise à niveau. Il est toutefois possible d'effectuer une mise à niveau manuelle. Reportez-vous à la section "Mise à niveau sur des systèmes HP-UX, Solaris et Linux à l'aide d'outils natifs" à la page 388.

Utilisation des fichiers journaux

Si l'installation de Data Protector pose un problème, vous pouvez consulter l'un des fichiers journaux suivants pour le diagnostiquer :

- Journaux d'installation (Windows)
- Journaux système (UNIX)
- Fichiers journaux Data Protector

En cas de problème lors de l'installation, vous devrez consulter les fichiers journaux correspondant à votre type d'installation (en local ou à distance) et au système d'exploitation que vous utilisez.

Installation en local

Si vous rencontrez des difficultés lors d'une installation en local, reportez-vous aux fichiers journaux suivants :

HP-UX Gestionnaire de cellule:

- `/var/adm/sw/swinstall.log`
- `/var/adm/sw/swagent.log` (pour plus d'informations)

Sur le Gestionnaire de cellule Solaris et Linux :

`/var/opt/omni/log/debug.log`

Clients Windows (sur le système sur lequel tourne le programme d'installation) :

- *Temp*\SetupLog.log
- *Temp*\OB2DBG_*did*__setup_*Hôte*_*num_débogage*_setup.txt (pour plus d'informations)
  où :
  - *did* (ID de débogage) est l'ID de processus du premier processus acceptant les paramètres de débogage. Cet ID est également l'ID de la session de débogage. Tous les autres processus utiliseront cet ID.
  - *Hôte* est le nom de l'hôte sur lequel le fichier de trace est créé.
  - *num_débogage* est un numéro généré par Data Protector.
- *TEMP*\CLUS_DBG_*num_débogage*.TXT (dans des environnements de clusters)

L'emplacement du répertoire *Temp* est spécifié par la variable d'environnement TEMP. Pour connaître la valeur de cette variable, exécutez la commande `set`.

Installation distante

Si vous rencontrez des difficultés lors d'une installation à distance, reportez-vous aux fichiers journaux suivants :

UNIX Serveur d'installation:

`/var/opt/omni/log/IS_install.log`

Clients Windows (uniquement sur le système client à distance) :

- *SystemRoot*\TEMP\OB2DBG_*did*_INSTALL_SERVICE_*num_débogage*_debug.txt
- *SystemRoot*\TEMP\CLUS_DBG_*num_débogage*.TXT

où *Temp* est un répertoire spécifié dans la variable d'environnement TEMP et *SystemRoot* est un répertoire spécifié dans la variable d'environnement SystemRoot.

Si les fichiers journaux n'ont pas été créés, exécutez l'installation à distance avec l'option de débogage. Reportez-vous à la section "Création de traces d'exécution de l'installation" à la page 347.

Fichiers journaux Data Protector

Les fichiers journaux Data Protector répertoriés ci-dessous se trouvent dans :

Windows Vista, Windows Server 2008 :
donnes_programme_Data_Protector\log

Autres systèmes Windows : `répertoire_Data_Protector\log`

HP-UX, Solaris et Linux : `/var/opt/omni/log` et `/var/opt/omni/server/log`

Autres systèmes UNIX : `/usr/omni/log`

Novell NetWare : `SYS:\USR\OMNI\LOG`

Les fichiers journaux suivants sont importants pour la résolution des problèmes d'installation :

`debug.log`	Contient des conditions inattendues. Bien que certaines pourront vous servir, ces informations sont surtout destinées au service de support.
`inet.log`	Contient des demandes effectuées auprès du service `inet` Data Protector. Il peut être utile pour contrôler les dernières activités de Data Protector sur les clients.
`IS_install.log`	Contient une trace d'installation à distance et se trouve sur le Serveur d'installation.
`omnisv.log`	Contient des informations relatives au démarrage et à l'arrêt des services Data Protector.
`upgrade.log`	Ce journal est créé lors de la mise à niveau et contient des messages relatifs à la mise à niveau de la partie centrale (UCP) et à la mise à niveau de la partie concernant les détails (UDP).
`OB2_Upgrade.log`	Ce fichier, créé lors de la mise à niveau, contient les traces de la procédure de celle-ci.

Pour obtenir des informations sur d'autres fichiers journaux, reportez-vous au *Guide de dépannage HP Data Protector*.

Création de traces d'exécution de l'installation

Exécutez l'installation avec l'option `debug` si le service support clientèle HP vous le demande. Pour plus d'informations sur le débogage, notamment sur les options de débogage ci-dessous, et sur la préparation des données à envoyer au service support clientèle HP, reportez-vous *au Guide de dépannage HP Data Protector*.

Windows :

Pour déboguer une installation à distance sur un système Windows, exécutez l'interface graphique utilisateur de Data Protector en utilisant l'option de débogage :

`Manager -debug 1-99 Suffixe_débogage`

Une fois la session terminée/abandonnée, récupérez les résultats du débogage dans les fichiers suivants :

- Sur le système du Serveur d'installation :
  donnes_programme_Data_Protector\tmp\OB2DBG_*did*__BM_*NomHôte_NumDébogage_SuffixeDébogage* (Windows Server 2008)
  répertoire_Data_Protector\tmp\OB2DBG_*did*__BM_*NomHôte_NumDébogage_SuffixeDébogage* (autres systèmes Windows)
- Sur le système distant :
  SystemRoot:\Temp\OB2DBG_*did*__INSTALL_SERVICE_*Hôte_num_débogage_Suffixe_débogage*

UNIX :

Pour procéder au débogage de l'installation sur un système UNIX, exécutez l'interface graphique utilisateur de Data Protector en utilisant l'option de débogage :

`xomni -debug 1-99 Suffixe_débogage`

ou

`xomniadmin -debug 1-99 Suffixe_débogage`

Une fois la session terminée/abandonnée, récupérez les résultats du débogage dans le répertoire `tmp` du système Serveur d'installation.

A Annexe A

Structure de produit et licences de Data Protector A.06.10

Cette annexe décrit la structure du produit Data Protector en détails afin de faciliter la commande et le repérage des numéros de produit.

La structure du produit se divise en différentes sections, comme l'indique la Figure 58 à la page 350. Lorsque vous commandez une solution Data Protector, suivez la procédure suivante :

1. sélectionnez un Pack Starter. Le numéro de produit approprié dépend du système d'exploitation de votre Gestionnaire de cellule.
2. Déterminez le nombre de lecteurs configurés dans votre environnement et les bibliothèques de bandes associées.
3. Identifiez les autres fonctions dont vous avez besoin. Les licences recommandées peuvent concerner aussi bien la fonction de sauvegarde en ligne que .

Vous devez au moins vous procurer une licence et des supports Pack Starter.

REMARQUE :

Les licences fournies pour les produits UNIX peuvent s'appliquer à tous les systèmes d'exploitation.

1. Packs Starter	(obligatoire)	ttes plates-formes	Windows	Linux	HP-UX	Solaris
licence et DVD	1 x cellule	B6960IA/J/F	B6961AA	B6961DA	B6951AA	B6951DA
manuels papier Pack Starter anglais US/japonais/français						
licence seule	1 x cellule		B6961BA	B6961CA	B6951BA	B6951CA
jeu de DVD	comprend 3 DVD	B6960MA				

2. extensions lecteurs et bibliothèques		ttes plates-formes	Windows, NetWare, Linux	SAN, UNIX, NAS
licence lecteur	1 x lecteur		B6963AA	B6953AA
licence bibliothèque	1 x 61-250/empl. illimités	B6957BA/B6958BA		
	1 x mise à niv. emp. illim.	B6958CA		

3. extensions fonctionnelles		ttes plates-formes	Windows et Linux	UNIX
manuels papier extensions fonctionnelles US/jap.		B6960EA/J		
licence sauv. en ligne	1 x système		B6965BA	B6955BA
licence cryptage	1 x 1/10 serveurs	BB618AA/BA		
licence MoM	1 x système		B6966AA	B6956AA
licence sauv. av. disque	1 x To/10 x To/100 x To	B7038AA/BA/CA		
licence sauv. sur IAP	1 x To	TA030AA		
licence sauv. fich. ouv.	1 x serveur d'entreprise	BA155AA		
	1 x 1 serv./1 x 10 serv.	BA153AA/BA		
lic. opérations supports	1 x 2 000/10 000 supp.	B7100AA/B7101AA		
	1 x nbre illim. supports	B7102AA		
	CD uniq./manuels uniq.	B7129AA/B7128AA		

		NDMP	HP XP	HP EVA	EMC
licence ZDB	1 x To /10 x To		B7023CA/DA	B7025CA/DA	B6959CA/DA
licence restaur. instant.	1 x To /10 x To		B7026CA/DA	B7028AA/DA	
licence sauv. directe	1 x To /10 x To	B7022BA/DA	B7027AA/DA		

édition serveur unique	Windows	HP-UX	Solaris
licence et supports / licence seule	B7030AA/BA	B7020AA/BA	B7020DA/CA
migration vers Pack Starter	B7031AA	B7021AA	B7021DA

Figure 58 - Structure du produit HP Data Protector

Les nouveaux numéros de produits dans le tableau ci-dessus sont indiqués en rouge.

Packs Starter

Le Tableau 14 à la page 350 contient les numéros de licence des Packs Starter Data Protector A.06.10.

Tableau 14 - Numéros de licence des Packs Starter HP Data Protector

B6951AA	DVD et licence d'utilisation pour HP-UX
B6951BA	Licence d'utilisation uniquement pour HP-UX
B6951DA	DVD et licence d'utilisation pour Sun Solaris
B6951CA	Licence d'utilisation uniquement pour Sun Solaris
B6961AA	DVD et licence d'utilisation pour Windows
B6961BA	Licence d'utilisation uniquement pour Windows
B6961DA	DVD et licence d'utilisation pour Linux
B6961CA	Licence d'utilisation uniquement pour Linux

B6960MA B6960LA	Kit DVD Manuels Pack Starter - imprimés (anglais)
B6960LJ	Manuels Pack Starter - imprimés (japonais)
B6960LF	Manuels Pack Starter - imprimés (français)

La licence d'utilisation du Pack Starter inclut une licence pour les éléments suivants :

- Un Gestionnaire de cellule sur la plate-forme indiquée
- Un nombre illimité d'Agents de sauvegarde sur n'importe quelle plate-forme
- Une licence Lecteur (B6951xx contient 1xB6953AA et B6961xx contient 1xB6963AA)
- La gestion de supports intégrée
- Les bibliothèques comportant 60 emplacements au maximum
- Les options de récupération après sinistre
- La génération avancée de rapports (dans l'interface graphique utilisateur de Data Protector et via le Web)
- Le support SAN (avec le Gestionnaire de cellule sous HP-UX ou Solaris)
- La gestion centrée service via les intégrations au logiciel HP

Supports

Data Protector A.06.10 est livré sur deux DVD (UNIX et Windows). Si vous avez besoin de CD, il existe aussi un kit CD (B6960MB) qui contient 15 CD. Il est toutefois recommandé d'utiliser le kit DVD.

Manuels

Tous les manuels sont disponibles sur les DVD, les CD et sur le site http://www.hp.com/support/manuals.

Vous pouvez commander des manuels imprimés avec les deux options suivantes : Pack Starter et Extensions fonctionnelles. Les manuels Pack Starter imprimés comportent :

- *Guide conceptuel HP Data Protector*
- *Guide d'installation et de choix des licences HP Data Protector*
- *Guide de dépannage HP Data Protector*
- *Guide de récupération aprs sinistre HP Data Protector*
- *Références, notes de publication et annonces produits HP Data Protector*

REMARQUE :

Après avoir passé commande en utilisant les numéros de produits correspondant au DVD et à la licence d'utilisation, vous recevez un coffret DVD qui contient les DVD, la licence d'utilisation et le *Guide de démarrage rapide HP Data Protector*. Cette livraison ne comprend pas d'autres manuels imprimés. Les manuels sont disponibles au format électronique sur le DVD ou à l'adresse http://www.hp.com/support/manuals et peuvent également être commandés séparément.

Extensions de lecteur et de bibliothèque

Les licences suivantes concernent un seul lecteur. Vous avez besoin d'autant de licences que de lecteurs utilisés à tout moment. Il s'agit généralement du nombre total de lecteurs configurés, ce qui permet une utilisation simultanée de tous les lecteurs. Un lecteur de sauvegarde peut être un lecteur de bande, une unité logique sur disque (sauvegarde sur disque à l'aide d'un périphérique de fichier) ou un lecteur magnéto-optique. Il est possible d'accéder au lecteur et de le gérer en local ou via le réseau à partir d'un système disposant de n'importe quelle licence Data Protector. Les licences de lecteurs ne peuvent pas être partagées entre plusieurs cellules. Pour connaître les lecteurs pris en charge, reportez-vous aux matrices de support Data Protector sous Specifications à l'adresse http://www.hp.com/support/manuals.

Le Tableau 15 à la page 352 contient le numéro de licence des extensions de lecteur Data Protector A.06.10 et le Tableau 17 à la page 353 celui des extensions de bibliothèque Data Protector A.06.10.

Tableau 15 - Extensions de lecteur HP Data Protector

B6953AA	pour SAN, UNIX et NAS

Comprend la licence d'utilisation (LTU) pour un lecteur de sauvegarde connecté directement à un système UNIX, un périphérique NAS, utilisé dans un environnement SAN ou pour la sauvegarde sans serveur.

Les lecteurs connectés aux systèmes MPE et OpenVMS de HP requièrent cette licence.

Cette licence d'utilisation est également requise pour les configurations suivantes :

Systèmes NAS gérés via NDMP (par exemple, les serveurs de fichiers Network Appliance et EMC Celerra) ou systèmes NAS nécessitant un serveur de périphérique propriétaire Data Protector (Agent de support), HP Storage Works NAS 8000, par exemple.

Les systèmes NAS sous Windows, NetWare ou Linux standard pouvant exécuter un serveur de périphérique Data Protector standard (Agent de support) requièrent uniquement des extensions de lecteur Data Protector pour Windows, NetWare et Linux (B6963AA).

Elle peut aussi être utilisée pour les lecteurs uniques connectés à des systèmes Windows, NetWare et Linux. Toutefois, dans les cas où le lecteur n'est pas utilisé dans un SAN, la licence B6963AA constitue une solution plus économique.

Tableau 16 - Extensions de lecteur HP Data Protector

B6963AA	pour Windows, NetWare et Linux

Comprend la licence d'utilisation (LTU) pour un lecteur de sauvegarde supplémentaire connecté directement à un système Windows, NetWare ou Linux (Intel).

Cette licence est valable pour les lecteurs connectés à des périphériques NAS sous Windows, NetWare ou Linux qui peuvent exécuter un Agent de support Data Protector standard.

Vous avez besoin d'autant de licences que de lecteurs utilisés à tout moment. Il s'agit généralement du nombre total de lecteurs configurés permettant une utilisation simultanée de tous les lecteurs.

Pour connaître les lecteurs pris en charge, reportez-vous aux matrices de support Data Protector sous Specifications à l'adresse www.hp.com/go/dataprotector.

Tableau 17 - Extensions de bibliothèque HP Data Protector

B6957BA	pour les bibliothèques de 61 à 250 emplacements
B6958BA	pour les bibliothèques avec un nombre illimité d'emplacements
B6958CA	licence de mise à niveau avec nombre illimité d'emplacements

La licence d'utilisation des extensions de bibliothèque inclut la licence pour la gestion des bibliothèques de bandes dans une cellule Data Protector. Vous devez disposer d'une licence par bibliothèque.

- Les silos StorageTek utilisant les systèmes de bibliothèque ACSLS et GRAU/EMASS et utilisant le DAS requièrent la licence B6958BA.
- Dans le cas où plusieurs cellules se partagent une bibliothèque, la licence d'utilisation Manager-of-Managers est requise pour chaque cellule afin qu'une seule licence couvre la bibliothèque sur toutes les cellules.
- Cette licence prend en compte les emplacements physiques à l'intérieur de la bibliothèque et non les emplacements logiques.
- Les bibliothèques permettant de créer des partitions virtuelles nécessitent également une licence basée sur le nombre d'emplacements physiques disponibles par bibliothèque physique.
  Exemples :
  - Une bibliothèque de 120 emplacements utilisée dans une seule cellule divisée en deux bibliothèques de 60 emplacements nécessite une licence B6957BA.

- Une bibliothèque de 300 emplacements partagée par trois cellules (sans Manager-of-Managers) utilisant chacune 100 emplacements nécessite une licence B6957BA pour chaque cellule.
- Une bibliothèque de 300 emplacements partagée par cinq cellules (sans Manager-of-Managers) utilisant chacune 60 emplacements ne nécessite aucune licence de bibliothèque.
- Une bibliothèque de 300 emplacements partagée par trois cellules utilisant chacune 100 emplacements et gérées de façon centralisée via Manager-of-Managers avec gestion centrale des supports et des licences, nécessite une licence B6958BA pour toutes les cellules.

Pour connaître les lecteurs pris en charge, reportez-vous aux matrices de support Data Protector sous Specifications à l'adresse http://www.hp.com/support/manuals.

Extensions fonctionnelles

Les tableaux de cette section contiennent les numéros de licence des extensions fonctionnelles Data Protector A.06.10.

Tableau 18 - Extension en ligne HP Data Protector

B6955BA	pour UNIX
B6965BA	pour Windows ou Linux

La licence d'utilisation de l'extension de sauvegarde en ligne inclut la licence nécessaire pour effectuer la sauvegarde en ligne des bases de données et des applications qui s'exécutent sur la plate-forme spécifiée.

- Si un système exécute plusieurs partitions, cette licence d'utilisation est requise pour chaque partition.
- Dans un environnement de clusters, chaque système participant au cluster doit disposer de cette licence d'utilisation.
- Dans une configuration Oracle Real Application Cluster (RAC), une licence en ligne est requise pour chaque noeud de cluster sur lequel un Agent d'application est installé.
- Cette licence est requise pour chaque noeud pour lequel une base de données Oracle DataGuard en attente est configurée dans Data Protector.
- Les licences de sauvegarde en ligne sont requises pour les sauvegardes avec temps d'indisponibilité nul (ZDB).
- Prise en charge de la fonctionnalité d'image instantanée VSS (Volume Shadow copy Service) du système de fichiers Windows 2003 sans supplément de prix. Cependant, les bases de données de sauvegarde, qui ne font pas partie du système d'exploitation, requièrent cette extension de sauvegarde en ligne. La sauvegarde de la configuration système ne requiert pas d'extension de sauvegarde en ligne.

- Cette licence d'utilisation est requise pour la sauvegarde de la boîte aux lettres unique Microsoft Exchange.
- Pour les solutions VMware Consolidated Backup (VCB) et VMware ESX Server, une licence Windows/Linux est requise par serveur ESX, VCB Proxy et VMware Virtual Center participant au processus de sauvegarde et de restauration. Aucune licence de sauvegarde en ligne n'est requise pour la sauvegarde VCB et ESX Server basée sur les scripts.
- Cette licence d'utilisation n'est pas requise pour la sauvegarde en ligne HP Network Node Manager.
- Cette licence d'utilisation n'est pas requise pour la sauvegarde en ligne HP Systems Insight Manager.

Pour connaître les bases de données prises en charge, reportez-vous aux matrices de support Data Protector à l'adresse http://www.hp.com/support/manuals.

Tableau 19 - Extension de sauvegarde des fichiers ouverts HP Data Protector

BA153AA	1 serveur
BA153BA	10 serveurs
BA154AA	5 stations de travail
BA155AA	1 serveur d'entreprise
BA152AA	CD

La licence d'utilisation de l'extension de sauvegarde des fichiers ouverts inclut la licence pour la sauvegarde de fichiers ouverts d'applications, les bases de données et les fichiers e-mail (par exemple, `.pst` - fichiers Microsoft Outlook) exécutés sur des serveurs spécifiés qui ne sont pas couverts par les matrices d'intégration et de plates-formes Data Protector.

Le CD est inclus dans le Pack Starter Data Protector. Il peut également être commandé séparément via BA152AA (qui inclut le CD de sauvegarde de fichiers ouverts).

Pour connaître les configurations prises en charge, reportez-vous aux matrices de support Data Protector à l'adresse http://www.hp.com/support/manuals.

Tableau 20 - Extension Manager-of-Managers HP Data Protector

B6956AA	pour UNIX
B6966AA	pour Windows ou Linux

La licence d'utilisation de l'extension Manager-of-Managers inclut la licence requise pour que chaque serveur de gestion (Gestionnaire de cellule) Data Protector qui s'exécute sur la plate-forme spécifiée s'intègre à un environnement Manager-of-Managers.

Vous devez disposer de cette licence pour le partage de bibliothèques de bandes entre plusieurs cellules Data Protector. Cette solution est idéale pour la gestion de sauvegarde centralisée de filiales.

Le produit B6956AA peut aussi être utilisé pour un Gestionnaire de cellule Windows. Il est toutefois plus économique d'opter pour le produit B6966AA.

Tableau 21 - Extension HP Data Protector Media Operations

B7100AA	Niveau Entrée
B7101AA	Entreprise
B7102AA	Illimité
B7128AA	Manuels
B7129AA	Supports

- Le niveau Entrée inclut la licence d'utilisation pour 2000 supports, un serveur de gestion et un nombre illimité de clients.
- Le niveau Entreprise inclut la licence d'utilisation pour 10 000 supports, un serveur de gestion et un nombre illimité de clients.
- Le niveau Illimité inclut la licence d'utilisation pour un nombre illimité de supports, un serveur de gestion et un nombre illimité de clients.
- Le niveau Supports correspond au nombre total de supports à bande consignés dans la base de données interne Data Protector Media Operations. Vous pouvez utiliser n'importe quelle combinaison de licences des niveaux Entrée et Entreprise afin de correspondre avec le nombre total de bandes à consigner.
- Le CD-ROM Data Protector Media Operations est inclus dans le Pack Starter Data Protector, mais peut également être commandé séparément via B7129AA.
- Les manuels Data Protector Media Operations sont inclus dans le pack de manuels Extensions fonctionnelles Data Protector, mais peuvent être commandés séparément via B7128AA.

Tableau 22 - Extension de sauvegarde avancée sur disque HP Data Protector

B7038AA	pour 1 To
B7038BA	pour 10 To
B7038CA	pour 100 To

Comprend la licence d'utilisation pour 1 To d'espace de sauvegarde sur disque. Licence requise par capacité native utilisable d'espace de sauvegarde sur disque en teraoctets (To).

- La licence de sauvegarde avancée sur disque est requise pour pouvoir réaliser une sauvegarde sur une bibliothèque de fichiers Data Protector et peut être

utilisée pour une sauvegarde sur bibliothèque de bandes virtuelle à la place des licences d'utilisation de lecteurs.

- La capacité native utilisable d'une bibliothèque de fichiers Data Protector correspond à la taille sur disque de tous les fichiers utilisés pour la bibliothèque de fichiers, telle que l'indique le système de fichiers.
  - Sauvegarde complète virtuelle et sauvegarde complète synthétique Data Protector : les sauvegardes complètes virtuelles et les sauvegardes incrémentales à consolider en sauvegarde complète synthétique/virtuelle doivent être stockées dans la bibliothèque de fichiers Data Protector qui requiert cette licence.
- La capacité native utilisable d'une bibliothèque de bandes virtuelle correspond à la taille sur disque de la bibliothèque de bandes virtuelle utilisée par toutes les sauvegardes Data Protector protégées, telle que l'indique la bibliothèque.
  - Si la bibliothèque dispose de la fonction intégrée pour migrer des données de sauvegarde du cache de disque vers un disque ou une bande plus économique, la capacité de stockage migrée doit faire l'objet d'une licence complète. Aucune licence de lecteur et de bibliothèque n'est requise pour la bibliothèque de bandes contrôlée exclusivement par la bibliothèque de bandes virtuelle, mais la capacité utilisée de toutes les bandes de la bibliothèque physique doit faire l'objet d'une licence. Dans ces cas, il peut s'avérer plus économique d'adopter le modèle de licence de lecteur de bandes (références B6953AA et B6963AA). Ceci ne s'applique pas si la copie d'objet Data Protector a servi à migrer les données de sauvegarde vers un autre disque ou une autre bande.
  - Pour chaque bibliothèque de bandes virtuelle, vous pouvez choisir d'utiliser le modèle de licence de sauvegarde sur disque ou sur lecteur de bandes. Les deux modèles ne doivent pas être combinés dans une même bibliothèque.
  - Par défaut, Data Protector traite les bibliothèques de bandes virtuelles comme des bibliothèques ordinaires (comme les bibliothèques SCSI II par exemple). Pour pouvoir utiliser les licences de sauvegarde avancée sur disque, il faut que le périphérique soit identifié comme bibliothèque de bandes virtuelle lors de sa configuration. Pour plus d'informations, recherchez dans l'index de l'aide en ligne : "bibliothèque de bandes virtuelle".
  - Si la licence a été achetée avant le 1er juillet 2008, HP s'engage à une pleine protection des investissements. En d'autres termes, vous pouvez choisir d'utiliser la licence pour la bibliothèque de bandes virtuelle selon les anciennes conditions : la capacité native utilisable d'une bibliothèque de bandes virtuelle correspond à l'espace occupé par les sauvegardes protégées et les miroirs et copies de sauvegarde protégés selon la base de données interne de Data Protector. Pour que la gestion des licences des bibliothèques de bandes virtuelles reste simple, un taux de compression hypothétique de 2 pour 1 est appliqué pour les bibliothèques de ce type sans supplément de prix. Le maintien du modèle précédent n'a de sens que si vous n'utilisez pas une technologie de compression ou de déduplication. Sinon, vous obtenez

une solution plus avantageuse en utilisant des licences achetées auparavant selon le nouveau modèle de licence.

  - Si Data Protector utilise exclusivement la bibliothèque de bandes virtuelle, il est conseillé d'acquérir une licence pour une quantité correspondant à la capacité physique de la bibliothèque de bandes virtuelle. HP parle de "capacité native utilisable" pour désigner la capacité physique de la bibliothèque de bandes virtuelle. D'autres fournisseurs parlent de "capacité brute".
  - Aucune licence Data Protector supplémentaire n'est requise pour la réplication de la bibliothèque de bandes virtuelle.

- Avec ce concept d'attribution de licences en fonction de la taille sur disque, il n'est pas nécessaire de prendre en compte les taux de compression et de déduplication, ni la configuration RAID.
- 1 To = 1024 Go, 1 Go = 1024 Mo, 1 Mo = 1024 Ko, 1 Ko = 1024 octets
- Dans le cas de la gestion centrale des licences avec le Gestionnaire MoM, au moins 1 To doit être affecté à chaque cellule via la fonctionnalité de sauvegarde avancée sur disque.

REMARQUE :

Data Protector n'est pas en mesure d'indiquer le nombre requis de licences car les bibliothèques de bandes virtuelles actuelles et certains serveurs de fichiers hébergeant la bibliothèque de fichiers Data Protector ne disposent pas des interfaces et des outils adéquats. L'utilisateur est responsable d'acquérir une licence couvrant la capacité en fonction des définitions de licence. Lorsque vous commandez une nouvelle capacité d'espace de sauvegarde, vérifiez toujours que les licences Data Protector disponibles couvrent la capacité de votre infrastructure de sauvegarde.

Exemples :

- Une baie de disques de sauvegarde avec une capacité native utilisable totale de 2,5 To, entièrement utilisée pour la sauvegarde avancée sur disque, requiert 3 licences B7038AA.
- Une baie de disques de sauvegarde avec une capacité brute totale de 2,5 To, entièrement configurée en RAID 1 (mise en miroir), a seulement une capacité native utilisable de 1,25 To et ne requiert que deux licences B7038AA si elle est entièrement utilisée pour la sauvegarde avancée sur disque.
- Deux baies de disques de sauvegarde avec une capacité native utilisable totale de 2,5 To chacune, entièrement utilisées pour la sauvegarde avancée sur disque, nécessitent 5 licences B7038AA.
- Dix serveurs lame avec une capacité native utilisable de 0,75 To chacun, entièrement utilisés pour la sauvegarde avancée sur disque, requièrent huit licences B7038AA (en fait, il serait plus économique d'acquérir une licence B7038BA (10 To)).

- Une bibliothèque de bandes virtuelle avec une capacité de disque utilisable de 10 To et contrôlant 90 To de données de sauvegarde sur bandes requiert une licence B7038CA (100 To).

Tableau 23 - Extension de sauvegarde sur HP IAP HP Data Protector

TA030AA	pour 1 To

Comprend la licence d'utilisation pour 1 To d'espace d'archivage sur disque. Licence requise par capacité native utilisable d'espace d'archivage sur disque en teraoctets (To).

- La licence de sauvegarde sur HP IAP est requise pour pouvoir réaliser une sauvegarde sur HP Integrated Archive Platform (IAP).
- La capacité native utilisable correspond à l'espace utilisable du système de fichiers selon le système d'exploitation sous-jacent.
- La capacité utilisable se distingue de la capacité brute en ce qu'elle exclut le surdébit RAID. Cela signifie qu'il n'est pas nécessaire de prendre en compte la configuration RAID.
- Aucune licence d'utilisation de lecteur ou de bibliothèque n'est requise.
- Aucun supplément de prix n'est demandé pour la compression au niveau de la capacité native utilisable. La compression peut être assurée par le système d'exploitation sous-jacent. C'est également le cas pour l'instanciation unique.
- Aucune licence supplémentaire n'est requise pour la réplication vers une autre plate-forme HP IAP à l'aide de la technologie de réplication intégrée HP IAP.
- Dans le cas de la gestion centrale des licences avec le Gestionnaire MoM, au moins 1 To doit être affecté à chaque cellule via la fonctionnalité de sauvegarde sur HP IAP.

Exemple :

Une plate-forme HP IAP avec une capacité native utilisable totale de 2,5 To, entièrement utilisée pour la sauvegarde sur HP IAP avec instanciation unique et offrant un stockage de 100 To de données non compressées, requiert trois licences TA030AA.

Tableau 24 - Extension de sauvegarde avec temps d'indisponibilité nul (ZDB) HP Data Protector

B7023CA	pour HP StorageWorks Disk Array XP, 1 To
B7023DA	pour HP StorageWorks Disk Array XP, 10 To
B7025CA	pour HP StorageWorks Enterprise Virtual Array, 1 To
B7025DA	pour HP StorageWorks Enterprise Virtual Array, 10 To
B6959CA	pour EMC Symmetrix / DMX, 1 To
B6959DA	pour EMC Symmetrix / DMX, 10 To

La licence d'utilisation de l'extension de sauvegarde avec temps d'indisponibilité nul inclut la licence pour une capacité correspondant au nombre de téraoctets (To) pour l'espace disque utilisé sur la baie de disques spécifiée protégée par la sauvegarde avec temps d'indisponibilité nul (ZDB) et utilisant :

- HP Business Copy XP/EVA et/ou HP Continuous Access XP/EVA ou
- EMC TimeFinder et/ou EMC SRDF

La capacité d'espace disque utilisée est la capacité cumulée de tous les volumes principaux sur le type de baie de disques utilisé pour la sauvegarde avec temps d'indisponibilité nul ou pour la restauration instantanée. Le terme "principal" désigne les volumes de données de production d'origine. Cette quantité représente la capacité totale utilisable de ces volumes, en fonction de la taille configurée pour leurs LDEV. Data Protector ne requiert pas de licences pour la capacité consommée par les volumes secondaires, les miroirs ou les snapshots utilisés pour la protection des données.

- Le surdébit RAID est exclu. Cela signifie qu'il n'est pas nécessaire de prendre en compte la configuration RAID.
- Un licence d'utilisation pour la sauvegarde en ligne (B6955BA, B6865BA) est requise pour l'exécution de la sauvegarde avec temps d'indisponibilité nul.
- La sauvegarde avec temps d'indisponibilité nul via un fournisseur matériel Microsoft Windows 2003 VSS (Volume Shadow copy Service) requiert une licence avec cette extension ZDB (par exemple, l'image instantanée du système de fichiers, Microsoft Exchange Server ou la sauvegarde Microsoft SQL Server via un fournisseur de baies de disques HP).

Tableau 25 - Extension de restauration instantanée HP Data Protector

B7026CA	pour HP StorageWorks Disk Array XP, 1 To
B7026DA	pour HP StorageWorks Disk Array XP, 10 To
B7028AA	pour HP StorageWorks Enterprise Virtual Array, 1 To
B7028DA	pour HP StorageWorks Enterprise Virtual Array, 10 To

La licence d'utilisation de l'extension de restauration instantanée inclut la licence pour une capacité correspondant au nombre de téraoctets (To) spécifiés pour un espace disque utilisé ; cette licence est requise pour la restauration instantanée de la baie de disques avec la fonction Restauration instantanée. La restauration instantanée Data Protector permet de restaurer en quelques minutes des téraoctets de données à partir d'un ou de plusieurs disques de restauration, au lieu d'effectuer la restauration à partir d'une bande, ce qui pourrait demander plusieurs heures.

La capacité d'espace disque utilisée est la capacité cumulée de tous les volumes sur les types de baies de disques utilisés pour la sauvegarde avec temps d'indisponibilité nul ou pour la restauration instantanée. Le terme "principal" désigne les volumes de données de production d'origine. Cette quantité représente la capacité totale utilisable de ces volumes, en fonction de la taille configurée pour leurs LDEV. Data Protector ne requiert

pas de licences pour la capacité consommée par les volumes secondaires, les miroirs ou les snapshots utilisés pour la protection des données.

- Le surdébit RAID est exclu. Cela signifie qu'il n'est pas nécessaire de prendre en compte la configuration RAID.
- Requiert un nombre équivalent de licences d'utilisation Data Protector ZDB, qui elles-mêmes requièrent une licence d'utilisation en ligne.

Tableau 26 - Extension de la sauvegarde directe HP Data Protector

B7027AA	pour HP StorageWorks Disk Array XP, 1 To
B7027DA	pour HP StorageWorks Disk Array XP, 10 To

La licence d'utilisation de l'extension de sauvegarde directe inclut la licence nécessaire pour effectuer la sauvegarde directe avec HP StorageWorks Disk Array XP, requise pour le nombre de téraoctets (To) spécifiés pour l'espace disque source utilisé nécessaire à la sauvegarde directe (sans serveur).

Requiert un nombre équivalent de licences d'utilisation Data Protector ZDB, qui elles-mêmes requièrent une licence d'utilisation en ligne.

Tableau 27 - Sauvegarde directe HP Data Protector à l'aide de NDMP

B7022BA	pour 1 To
B7022DA	pour 10 To

Comprend la licence nécessaire pour effectuer la sauvegarde du nombre de téraoctets (To) spécifié sur un serveur NDMP.

Une licence est requise par téraoctet (To) d'espace disque utilisé pour chaque système de fichiers sauvegardé via NDMP (par exemple, les serveurs de fichiers Network Appliance ou EMC Celerra).

La capacité de disque utilisée correspond à la capacité totale de l'ensemble des volumes présents dans les fichiers sauvegardés via NDMP. Cette quantité représente la quantité totale utilisable de ces volumes, en fonction de la taille configurée pour leurs LDEV.

Tableau 28 - Extension de cryptage HP Data Protector

BB618AA	pour 1 client
BB618BA	pour 10 clients

Comprend la licence d'utilisation et les supports pour le cryptage de toutes les données d'un poste de travail ou serveur client Data Protector. Licence requise pour chaque client (agent) Data Protector pour lequel le cryptage est configuré.

- Dans les environnements de clusters, chaque système participant au cluster doit disposer d'une licence d'utilisation.

Tableau 29 - Manuels imprimés Extensions fonctionnelles HP Data Protector

B6960EA	Anglais
B6960EJ	Japonais

Les manuels sont disponibles au format électronique sur les DVD, les CD et sur le site http://www.hp.com/support/manuals. Vous pouvez commander des manuels imprimés avec les deux options suivantes : Pack Starter et Extensions fonctionnelles. Pour connaître la liste des manuels Pack Starter, reportez-vous à la section "Manuels" à la page 364.

Les manuels imprimés Extensions fonctionnelles comportent les éléments suivants :

- *Guide d'intégration HP Data Protector pour les applications Microsoft : SQL Server, SharePoint Portal Server, Exchange Server et Volume Shadow Copy Service*
- *Guide d'intégration HP Data Protector pour Oracle et SAP*
- *Guide d'intégration HP Data Protector pour les applications IBM : Informix, DB2 et Lotus Notes/Domino*
- *Guide d'intégration HP Data Protector pour VMware Virtual Infrastructure, Sybase, Network Node Manager et le serveur NDMP (Network Data Management Protocol)*
- *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*
- *Guide conceptuel ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*
- *Guide de l'administrateur ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*
- *Guide d'intégration HP Data Protector pour HP Service Information Portal*
- *Guide d'intégration HP Data Protector pour HP Reporter*
- *Guide d'intégration HP Data Protector pour HP Operations Manager sous UNIX*
- *Guide d'intégration HP Data Protector pour HP Operations Manager sous Windows*
- *Guide d'intégration HP Data Protector pour HP Performance Manager et HP Performance Agent*
- *Références, notes de publication et annonces produits HP Data Protector pour les intégrations à HP Operations Manager, HP Reporter, HP Performance Manager, HP Performance Agent et HP Service Information Portal*
- *Data Protector Guide de l'utilisateur Media Operations*
- *Data Protector Références, notes de publication et annonces produits Media Operations*

Editions serveur unique (SSE)

Le Tableau 30 à la page 363 contient les numéros de licence des Packs Starter de l'Edition serveur unique Data Protector A.06.10.

Tableau 30 - Numéros de licence des Packs Starter HP Data Protector SSE

B7020AA	DVD et licence d'utilisation SSE pour HP-UX
B7020BA	Licence d'utilisation SSE uniquement pour HP-UX
B7020DA	DVD et licence d'utilisation SSE pour Solaris
B7020CA	Licence d'utilisation SSE uniquement pour Solaris
B7030AA	DVD et licence d'utilisation SSE pour Windows
B7030BA	Licence d'utilisation SSE uniquement pour Windows
B7021AA	Migration vers la version SSE pour HP-UX
B7021DA	Migration vers la version SSE pour Solaris
B7031AA	Migration vers la version SSE pour Windows
B6960MA	kit DVD
B6960LA	Manuels SSE - imprimés (anglais)
B6960LJ	Manuels SSE - imprimés (japonais)
B6960LF	Manuels SSE - imprimés (français)

Licence

La licence d'utilisation de l'Edition serveur unique inclut la licence qui permet de sauvegarder un serveur unique sur la plate-forme spécifiée avec un nombre illimité de stations de travail UNIX et/ou Windows et un lecteur de sauvegarde. En outre, cette édition peut gérer un changeur automatique/une bibliothèque comprenant 10 emplacements au maximum.

Migration

La licence d'utilisation de la migration inclut la licence qui permet d'effectuer une migration depuis SSE ou Data Protector Express vers le Pack Starter Data Protector.

Faites migrer l'Edition serveur unique vers le Pack Starter afin de bénéficier des fonctions suivantes :

- Clients de sauvegarde supplémentaires (agents) sur toute plate-forme
- Lecteurs de sauvegarde supplémentaires

- Capacité de gérer les chargeurs automatiques/bibliothèques de plus de 10 emplacements
- Récupération après sinistre des systèmes
- Génération avancée de rapports (dans l'interface graphique utilisateur de Data Protector et via le Web)
- Prise en charge SAN (avec le serveur de gestion pour HP-UX, Solaris ou Linux)
- Gestion centrée service via les intégrations au logiciel HP

Pour commander la licence d'utilisation de la migration, vous devez disposer d'une licence d'utilisation pour Edition serveur unique.

Supports

Data Protector A.06.10 sera livré avec deux DVD. Si vous avez besoin de CD, il existe aussi un kit CD (B6960MB) qui contient 15 CD. Il est toutefois recommandé d'utiliser le kit DVD.

Manuels

Tous les manuels sont disponibles au format électronique sur les DVD, les CD et sur le site http://www.hp.com/support/manuals.

Vous pouvez commander des manuels imprimés avec les deux options suivantes : Pack Starter et Extensions fonctionnelles. Les manuels Pack Starter imprimés comportent les éléments suivants :

- *Guide conceptuel HP Data Protector*
- *Guide d'installation et de choix des licences HP Data Protector*
- *Guide de dépannage HP Data Protector*
- *Guide de récupération aprs sinistre HP Data Protector*
- *Références, notes de publication et annonces produits HP Data Protector*

REMARQUE :

L'Edition serveur unique pour Windows ne peut gérer que les stations de travail Windows.

Pour connaître la liste des manuels Extensions fonctionnelles, reportez-vous au Tableau 29 à la page 362.

Migration de licence vers Data Protector A.06.10

La migration à partir des versions antérieures de Data Protector s'effectue comme suit :

Data Protector A.05.10, A.05.50 et A.06.00

Migrez directement vers Data Protector A.06.10. Aucune migration de licence ou de toute autre sorte n'est requise. Data Protector Les clients de Data Protector A.05.10, A.05.50 et A.06.00 sous contrat de support recevront gratuitement Data Protector A.06.10. Une fois la mise à niveau de votre environnement vers Data Protector A.06.10 effectuée, la fonctionnalité que vous utilisiez avec la version A.05.10, A.05.50 ou A.06.00 est disponible avec Data Protector A.06.10 sans supplément de prix. Vous devez simplement acquérir de nouvelles licences si vous souhaitez vous procurer les nouvelles extensions fonctionnelles.

Présentation de la licence graphique

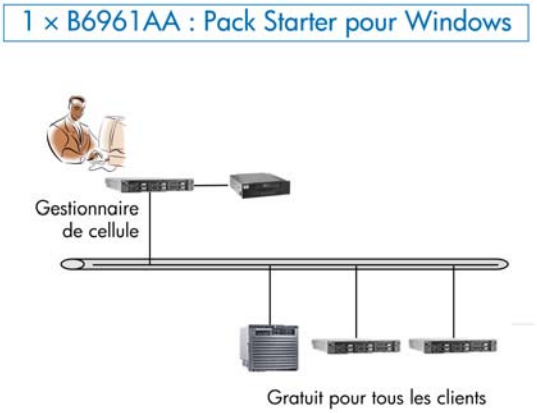

Figure 59 - Pack Starter pour HP-UX

1 × B6951AA : Pack Starter pour HP-UX
11 × B6953AA : Extension de lecteur pour UNIX, NAS, SAN
4 × B6963AA : Extension de lecteur pour Windows, NetWare, Linux (Intel)

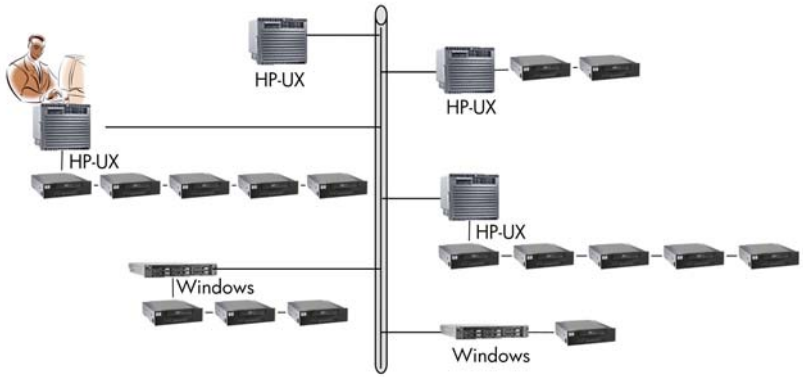

Figure 60 - Environnement mixte

1 × B6961AA : Pack Starter pour Windows
9 × B6963AA : Extension de lecteur pour Windows, NetWare, Linux (Intel)
4 × B6953AA : Extension de lecteur pour UNIX, NAS, SAN
1 × B6957BA : Extension pour bibliothèques 61 - 250 emplacements
1 × B6958BA : Extension pour biblio. sans limitation en nombre

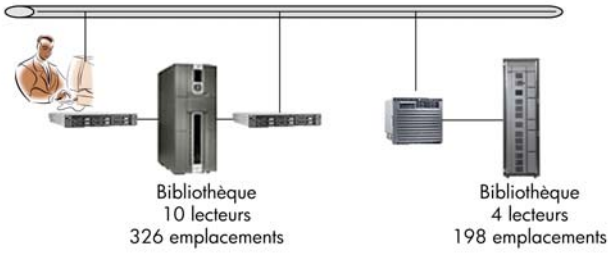

Figure 61 - 61 - 250 emplacements de bibliothèque - exemple 1

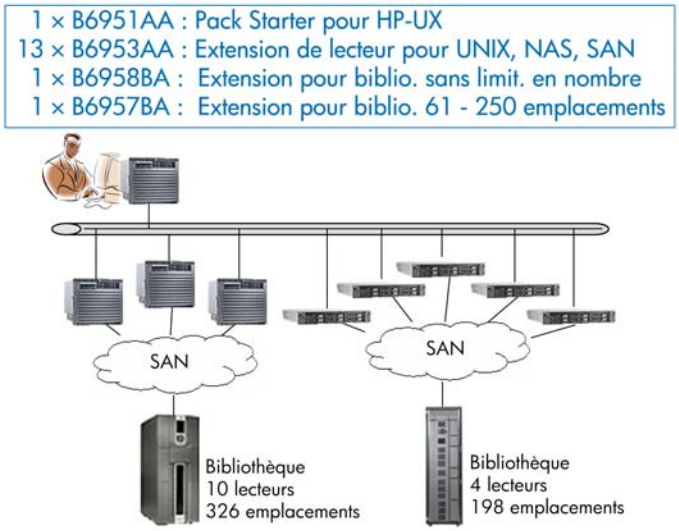

Figure 62 - 61 - 250 emplacements de bibliothèque - exemple 2

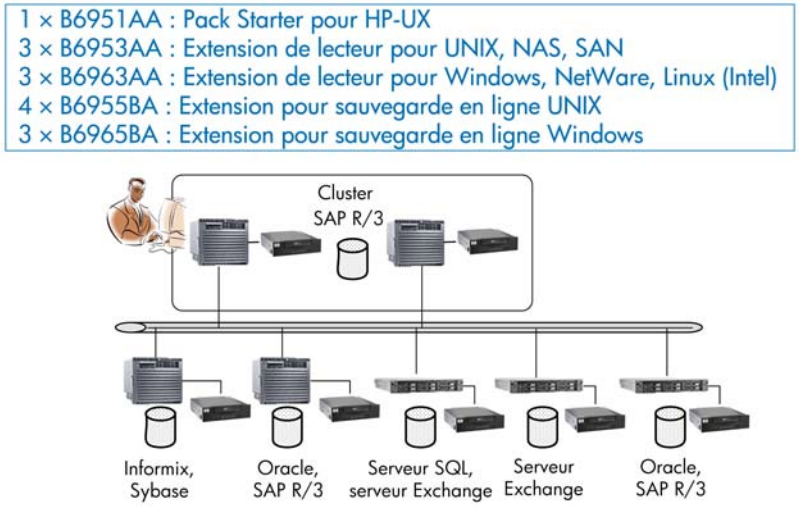

Figure 63 - Sauvegarde en ligne

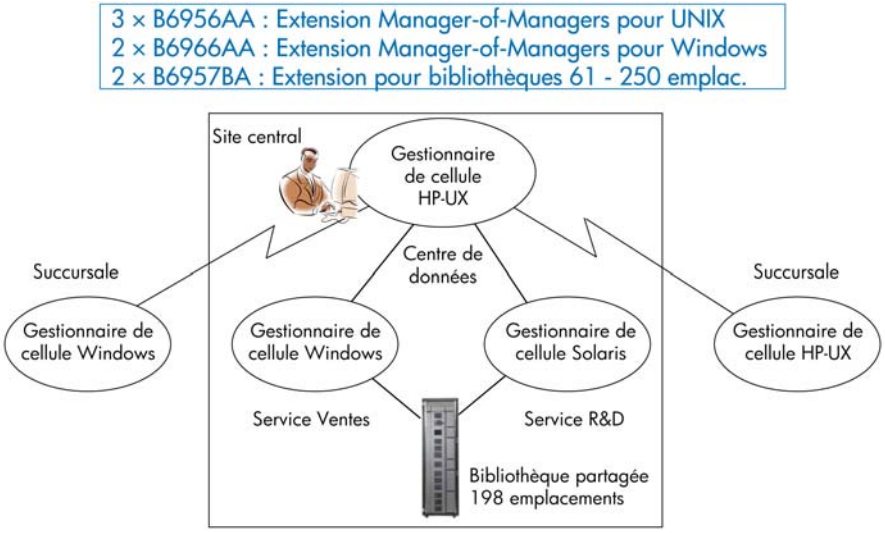

Figure 64 - Manager-of-Managers

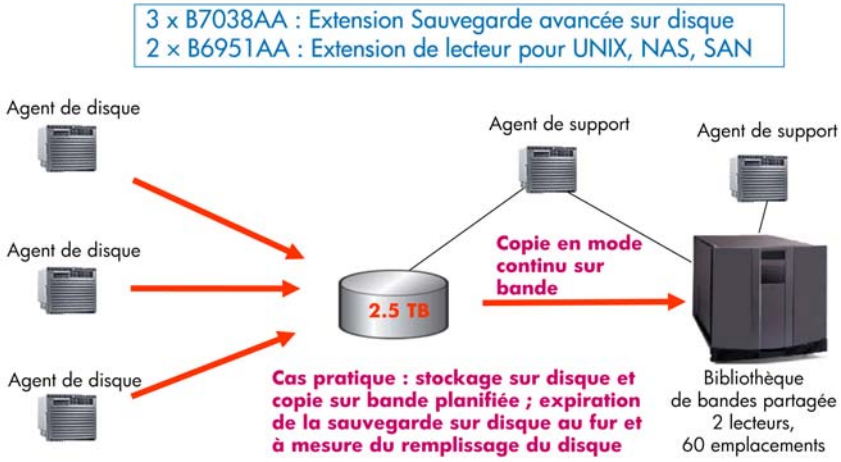

Figure 65 - Sauvegarde avancée sur disque

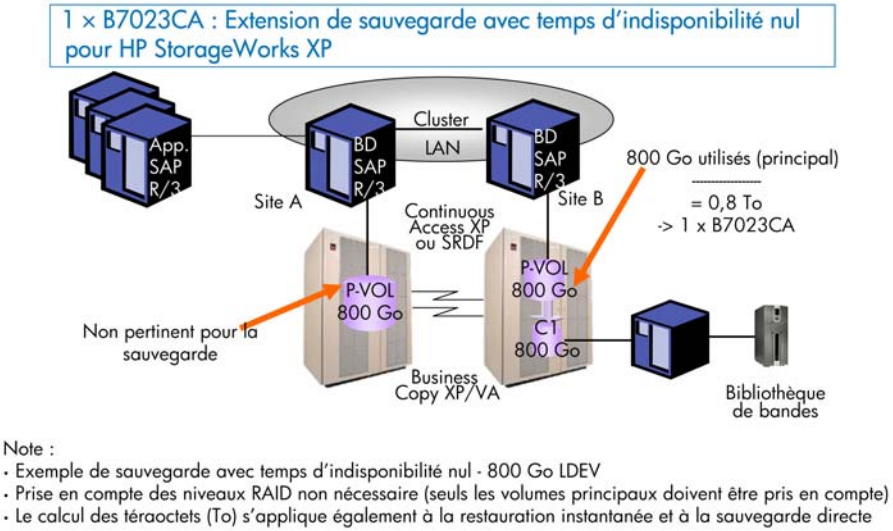

Figure 66 - Sauvegarde avec temps d'indisponibilité nul

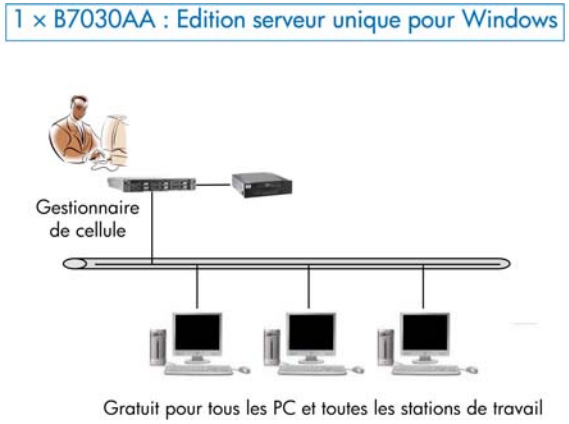

Figure 67 - Edition serveur unique

Formulaires d'attribution de licences Data Protector

Ce chapitre présente les formulaires d'attribution de licence Data Protector. Remplissez-les pour commander des mots de passe permanents à l'aide d'une des méthodes suivantes :

- Utilisez l'utilitaire HP AutoPass pour obtenir et installer les nouveaux mots de passe permanents directement via Internet à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus d'informations, reportez-vous à la section

"Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP AutoPass" à la page 322. Cette méthode est recommandée.

- Imprimez la version électronique de ces formulaires de licence qui se trouve dans les fichiers suivants sur le système Gestionnaire de cellule et les supports de distribution :
  - HP-UX, Solaris et Linux : `/opt/omni/doc/C/license_forms_UNIX`
  - DVD-ROM Windows : *`Nom_disque`*`:Docs\license_forms.txt`

  ou utilisez les fichiers électroniques pour "copier" et "coller" votre message avant de l'adresser au *Centre de remise de mot de passe (PDC)*.
- Commandez des mots de passe permanents via le site Internet du *Centre de remise de mot de passe*, à l'adresse http://www.webware.hp.com.

IMPORTANT :

Assurez-vous que vous saisissez clairement les informations et que vous n'oubliez pas de renseigner les champs obligatoires.

Vous trouverez ci-après une brève description des champs des formulaires d'attribution de licence que vous devez renseigner :

Données personnelles	Ce champ contient les informations relatives au client, notamment la personne à laquelle le nouveau mot de passe doit être communiqué.
Données d'attribution de licence	Ce champ contient les informations d'attribution de licence relatives à votre cellule Data Protector.
Courant Gestionnaire de cellule	Saisissez les informations requises relatives à votre Gestionnaire de cellule courant.
Nouveau Gestionnaire de cellule	Saisissez les informations requises relatives à votre nouveau Gestionnaire de cellule.
Numéro de commande	Saisissez le *numéro de commande* imprimé sur l'*attestation de droit.* Le *numéro de commande* est nécessaire pour vérifier que vous êtes autorisé à demander un mot de passe permanent.

Adresse IP	Ce champ définit le système pour lequel le *Centre de remise de mot de passe* fournira des mots de passe. Si vous souhaitez utiliser la gestion centralisée des licences (environnements MoM uniquement), ce système doit être le système Gestionnaire MoM. Si le Gestionnaire de cellule est doté de plusieurs cartes réseau, vous pouvez saisir n'importe quelle adresse IP correspondante. Il est recommandé d'utiliser l'adresse IP principale. Si vous utilisez Data Protector dans un environnement MC/Service Guard ou Microsoft Cluster, saisissez l'adresse IP de votre serveur virtuel. Pour plus d'informations sur les clusters, reportez-vous à l'aide en ligne.
Centre de remise de mot de passe Numéros de télécopie	Pour obtenir les coordonnées, reportez-vous à l'*attestation de droit* livrée avec votre produit.
Type de licence de produit	Dans les champs situés en regard des *numéros de produit*, indiquez le nombre de licences que vous souhaitez installer sur ce Gestionnaire de cellule. Ce nombre doit être égal ou inférieur à la totalité des licences acquises avec le *numéro de commande*.

B Annexe B

Dans cette annexe

Vous trouverez dans cette annexe des informations supplémentaires relatives aux tâches qui dépassent le cadre de ce document, mais qui sont d'importance pour la procédure d'installation.

L'installation et la configuration des systèmes et périphériques pour les systèmes Windows, HP-UX, Solaris et Linux sont illustrées par des exemples.

Installation sur des systèmes HP-UX, Solaris et Linux à l'aide d'outils natifs

REMARQUE :

Les procédures d'installations natives sur HP-UX, Solaris et Linux ne sont documentées que si vous avez l'intention d'installer un Serveur d'installation comportant un nombre limité de packages. Il est recommandé d'installer Data Protector à l'aide de `omnisetup.sh`.

Installation d'un Gestionnaire de cellule sur un système HP-UX à l'aide de swinstall

Suivez la procédure ci-dessous pour installer le Gestionnaire de cellule UNIX sur un système HP-UX :

1. Insérez et montez le DVD-ROM d'installation UNIX et exécutez l'utilitaire `/usr/sbin/swinstall`.
2. Dans la fenêtre Spécifier source, sélectionnez Chemin réseau/CDROM, puis saisissez :
   - Sur un système PA-RISC sous HP-UX : *`Point_de_montage`*`/hpux_pa/DP_DEPOT/DP_A0610_UX11x.sd_depot`
   - Sur un système IA-64 sous HP-UX : *`Point_de_montage`*`/hpux_ia/DP_DEPOT/DP_A0610_UXia64.sd_depot`

   dans le `Chemin d'accès au dépôt source`. Cliquez ensuite sur OK pour ouvrir la fenêtre Installation SD - Sélection de logiciel.

3. Dans la liste des produits logiciels disponibles pour l'installation, vous trouverez le produit Data Protector sous la référence `B6960MA`. Cliquez deux fois sur ce dernier pour afficher le produit DATA-PROTECTOR pour UNIX. Cliquez deux fois sur ce dernier pour en afficher le contenu.

   Ce produit contient les sous-produits suivants :

OB2-CM	Logiciel du Gestionnaire de cellule
OB2-DOCS	Documentation de Data Protector comprenant les manuels Data Protector au format PDF et l'aide en ligne (WebHelp).
OMNI-JGUI-P	Interface graphique utilisateur compatible Java. Pour installer l'interface de ligne de commande sur un client disposant de l'interface graphique utilisateur Java, vous devez installer le package OB2-CC.

4. Cliquez avec le bouton droit de la souris sur DATA-PROTECTOR, puis cliquez sur Marquer pour l'installation afin d'installer le logiciel dans son intégralité.

   Si vous n'avez pas besoin de tous les sous-produits, cliquez deux fois sur DATA-PROTECTOR, puis cliquez avec le bouton droit de la souris sur un élément de la liste. Cliquez sur Annuler les marques pour l'installation pour exclure le package, ou sur Marquer pour l'installation pour l'intégrer à l'installation.

   Assurez-vous que la valeur d'état `Marqué ?` en regard du package `OB2-CM` est réglée sur `Oui` si vous installez le Gestionnaire de cellule pour UNIX sur le système. Reportez-vous à la Figure 68 à la page 375.

REMARQUE :

Si vous utilisez des ID utilisateur de plus de 32 bits, vous devez installer le composant Interface utilisateur (OMNI-CS) à distance sur le Gestionnaire de cellule après avoir installé le composant logiciel central Gestionnaire de cellule.

5. Dans la liste Actions, cliquez sur Installation (analyse), puis sur OK pour continuer. Si l'opération `Installation (analyse)` échoue et qu'un message d'erreur s'affiche, cliquez sur Fichier journal pour visualiser ce fichier.

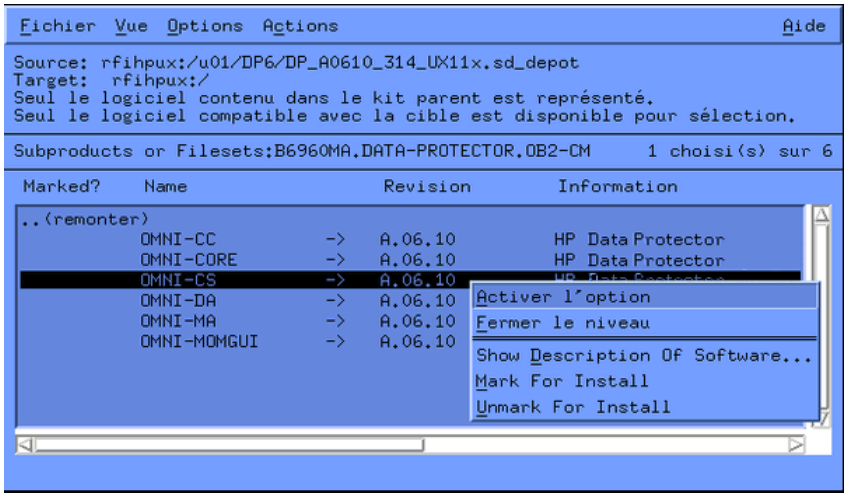

Figure 68 - Fenêtre Installation SD - Sélection de logiciel

REMARQUE :

Pour installer des logiciels à partir d'un lecteur de bande via le réseau, vous devez d'abord monter le répertoire source sur votre ordinateur.

Installation d'un Gestionnaire de cellule sur des systèmes Solaris à l'aide de pkgadd

Pour installer le Gestionnaire de cellule sur un système Solaris, suivez la procédure ci-dessous :

1. Insérez le DVD-ROM d'installation UNIX.
2. Accédez au répertoire principal *package_source*, c'est-à-dire le répertoire contenant le fichier dépôt d'installation (dans ce cas, *Point_de_montage* /solaris/DP_DEPOT).

   Les packages de sous-produits suivants liés à l'installation du Gestionnaire de cellule sont inclus dans le produit :

OB2-CORE	Logiciel central Data Protector.
OB2-CC	Logiciel de la Console de cellule. Ce logiciel contient l'interface graphique utilisateur et l'interface de ligne de commande.

OB2-CS	Logiciel du Gestionnaire de cellule.
OB2-DA	Logiciel Agent de disque. Ce logiciel est requis ; il est indispensable pour sauvegarder la base de données IDB.

et (facultatif) :

OB2-MA	Logiciel Agent général de support. Ce logiciel est requis si vous souhaitez connecter un périphérique de sauvegarde au Gestionnaire de cellule.
OB2-DOCS	Documentation de Data Protector comprenant les manuels Data Protector au format PDF et l'aide en ligne (WebHelp).
OB2-JGUI-P	Interface graphique utilisateur compatible Java. Pour installer l'interface de ligne de commande sur un client disposant de l'interface graphique utilisateur Java, vous devez installer le package OB2-CC.

3. Utilisez la fonction `pkgadd` pour installer les packages ci-dessus.

IMPORTANT :

Les packages de sous-produits sous Solaris sont interdépendants. Vous devez installer ces packages en respectant l'ordre de la liste ci-dessus.

Pour installer chaque package, exécutez la commande suivante :

```
pkgadd -d DP_A0610_SUN8.pkg nom_package
```

4. Redémarrez les services Data Protector :

```
/opt/omni/sbin/omnisv stop
/opt/omni/sbin/omnisv start
```

REMARQUE :

Si vous avez installé le Gestionnaire de cellule sous Solaris 9 ou Solaris 10, installez l'Agent de disque à distance sur le Serveur d'installation à l'aide d'un Gestionnaire de cellule. L'Agent de disque Solaris générique sera ainsi remplacé par l'Agent de disque Solaris 9 ou Solaris 10. Reportez-vous à la section "Installation distante de clients Data Protector" à la page 78 ou à la page de manuel `ob2install`.

Installation du Gestionnaire de cellule sur des systèmes Linux à l'aide de rpm

Pour installer le Gestionnaire de cellule sur un système Linux, suivez la procédure ci-dessous :

1. Insérez et montez le DVD-ROM d'installation UNIX.
2. Procédez à l'extraction des packages individuels :
   - Utilisez `rpm2cpio` (recommandé) :
     Accédez au répertoire temporaire dans lequel extraire les fichiers d'archives et exécutez la commande suivante :
     `rpm2cpio` *`source_package/`* `DP_A0610_GPLx86_64.rpm | cpio -ivd`
     Où *`source_package`* est le répertoire contenant le fichier d'archives d'installation (dans ce cas, *`Point_montage`*`/linux/DP_DEPOT`).
   - Vous pouvez également utiliser `rpm` :
     Accédez au répertoire contenant le fichier d'archives d'installation (dans ce cas, *`Point_montage`*`/linux/DP_DEPOT`, puis exécutez la commande suivante :
     `rpm -i DP_A0610_GPLx86_64.rpm`

   REMARQUE :

   La commande `rpm -i` ci-dessus n'installe pas le logiciel. Seuls les packages RPM individuels sont copiés dans `/opt/omni`.

   Toutefois, le package principal est toujours enregistré ; vous devez donc supprimer le package `OB2-CM` une fois l'installation des packages individuels terminée.

3. Accédez au répertoire dans lequel sont extraits les packages individuels :
   - Si vous avez utilisé `rpm2cpio` : `cd` *`répertoire_temporaire`*`/opt/omni`
   - Si vous avez utilisé `rpm` : `cd /opt/omni`

   Pour installer un package, exécutez la commande ci-dessous :

```
rpm -i nom_package-A.06.10-1.x86_64.rpm
```

où *nom_package* est le nom du package de sous-produit.

Vous devez installer les packages suivants :

OB2-CORE	Logiciel central Data Protector.
OB2-CC	Logiciel de la Console de cellule. Ce logiciel contient l'interface de ligne de commande.
OB2-CS	Logiciel du Gestionnaire de cellule.
OB2-DA	Logiciel Agent de disque. Ce logiciel est requis ; il est indispensable pour sauvegarder la base de données IDB.

Vous pouvez également installer les packages suivants :

OB2-MA	Logiciel Agent général de support. Ce logiciel est requis si vous souhaitez connecter un périphérique de sauvegarde au Gestionnaire de cellule.
OB2-DOCS	Documentation de Data Protector comprenant les manuels Data Protector au format PDF et l'aide en ligne (WebHelp).
OB2-JGUI-P	Interface graphique utilisateur compatible Java. Pour installer l'interface de ligne de commande sur un client disposant de l'interface graphique utilisateur Java, vous devez installer le package OB2-CC.

IMPORTANT :

Les packages de sous-produits sous Linux sont interdépendants. Vous devez installer ces packages en respectant l'ordre de la liste ci-dessus.

4. Redémarrez les services Data Protector :

   `/opt/omni/sbin/omnisv stop`

   `/opt/omni/sbin/omnisv start`

5. Si vous avez utilisé `rpm` pour l'extraction du fichier d'archives RPM principal, supprimez le package `OB2-CM` :

   `rpm -e OB2-CM`

Installation d'un Serveur d'installation sur un système HP-UX à l'aide de swinstall

1. Insérez et montez le DVD-ROM d'installation UNIX.
2. Dans la ligne de commande, tapez `/usr/sbin/swinstall` pour exécuter le programme d'installation.
3. Dans la fenêtre Spécifier source, sélectionnez Chemin réseau/CD-ROM, puis dans la zone Chemin d'accès au dépôt source, saisissez :
   - Sur un système PA-RISC sous HP-UX : *Point_de_montage*`/hpux_pa/DP_DEPOT/DP_A0610_UX11x_IS.sd_depot`.
   - Sur un système IA-64 sous HP-UX : *Point_de_montage*`/hpux_ia/DP_DEPOT/DP_A0610_UXia64_IS.sd_depot`.

   Ouvrez ensuite la fenêtre Installation SD - Sélection de logiciel.
4. Dans cette dernière, cliquez deux fois sur DATA-PROTECTOR pour obtenir la liste des logiciels d'installation. Cliquez avec le bouton droit de la souris sur OB2-IS, puis cliquez sur Marquer pour l'installation.
5. Dans le menu Actions, cliquez sur Installation (analyse). Cliquez sur OK pour continuer.

Au terme de l'installation, le dépôt de logiciel pour UNIX réside dans le répertoire `/opt/omni/databases/vendor`.

IMPORTANT :

Si vous n'installez pas le Serveur d'installation pour UNIX sur votre réseau, vous devrez installer chaque client UNIX en local à partir du DVD-ROM d'installation UNIX.

Installation d'un Serveur d'installation sur des systèmes Solaris à l'aide de pkgadd

Installation locale sous Solaris

Pour installer le Serveur d'installation pour UNIX sur un système Solaris, procédez comme suit :

1. Insérez le DVD-ROM d'installation UNIX.
2. Accédez au répertoire principal *package_source*, c'est-à-dire au répertoire contenant le fichier dépôt d'installation (dans ce cas, *Point_montage*/solaris/DP_DEPOT).

   Les packages de sous-produits suivants liés à l'installation du Serveur d'installation sont inclus dans le produit :

OB2-CORE	Logiciel central Data Protector. Notez que si vous installez le Serveur d'installation sur le Gestionnaire de cellule, le logiciel central est déjà installé.
OB2-C-IS	Logiciel central Serveur d'installation.
OB2-SOLUX	Paquets push de l'Agent de disque, l'Agent de support et l'interface graphique utilisateur pour les systèmes Solaris distants.
OB2-OTHUX	Paquets push de l'Agent de disque et de l'Agent de support pour systèmes UNIX non-Solaris distants.

   De plus, si vous configurez un Serveur d'installation indépendant (c'est-à-dire ne figurant pas dans le Gestionnaire de cellule) et souhaitez utiliser l'interface utilisateur :

OB2-CC	Logiciel de la Console de cellule. Ce logiciel contient l'interface graphique utilisateur et l'interface de ligne de commande.

3. Utilisez la fonction `pkgadd` pour installer les packages ci-dessus.

IMPORTANT :

Les packages de sous-produits sous Solaris sont interdépendants. Vous devez installer ces packages en respectant l'ordre de la liste ci-dessus.

Pour installer chaque package, exécutez la commande suivante :

```
pkgadd -d DP_A0610_SUN8_IS.pkg nom_package
```

REMARQUE :

La fonction `pkgadd` ne peut être exécutée que localement, pas à distance.

4. Une fois ces composants installés, utilisez `pkgadd` pour installer les paquets push de tous les packages d'intégration que vous souhaiterez installer à distance. Par exemple :

OB2-INTGP	Logiciel d'intégration central Data Protector. Ce composant est nécessaire pour installer les intégrations.
OB2-ORACORE	Logiciel d'intégration Core Oracle et SAP R/3 Data Protector. Ce composant est nécessaire pour installer l'intégration SAP R/3 ou Oracle Data Protector.
OB2-SAPP	Composant d'intégration SAP.
OB2-SAPDBP	Composant d'intégration SAP DB.
OB2-INFP	Composant d'intégration Informix.
OB2-LOTP	Composant d'intégration Lotus Notes/Domino.
OB2-SYBP	Composant d'intégration Sybase.
OB2-OR8P	Composant d'intégration Oracle.
OB2-DB2P	Composant d'intégration DB2.
OB2-EMCP	Composant d'intégration EMC Symmetrix.

OB2-SNAPP	HP StorageWorks Virtual Array.
OB2-SMISAP	HP StorageWorks Enterprise Virtual Array.
OB2-SSEAP	HP StorageWorks Disk Array XP.
OB2-NDMPP	Logiciel Agent de support NDMP.
OB2-OVP	Composant d'intégration HP NNM.
OB2-FRAP	Package de localisation en français.
OB2-JPNP	Package de localisation en japonais.

Au terme de l'installation, le dépôt de logiciel pour UNIX réside dans le répertoire `/opt/omni/databases/vendor`.

IMPORTANT :

Si vous n'installez pas un Serveur d'installation pour UNIX sur votre réseau, vous devrez installer chaque client UNIX en local à partir du DVD-ROM d'installation UNIX.

IMPORTANT :

Si vous souhaitez installer Data Protector sur des répertoires liés, par exemple :

`/opt/omni/ -> /`*`préfixe`*`/opt/omni/`

`/etc/opt/omni/ -> /`*`préfixe`*`/etc/opt/omni/`

`/var/opt/omni/ -> /`*`préfixe`*`/var/opt/omni/`

Vous devez créer les liens avant l'installation et vous assurer que les répertoires cible existent.

REMARQUE :

Si vous installez le composant Interface utilisateur (interface graphique utilisateur ou interface de ligne de commande), il faut au préalable mettre à jour les variables d'environnement. Pour plus d'informations, reportez-vous à la section "Configuration des variables d'environnement" à la page 51.

Si vous avez l'intention d'utiliser l'interface utilisateur Data Protector pour effectuer des sauvegardes ou des restaurations sur plusieurs plates-formes, reportez-vous aux Références, notes de publication et annonces produits HP Data Protector pour connaître les limites en vigueur.

Etape suivante

A ce stade de la procédure, les serveurs d'installation pour UNIX doivent être installés sur votre réseau. Vous devez maintenant effectuer les tâches suivantes :

1. Si vous avez configuré un Serveur d'installation indépendant (c'est-à-dire ne figurant pas dans le Gestionnaire de cellule), il faut ajouter (importer) manuellement le système dans la cellule Data Protector. Reportez-vous à la section "Importation d'un serveur d'installation dans une cellule" à la page 207.

   REMARQUE :

   Lorsqu'un Serveur d'installation est importé, le fichier `/etc/opt/omni/server/cell/installation_servers` du Gestionnaire de cellule est mis à jour et répertorie les paquets push installés. Ce fichier peut être utilisé à partir de l'interface de ligne de commande pour vérifier les paquets push disponibles. Pour maintenir ce fichier à jour, vous devrez exporter, puis réimporter un Serveur d'installation à chaque installation ou suppression d'un paquet push. Cette procédure est valable même dans le cas où un Serveur d'installation est installé sur le même système que le Gestionnaire de cellule.

2. Installez le Serveur d'installation pour Windows si vous disposez de systèmes Windows dans votre cellule Data Protector. Reportez-vous à la section Configuration système requise à la page 65.
3. Distribuez le logiciel aux clients. Reportez-vous à la section "Installation des clients Data Protector" à la page 70.

Installation d'un Serveur d'installation sur des systèmes Linux à l'aide de rpm

Installation locale sous Linux

Pour installer le Serveur d'installation pour UNIX sur un système Linux, procédez comme suit :

1. Insérez le DVD-ROM d'installation UNIX.
2. Procédez à l'extraction des packages individuels :
   - Utilisez `rpm2cpio` (recommandé) :
     Accédez au répertoire temporaire dans lequel extraire les fichiers d'archives et exécutez la commande suivante :
     `rpm2cpio` *`source_package/`* `DP_A0610_GPLx86_64.rpm | cpio -ivd`
     Où *`source_package`* est le répertoire contenant le fichier d'archives d'installation (dans ce cas, *`Point_montage`*`/linux/DP_DEPOT`).
   - Vous pouvez également utiliser `rpm` :
     Accédez au répertoire contenant le fichier d'archives d'installation (dans ce cas, *`Point_montage`*`/linux/DP_DEPOT`, puis exécutez la commande suivante :
     `rpm -i DP_A0610_GPLx86_64_IS.rpm`

   REMARQUE :

   La commande `rpm -i` ci-dessus n'installe pas le logiciel. Seuls les packages RPM individuels sont copiés dans `/opt/omni`.

   Toutefois, le package principal est toujours enregistré ; vous devez donc supprimer le package `OB2-CM` une fois l'installation des packages individuels terminée.

3. Accédez au répertoire dans lequel sont extraits les packages individuels :
   - Si vous avez utilisé `rpm2cpio` : `cd` *`répertoire_temporaire`*`/opt/omni`
   - Si vous avez utilisé `rpm` : `cd /opt/omni`

   Pour chaque package, exécutez la commande suivante :

   `rpm -i` *`nom_package`*`-A.06.10-1.x86_64.rpm`

   Les packages de sous-produits suivants (*`nom_package`*) liés à l'installation du Serveur d'installation sont inclus dans le produit :

OB2-CORE	Logiciel central Data Protector. Notez que si vous installez le Serveur d'installation sur le Gestionnaire de cellule, le logiciel central est déjà installé.
OB2-CORE-IS	Logiciel central Serveur d'installation.
OB2-LINUXP	Paquets push de l'Agent de disque, l'Agent de support et l'interface graphique utilisateur pour les systèmes Linux distants.
OB2-OTHUXP	Paquets push de l'Agent de disque et de l'Agent de support pour systèmes non-Linux distants.

De plus, si vous configurez un Serveur d'installation indépendant (c'est-à-dire ne figurant pas dans le Gestionnaire de cellule) et souhaitez utiliser l'interface utilisateur :

OB2-CC	Logiciel de la Console de cellule. Ce logiciel contient l'interface de ligne de commande.
OB2-DOCS	Documentation de Data Protector comprenant les manuels Data Protector au format PDF et l'aide en ligne (WebHelp).
OB2-JGUI-P	Interface graphique utilisateur compatible Java. Pour installer l'interface de ligne de commande sur un client disposant de l'interface graphique utilisateur Java, vous devez installer le package OB2-CC.

4. Une fois ces composants installés, utilisez `rpm` pour installer les paquets push de tous les packages d'intégration que vous souhaiterez installer à distance. Par exemple :

OB2-INTGP	Logiciel d'intégration central Data Protector. Ce composant est nécessaire pour installer les intégrations.
OB2-ORACORE	Logiciel d'intégration Core Oracle et SAP R/3 Data Protector. Ce composant est nécessaire pour installer l'intégration SAP R/3 ou Oracle Data Protector.
OB2-SAPP	Composant d'intégration SAP.

OB2-VMWARE	Composant d'intégration VMware.
OB2-SAPDBP	Composant d'intégration SAP DB.
OB2-INFP	Composant d'intégration Informix.
OB2-LOTP	Composant d'intégration Lotus Notes/Domino.
OB2-SYBP	Composant d'intégration Sybase.
OB2-OR8P	Composant d'intégration Oracle.
OB2-DB2P	Composant d'intégration DB2.
OB2-EMCP	Composant d'intégration EMC Symmetrix.
OB2-SNAPP	HP StorageWorks Virtual Array.
OB2-SMISAP	HP StorageWorks Enterprise Virtual Array.
OB2-SSEAP	HP StorageWorks Disk Array XP.
OB2-NDMPP	Logiciel Agent de support NDMP.
OB2-OVP	Composant d'intégration HP NNM.
OB2-FRAP	Package de localisation en français.
OB2-JPNP	Package de localisation en japonais.

Au terme de l'installation, le dépôt de logiciel pour UNIX réside dans le répertoire `/opt/omni/databases/vendor`.

IMPORTANT :

Si vous n'installez pas un Serveur d'installation pour UNIX sur votre réseau, vous devrez installer chaque client UNIX en local à partir du DVD-ROM d'installation UNIX.

5. Si vous avez utilisé `rpm` pour l'extraction du fichier d'archives RPM principal, supprimez le package `OB2-CM` :

```
rpm -e OB2-CM
```

IMPORTANT :

Si vous souhaitez installer Data Protector sur des répertoires liés, par exemple :

`/opt/omni/ -> /préfixe/opt/omni/`

`/etc/opt/omni/ -> /préfixe/etc/opt/omni/`

`/var/opt/omni/ -> /préfixe/var/opt/omni/`

Vous devez créer les liens avant l'installation et vous assurer que les répertoires cible existent.

Etape suivante

A ce stade de la procédure, les serveurs d'installation pour UNIX doivent être installés sur votre réseau. Vous devez maintenant effectuer les tâches suivantes :

1. Si vous avez configuré un Serveur d'installation indépendant (c'est-à-dire ne figurant pas dans le Gestionnaire de cellule), il faut ajouter (importer) manuellement le système dans la cellule Data Protector. Reportez-vous à la section "Importation d'un serveur d'installation dans une cellule" à la page 207.

   REMARQUE :

   Lorsqu'un Serveur d'installation est importé, le fichier `/etc/opt/omni/server/cell/installation_servers` du Gestionnaire de cellule est mis à jour et répertorie les paquets push installés. Ce fichier peut être utilisé à partir de l'interface de ligne de commande pour vérifier les paquets push disponibles. Pour maintenir ce fichier à jour, vous devrez exporter, puis réimporter un Serveur d'installation à chaque installation ou suppression d'un paquet push. Cette procédure est valable même dans le cas où un Serveur d'installation est installé sur le même système que le Gestionnaire de cellule.

2. Installez le Serveur d'installation pour Windows si vous disposez de systèmes Windows dans votre cellule Data Protector. Reportez-vous à la section Configuration système requise à la page 65.
3. Distribuez le logiciel aux clients. Reportez-vous à la section "Installation des clients Data Protector" à la page 70.

Installation des clients

Les clients ne sont pas installés pendant une installation du Gestionnaire de cellule ou du Serveur d'installation. Les clients doivent être installés soit en utilisant `omnisetup.sh`, soit en chargeant les composants d'installation à partir de l'interface graphique de Data

Protector. Pour plus d'informations sur l'installation des clients, reportez-vous à la section "Installation des clients Data Protector" à la page 70.

Mise à niveau sur des systèmes HP-UX, Solaris et Linux à l'aide d'outils natifs

Mise à niveau de Data Protector sur les systèmes HP-UX à l'aide de swinstall

Une mise à niveau du Gestionnaire de cellule doit être réalisée à partir du DVD-ROM d'installation UNIX.

Si vous mettez à niveau un Gestionnaire de cellule sur lequel un Serveur d'installation est installé, vous devez d'abord effectuer la mise à niveau du Gestionnaire de cellule, puis celle du Serveur d'installation.

Les composants du client installés sur le système Gestionnaire de cellule *ne* sont *pas* mis à niveau en même temps que Gestionnaire de cellule ; ils doivent être mis à niveau en chargeant `omnisetup.sh` ou en chargeant les composants d'installation à partir du Serveur d'installation. Pour plus de détails, reportez-vous à la section "Installation locale de clients UNIX" à la page 142 ou "Installation distante de clients Data Protector" à la page 78.

Procédure de mise à niveau

Pour mettre à niveau Data Protector A.05.10, A.05.50 ou A.06.00 vers Data Protector A.06.10, à l'aide de `swinstall`, procédez comme suit :

1. Connectez-vous en tant que `root` et arrêtez les services Data Protector sur le Gestionnaire de cellule en exécutant la commande `/opt/omni/sbin/omnisv -stop`.

   Tapez `ps -ef | grep omni` pour vérifier si tous les services ont bien été arrêtés. Aucun service Data Protector ne doit être répertorié sur exécution de la commande `ps -ef | grep omni`.

2. Pour mettre à niveau un Gestionnaire de cellule et/ou un Serveur d'installation, suivez les procédures décrites dans la section "Installation d'un Gestionnaire de cellule sur un système HP-UX à l'aide de swinstall" à la page 373 et/ou la section "Installation d'un Serveur d'installation sur un système HP-UX à l'aide de swinstall" à la page 379.

La procédure d'installation détectera automatiquement la version antérieure et mettra à niveau *uniquement les composants sélectionnés*. Si un composant installé dans la version précédente de Data Protector n'est pas sélectionné, il *n'est pas* mis à niveau. Par conséquent, vous devez veiller à sélectionner tous les composants à mettre à niveau.

REMARQUE :

L'option `Match what target has (Sélectionner les composants de la cible)` *n'est pas* prise en charge si vous mettez à niveau le Gestionnaire de cellule et le Serveur d'installation sur le même système.

Mise à niveau de Data Protector sur les systèmes Solaris à l'aide de pkgadd

Pour mettre à niveau le Gestionnaire de cellule ou le Serveur d'installation de Solaris, désinstallez l'ancienne version et installez la nouvelle version du produit.

Les composants du client installés sur le système Gestionnaire de cellule *ne* sont *pas* mis à niveau en même temps que Gestionnaire de cellule ; ils doivent être mis à niveau en chargeant `omnisetup.sh` ou en chargeant les composants d'installation à partir du Serveur d'installation. Pour plus de détails, reportez-vous à la section "Installation locale de clients UNIX" à la page 142 ou "Installation distante de clients Data Protector" à la page 78.

Procédure de mise à niveau

Pour mettre à niveau Data Protector A.05.10, A.05.50 ou A.06.00 vers Data Protector A.06.10, à l'aide de `pkgadd`, procédez comme suit :

1. Connectez-vous en tant que `root` et arrêtez les services Data Protector sur le Gestionnaire de cellule en exécutant la commande `/opt/omni/sbin/omnisv -stop`.

   Tapez `ps -ef | grep omni` pour vérifier si tous les services ont bien été arrêtés. Aucun service Data Protector ne doit être répertorié sur exécution de la commande `ps -ef | grep omni`.

2. Désinstallez Data Protector à l'aide de `pkgrm`.

   Les fichiers de configuration et la base de données sont préservés durant cette procédure.

3. Exécutez la commande `pkginfo` pour vérifier que vous avez bien désinstallé l'ancienne version de Data Protector. Les anciennes versions de Data Protector ne doivent pas figurer dans la liste.

   Assurez-vous que la base de données et les fichiers de configuration sont toujours présents. Les répertoires suivants doivent toujours exister et contenir les fichiers binaires :

   - `/opt/omni`
   - `/var/opt/omni`
   - `/etc/opt/omni`

4. Si vous mettez à niveau un Gestionnaire de cellule, insérez et montez le DVD-ROM d'installation UNIX et utilisez `pkgadd` pour installer le Gestionnaire de cellule. Pour obtenir des informations détaillées sur la procédure à suivre, reportez-vous à la section "Installation d'un Gestionnaire de cellule sur des systèmes Solaris à l'aide de pkgadd" à la page 375.

   Si vous mettez à niveau un Serveur d'installation, insérez et montez le DVD-ROM d'installation UNIX et installez le Serveur d'installation. Pour obtenir des informations détaillées sur la procédure à suivre, reportez-vous à la section "Installation d'un Serveur d'installation sur des systèmes Solaris à l'aide de pkgadd" à la page 380.

REMARQUE :

Si vous avez mis à niveau le Gestionnaire de cellule sous Solaris 9 ou Solaris 10, installez l'Agent de disque à distance sur le Gestionnaire de cellule après la mise à niveau à l'aide d'un Serveur d'installation. L'Agent de disque générique Solaris sera ainsi remplacé par l'Agent de disque Solaris 9 ou Solaris 10. Reportez-vous à la section "Installation distante de clients Data Protector" à la page 78 ou à la page man de `ob2install`.

Mise à niveau de Data Protector sur des systèmes Linux à l'aide de rpm

Pour mettre à niveau le Gestionnaire de cellule ou le Serveur d'installation de Linux, désinstallez l'ancienne version et installez la nouvelle version du produit.

Les composants du client installés sur le système Gestionnaire de cellule *ne* sont *pas* mis à niveau en même temps que Gestionnaire de cellule ; ils doivent être mis à niveau en chargeant `omnisetup.sh` ou en chargeant les composants d'installation à partir du Serveur d'installation. Pour plus de détails, reportez-vous à la section "Installation locale de clients UNIX" à la page 142 ou "Installation distante de clients Data Protector" à la page 78.

Procédure de mise à niveau

Pour mettre à niveau Data Protector A.05.10, A.05.50 ou A.06.00 vers Data Protector A.06.10, à l'aide de `rpm`, procédez comme suit :

1. Connectez-vous en tant que `root` et arrêtez les services Data Protector sur le Gestionnaire de cellule en exécutant la commande `/opt/omni/sbin/omnisv -stop`.

   Tapez `ps -ef | grep omni` pour vérifier si tous les services ont bien été arrêtés. Aucun service Data Protector ne doit être répertorié sur exécution de la commande `ps -ef | grep omni`.

2. Désinstallez Data Protector à l'aide de `rpm`.

   Les fichiers de configuration et la base de données sont préservés durant cette procédure.

3. Exécutez la commande `rpm–q` pour vérifier que vous avez bien désinstallé l'ancienne version de Data Protector. Les anciennes versions de Data Protector ne doivent pas figurer dans la liste.

   Assurez-vous que la base de données et les fichiers de configuration sont toujours présents. Les répertoires suivants doivent toujours exister et contenir les fichiers binaires :

   - `/opt/omni`
   - `/var/opt/omni`
   - `/etc/opt/omni`

4. Si vous mettez à niveau un Gestionnaire de cellule, insérez et montez le DVD-ROM d'installation UNIX et utilisez `rpm` pour installer le Gestionnaire de cellule. Pour obtenir des informations détaillées sur la procédure à suivre, reportez-vous à la section "Installation du Gestionnaire de cellule sur des systèmes Linux à l'aide de rpm" à la page 377.

   Si vous mettez à niveau un Serveur d'installation, insérez et montez le DVD-ROM d'installation UNIX et installez le Serveur d'installation. Pour obtenir des informations détaillées sur la procédure à suivre, reportez-vous à la section "Installation d'un Serveur d'installation sur des systèmes Linux à l'aide de rpm" à la page 384.

Paramétrage du protocole TCP/IP sur les systèmes Windows

IMPORTANT :

Seule la mise en œuvre Microsoft du protocole TCP/IP est prise en charge.

Data Protector utilise le protocole TCP/IP pour les communications réseau ; celui-ci doit donc être installé et configuré sur chaque client de la cellule.

La saisie d'une commande via l'interface utilisateur Data Protector établit une connexion avec le Gestionnaire de cellule par le biais du protocole TCP/IP.

Le protocole TCP/IP est un groupe de protocoles et utilitaires reliés entre eux, utilisé pour les communications réseau. Il est constitué des protocoles TCP (Transmission Control Protocol) et IP (Internet Protocol).

Le logiciel TCP/IP est installé sur le disque dur et chaque ordinateur utilisant ce protocole doit posséder les adresses suivantes, généralement attribuées par l'administrateur réseau :

- `Adresse IP` correspondant à chaque carte réseau installée sur l'ordinateur. Il s'agit d'un numéro à 32 bits, généralement présenté sous la forme de quatre nombres séparés par des points.
- `Masque de sous-réseau` correspondant à chaque carte réseau installée sur l'ordinateur qui, associé à l'`adresse IP`, identifie l'ID réseau et l'ID hôte. Le `masque de sous-réseau` se présente dans le même format que l'`adresse IP`.
- L'adresse de la `passerelle par défaut` est requise pour la passerelle locale par défaut (routeur IP) afin de permettre l'accès Internet.

Configuration système requise

Avant d'installer le protocole TCP/IP sur un ordinateur équipé de Windows, vous devez prendre connaissance des informations suivantes :

- Différentes options de configuration sont disponibles selon le type de logiciel Windows installé sur votre ordinateur.
  Un système serveur Windows peut être configuré entre autres en tant que serveur DHCP (Dynamic Host Configuration Protocol), WINS (Windows Internet Name Service) ou DNS (Domain Name System). Pour plus de détails, consultez l'aide en ligne de Windows.
- Vous pouvez configurer le protocole TCP/IP automatiquement à l'aide du DHCP à condition qu'un serveur DHCP soit installé sur votre réseau.
  Vous devez configurer le protocole TCP/IP manuellement si vous ne disposez pas d'un serveur DHCP sur votre réseau ou lorsque vous configurez le protocole TCP/IP sur le système serveur DHCP. Pour plus de détails, consultez l'aide en ligne de Windows.
- Lorsque vous configurez le protocole TCP/IP manuellement, vérifiez que vous êtes bien connecté en tant que membre du groupe Administrateurs sur l'ordinateur local. Pour éviter d'utiliser deux fois une même adresse, veillez à demander toutes les valeurs à votre administrateur réseau. Outre l'`adresse IP`, le `masque de sous-réseau` et la `passerelle par défaut` mentionnés ci-dessus, vous devez obtenir :
  - le nom de votre domaine DNS et les adresses IP des serveurs DNS si vous envisagez d'utiliser des services DNS ;
  - les adresses IP pour les serveurs WINS si des serveurs WINS sont présents sur votre réseau.

Installation et configuration du protocole TCP/IP sous Windows

Le protocole TCP/IP est installé sur les systèmes Windows au moment de l'installation du système d'exploitation.

Pour contrôler les paramètres TCP/IP actuels sur le système Windows 2000, procédez comme suit :

1. Dans le Panneau de configuration Windows, cliquez deux fois sur Connexions réseau et accès à distance puis sur Connexion au réseau local.
2. Cliquez sur Propriétés et double-cliquez sur Protocole Internet (TCP/IP). Vous pouvez alors modifier les paramètres IP.

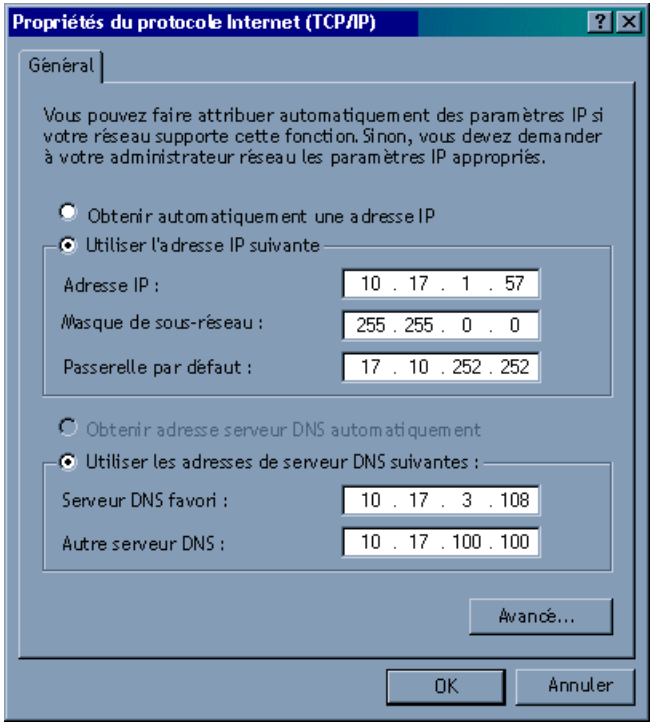

Figure 69 - Fenêtre Propriétés TCP/IP sous Windows

Pour modifier des paramètres avancés, cliquez sur Avancé.

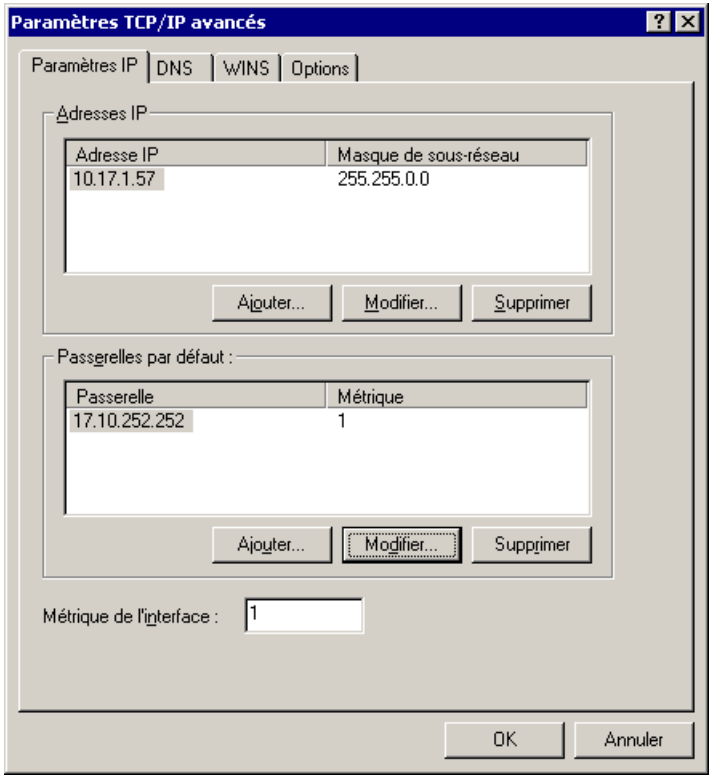

Figure 70 - Paramètres TCP/IP avancés sous Windows

Suffixe DNS

Pour configurer le suffixe DNS sur un système Windows 2000, cliquez avec le bouton droit sur l'icône Poste de travail du bureau, puis cliquez sur Propriétés, Identification réseau, Propriétés, Autres. Les nouveaux paramètres DNS seront pris en compte après le redémarrage du système.

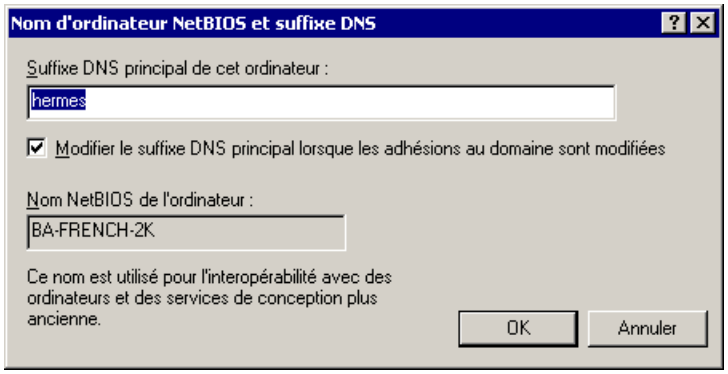

Figure 71 - Suffixe DNS et nom NetBIOS de l'ordinateur sous Windows

Vérification de la configuration TCP/IP

La mise en place d'un mécanisme de résolution des noms d'hôte constitue un élément important du processus de configuration du TCP/IP.

- S'ils utilisent des fichiers d'hôtes enregistrés dans leur dossier `%SystemRoot%\system32\drivers\etc`, tous les systèmes de la cellule doivent pouvoir assurer la résolution de l'adresse du Gestionnaire de cellule et de toutes les machines dotées d'Agents de support et de périphériques de sauvegarde. Le Gestionnaire de cellule doit être en mesure de résoudre les noms de tous les systèmes présents dans la cellule.
- Si vous utilisez un DNS, assurez-vous que le serveur DNS local est configuré correctement et spécifié dans les paramètres IP pour chaque système de la cellule.

Une fois que vous avez installé le protocole TCP/IP, vous pouvez vérifier que sa configuration TCP/IP est correcte à l'aide des utilitaires `ping` et `ipconfig`. Si vous avez modifié les paramètres TCP/IP, redémarrez l'ordinateur.

1. Sur la ligne de commande, tapez `ipconfig /all` pour afficher les informations détaillées sur votre configuration TCP/IP et les adresses qui ont été définies pour votre carte réseau. Assurez-vous que l'adresse IP et le masque de sous-réseau sont définis correctement.
2. Tapez `ping` *`votre_adresse_IP`* pour confirmer l'installation et la configuration du logiciel. Par défaut, vous devez recevoir quatre paquets d'écho.
3. Tapez `ping` *`passerelle_par_défaut`*.

   La passerelle doit être sur votre sous-réseau. Si vous ne parvenez pas à sonder votre passerelle, vérifiez que l'adresse IP de la passerelle est correcte et que la passerelle est opérationnelle.

4. Si vous avez suivi toutes les étapes précédentes sans problème, vous pouvez maintenant tester la résolution de nom. Saisissez le nom du système dans la commande `ping` pour tester le fichier hosts et/ou le DNS. Si le nom de votre machine est par exemple `kesukozi` et le nom de domaine `campo.com`, vous devez taper : `ping kesukozi.campo.com`.

   Si cela ne donne pas de résultat, reportez-vous à la section "Installation et configuration du protocole TCP/IP sous Windows" à la page 392, pour savoir comment accéder à la fenêtre `Propriétés de Protocole Internet (TCP/IP)`. Vérifiez dans cette fenêtre que le nom de domaine est correct. Contrôlez également le fichier hosts et le DNS.

   Assurez-vous que la résolution du nom pour le Gestionnaire de cellule et les clients fonctionne dans les deux sens :

   - Sur le Gestionnaire de cellule, vous devez être en mesure de sonder (faire un ping vers) chaque client.
   - Sur les clients, vous devez être en mesure de sonder (faire un ping vers) le Gestionnaire de cellule et chaque client doté d'un Agent de support.

REMARQUE :

Notez que, lors de l'utilisation du fichier de l'hôte pour la résolution du nom, le test ci-dessus ne garantit pas le fonctionnement de la résolution du nom. Dans ce cas, vous voudrez peut-être utiliser l'outil de vérification DNS une fois Data Protector installé.

IMPORTANT :

Si la résolution du nom, comme spécifiée ci-dessus, ne fonctionne pas, Data Protector ne peut pas être installé correctement.

Notez également que les noms de l'ordinateur Windows et de l'hôte doivent être identiques. Dans le cas contraire, Data Protector émet un avertissement.

Pour vérifier le nom d'hôte, reportez-vous à la section "Installation et configuration du protocole TCP/IP sous Windows" à la page 392, pour savoir comment accéder à la fenêtre `Propriétés de Protocole Internet (TCP/IP)`.

5. Une fois Data Protector installé et une cellule Data Protector créée, vous pouvez utiliser l'outil de vérification DNS pour vérifier que le Gestionnaire de cellule et chaque client sur lequel un Agent de support est installé résolvent correctement les connexions DNS vers tous les autres clients dans la cellule et vice versa. Pour cela, vous devez exécuter la commande `omnicheck -dns` à partir du répertoire *`répertoire_Data_Protector`*`\bin`. Les échecs des vérifications, ainsi que leur nombre sont répertoriés. Pour plus d'informations, reportez-vous à la section "Vérification des connexions DNS dans la cellule Data Protector" à la page 334.

   Pour obtenir des informations détaillées sur la commande `omnicheck`, reportez-vous au *Guide de rfrence de l'interface de ligne de commande HP Data Protector*.

MS Proxy

Si MS Proxy est installé, le port 5555 est occupé et les services Data Protector ne fonctionnent pas. Pour résoudre le problème, procédez comme suit :

1. Créez un fichier nommé `wspcfg.ini`, dans le répertoire *`répertoire_Data_Protector`*`\bin`.
2. Ajoutez au fichier les lignes suivantes :

   ```
   [OmniInet]Disable=1
   ```

Modification du nom du Gestionnaire de cellule

Lorsque Data Protector est installé, il utilise le nom d'hôte en vigueur pour identifier le Gestionnaire de cellule. Si vous changez le nom d'hôte de votre Gestionnaire de cellule, vous devez mettre à jour les fichiers Data Protector manuellement.

IMPORTANT :

Il est nécessaire de mettre à jour les informations du client relatives au nom du Gestionnaire de cellule. Avant de modifier le nom d'hôte de votre Gestionnaire de cellule, exportez les clients à partir de la cellule. Pour connaître la procédure à suivre, reportez-vous à la section "Exportation de clients d'une cellule" à la page 211. Une fois que vous avez modifié le nom d'hôte, réimportez les clients dans la cellule. Pour connaître la procédure à suivre, reportez-vous à la section "Importation de clients dans une cellule" à la page 205.

REMARQUE :

Tous les périphériques et les spécifications de sauvegarde configurés avec l'ancien nom du Gestionnaire de cellule doivent être modifiés en fonction du nouveau nom.

Sous UNIX

Avec un Gestionnaire de cellule UNIX, procédez comme suit :

1. Modifiez les entrées du nom d'hôte du Gestionnaire de cellule dans les fichiers suivants :

   `/etc/opt/omni/client/cell_server`

   `/etc/opt/omni/server/cell/cell_info`

   `/etc/opt/omni/server/users/UserList`

2. Vérifiez que la résolution du nom fonctionne parmi les membres d'une cellule Data Protector.

3. Changez le nom du Gestionnaire de cellule dans la base de données IDB en exécutant la commande suivante :

   `/opt/omni/sbin/omnidbutil -change_cell_name [`*`ancien_hôte`*`]`

Sous Windows

Avec un Gestionnaire de cellule Windows, procédez comme suit :

1. Modifiez les entrées du nom d'hôte du Gestionnaire de cellule dans les fichiers suivants :

   `répertoire_Data_Protector\config\server\cell\cell_info`
   `répertoire_Data_Protector\config\server\users\userlist`

2. Changez le nom du Gestionnaire de cellule dans la clé de registre suivante : `\\HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBack\Site\CellServer`

Modification du numéro de port par défaut

Modification du numéro de port par défaut de Data Protector

Le service (processus) Data Protector `Inet`, lequel lance les autres processus nécessaires pour la sauvegarde et la restauration, doit utiliser le même nombre de ports sur chaque système de la cellule.

Par défaut, Data Protector utilise le numéro de port 5555. Pour vérifier que ce numéro de port n'est pas utilisé par un autre programme, vous devez afficher `/etc/services` pour les systèmes UNIX ou exécuter la commande `netstat -a` commande sur les systèmes Windows. Si le numéro de port 5555 est déjà utilisé par un autre programme, vous devez modifier cette valeur et la remplacer par un numéro de port encore inutilisé. Si le numéro de port n'est pas disponible sur les systèmes client seulement, vous pouvez le modifier après l'installation du Gestionnaire de cellule. Si le numéro de port n'est pas

disponible sur le système sur lequel installer le Gestionnaire de cellule, vous devez modifier ce numéro avant l'installation.

UNIX

Pour modifier le numéro de port sur un système UNIX, procédez comme suit :

- Avant d'installer le Gestionnaire de cellule :
  Créez le fichier `/tmp/omni_tmp/socket.dat` avec le numéro de port requis.
- Une fois le Gestionnaire de cellule installé :
  1. Editez le fichier `/etc/services`. Par défaut, ce fichier doit contenir l'entrée suivante :

     ```
     omni 5555/tcp # DATA-PROTECTOR
     ```

     Remplacez le numéro `5555` par un numéro de port inutilisé.
  2. Si les fichiers `/etc/opt/omni/client/customize/socket` et `/opt/omni/newconfog/etc/opt/omni/client/customize/socket` figurent sur le système, mettez à jour leur contenu avec le numéro de port requis.
  3. Redémarrez le service `Inet` en terminant le processus concerné à l'aide de la commande `kill -HUP` *`inetd_pid`*. Pour déterminer l'ID de processus (*`inetd_pid`*), tapez la commande `ps -ef`.
  4. Dans le fichier d'options globales, redéfinissez la variable `Port`.
  5. Redémarrez les services Data Protector :

     ```
     /opt/omni/sbin/omnisv stop
     /opt/omni/sbin/omnisv start
     ```

Windows

Pour modifier le numéro de port sur un système Windows, procédez comme suit :

- Avant d'installer le Gestionnaire de cellule :
  1. Dans la ligne de commande, exécutez `regedit` pour ouvrir l'Editeur du Registre.
  2. Créez l'entrée de registre `InetPort` sous la clé `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\ OpenView\OmniBackII\Common`.

     Nom de l'entrée de registre : `InetPort`

     Type de l'entrée de registre : `REG_SZ (chaîne)`

     Valeur de l'entrée de registre : *`numéro_port`*
- Une fois le Gestionnaire de cellule installé :

1. Dans la ligne de commande, exécutez `regedit` pour ouvrir l'Editeur du Registre.
2. Développez HKEY_LOCAL_MACHINE, Software, Hewlett-Packard, OpenView, OmniBack et sélectionnez Common.
3. Cliquez deux fois sur InetPort pour ouvrir la fenêtre Modification de la chaîne. Dans le champ Données de la valeur, saisissez un numéro de port non utilisé. Procédez de même dans le sous-dossier `Parameters` du dossier `Common`.
4. Dans le panneau de configuration Windows, accédez à Outils d'administration, Services, puis sélectionnez le service Data ProtectorInet et redémarrez le service (cliquez sur l'icône Redémarrer dans la barre d'outils).

Novell NetWare

Pour modifier le numéro de port sur un système Novell NetWare, procédez comme suit :

1. Assurez-vous qu'aucune session Data Protector n'est en cours d'exécution dans la cellule.
2. A partir de la console Novell NetWare, exécutez la commande `UNLOAD HPINET`.
3. Ouvrez le fichier `AUTOEXEC.NCF` et recherchez la ligne suivante :

   ```
   LOAD HPINET.NLM -PORT 5555
   ```

   Remplacez l'entrée `5555` par un numéro de port inutilisé.
4. Ouvrez le fichier `SYS:\ETC\SERVICES` et ajoutez la ligne suivante :

   omni *NuméroPort*/tcp

   NuméroPort doit être identique au numéro de port utilisé à l'étape 3 de cette procédure.
5. A partir de la console Novell NetWare, exécutez la commande `WS2_32 RELOAD SERVICES` pour que le système lise à nouveau le fichier `SYS:\ETC\SERVICES`.
6. Exécutez la commande `LOAD HPINET` pour recharger `HPINET`.

Modification du numéro de port par défaut pour l'interface graphique Java

Pour modifier le numéro de port du serveur d'interface Java, procédez comme suit :

1. Copiez la variable `JGUI_BBC_SERVER_PORT` dans le fichier `omnirc` et attribuez-lui la valeur d'un numéro de port inutilisé.

   Par exemple :

   ```
   JGUI_BBC_SERVER_PORT=5557
   ```

2. Redémarrez les services Data Protector :

   ```
   omnisv –stop
   omnisv –start
   ```

Un client d'interface Java doit utiliser le même port pour se connecter au service `UIProxy`.

Lors de la connexion au Gestionnaire de cellule, entrez *`NomGestionnaireCellule:NuméroPort`* dans la boîte de dialogue Se connecter à un Gestionnaire de cellule et cliquez sur Connecter.

Par exemple :

`mycellmanager:5557`

Préparation d'un serveur NIS

Cette procédure permet à votre serveur NIS de reconnaître votre Gestionnaire de cellule Data Protector.

Pour ajouter les informations sur Data Protector au serveur NIS, procédez comme suit :

1. Connectez-vous comme utilisateur `root` sur le serveur `NIS`.
2. Si vous gérez le fichier `/etc/services` via `NIS`, ajoutez la ligne suivante au fichier `/etc/services` :

   ```
   omni 5555/tcp # Data Protector for Data Protector inet
   server
   ```

   Remplacez 5555 par un autre numéro si ce port n'est pas disponible. Reportez-vous à la section "Modification du numéro de port par défaut de Data Protector" à la page 398.

   Si vous gérez le fichier `/etc/inetd.conf` via `NIS`, ajoutez la ligne suivante au fichier `/etc/inetd.conf` :

   ```
   #Data Protector
   omni stream tcp nowait root /opt/omni/lbin/inet -log
   /var/opt/omni/log/inet.log
   ```

3. Exécutez la commande suivante pour que le serveur `NIS` lise le fichier et mette à jour la configuration.

   ```
   cd /var/yp; make
   ```

REMARQUE :

Dans l'environnement `NIS`, le fichier `nsswitch.conf` définit l'ordre dans lequel les différents fichiers de configuration seront utilisés. Vous pouvez par exemple définir que le fichier `/etc/inetd.conf` soit utilisé sur la machine locale ou à partir du serveur `NIS`. Vous pouvez également ajouter une phrase au fichier indiquant que le fichier `nsswitch.conf` contrôle l'emplacement où les noms sont conservés. Pour plus de détails, reportez-vous aux pages du manuel correspondantes.

Si vous avez déjà installé Data Protector, vous devez préparer le serveur `NIS`, puis redémarrer le service `inet` en arrêtant le processus concerné ; pour cela, utilisez la commande `kill -HUP pid` sur chaque client constituant à la fois un client `NIS` et un client Data Protector.

Dépannage

- Si le service `Inet Data Protector` ne démarre pas après l'installation de Data Protector dans votre environnement NIS, vérifiez le fichier `/etc/nsswitch.conf`. Si vous trouvez la ligne suivante :
  ```
  services: nis [NOTFOUND=RETURN] files
  ```
  remplacez-la par :
  ```
  services: nis [NOTFOUND=CONTINUE] files
  ```

Utilisation de pilotes de bandes et de pilotes de robots sous Windows

Data Protector prend en charge les pilotes de bandes natifs pour les lecteurs à bandes compatibles rattachés à un système Windows. Les pilotes natifs Windows chargés pour les périphériques changeurs de support (robots) ne sont pas pris en charge par Data Protector.

Dans les exemples ci-dessous, un lecteur de bandes HP 4 mm DDS est relié au système Windows. Vous devez désactiver le pilote natif chargé pour les périphériques changeurs de support si le périphérique à bandes HP 4 mm DDS est connecté à un système Windows et configuré pour être utilisé avec Data Protector. Vous trouverez dans la section ci-dessous la description des procédures correspondantes.

Lecteurs de bandes

Un pilote est généralement fourni avec Windows, si le périphérique est répertorié dans la liste de compatibilité matérielle (HCL). Cette liste regroupe les périphériques supportés par Windows. Vous pouvez la trouver sur Internet, à l'adresse suivante:

http://www.microsoft.com/whdc/hcl/default.mspx

Les pilotes de périphérique sont chargés automatiquement pour tous les périphériques activés une fois que l'ordinateur a été démarré. Il est inutile de charger séparément le pilote de bandes natif, mais vous pouvez le mettre à jour. Pour mettre à jour ou remplacer le pilote de bandes natif sur un système Windows, procédez comme suit :

1. Dans le Panneau de configuration Windows, cliquez deux fois sur Outils d'administration.
2. Dans la fenêtre Outils d'administration, cliquez deux fois sur Gestion de l'ordinateur. Cliquez sur Gestionnaire de périphériques.
3. Développez Lecteurs de bande. Pour savoir quel pilote est actuellement chargé pour le périphérique, cliquez avec le bouton droit de la souris sur le lecteur de bandes, puis sélectionnez Propriétés.
4. Cliquez sur l'onglet Pilote, puis sur Mettre à jour le pilote. Reportez-vous à la Figure 72 à la page 404. Suivez ensuite les instructions de l'assistant. Vous pouvez indiquer si vous souhaitez mettre à jour le pilote de bandes natif actuellement installé ou le remplacer par un autre.
5. Redémarrez le système pour appliquer les modifications.

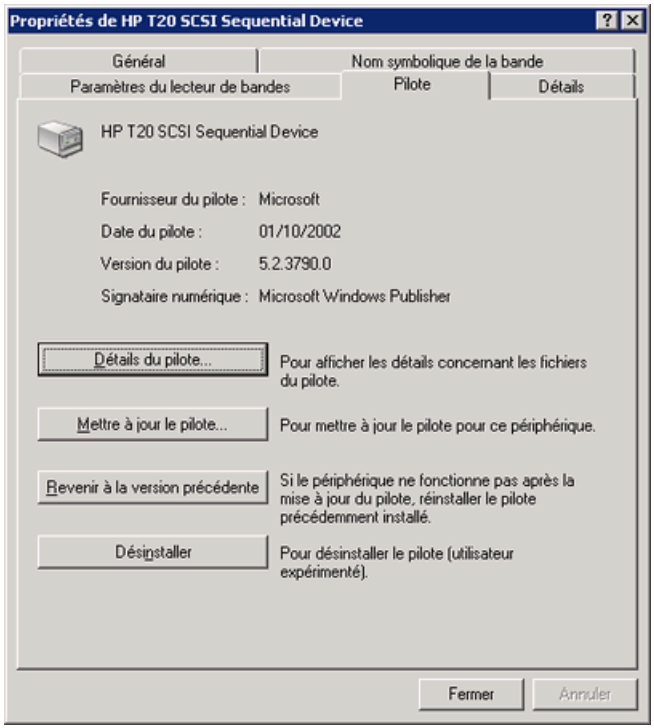

Figure 72 - Propriétés du pilote

IMPORTANT :

Si vous avez déjà configuré un périphérique pour Data Protector sans utiliser le pilote de bandes natif, vous devez renommer les fichiers de périphérique pour tous les périphériques de sauvegarde Data Protector configurés qui font référence au lecteur de bandes en question (par exemple, remplacez `scsi1:0:4:0` par `tape3:0:4:0`).

Pour plus de détails, reportez-vous à la section "Création de fichiers de périphérique (adresses SCSI) sous Windows" à la page 406.

Pilotes de robots

Sous Windows, les pilotes de robots sont automatiquement chargés pour les bibliothèques à bande activées. Pour pouvoir utiliser le robot de bibliothèque avec Data Protector, vous devez désactiver le pilote correspondant.

L'exemple ci-dessous présente une bibliothèque de bandes HP 1557A utilisant des bandes DDS 4 mm. Pour désactiver le pilote de robots `(ddsmc.sys)` chargé automatiquement sur un système Windows, procédez comme suit :

1. Dans le Panneau de configuration Windows, cliquez deux fois sur Outils d'administration.
2. Dans la fenêtre Outils d'administration, cliquez deux fois sur Gestion de l'ordinateur. Cliquez sur Gestionnaire de périphériques.
3. Dans la zone de résultats de la fenêtre Gestionnaire de périphériques, développez Changeurs de support.
4. Pour savoir quel pilote est actuellement chargé, cliquez avec le bouton droit de la souris sur Changeur de support DDS 4mm, puis sur Propriétés.

   Cliquez sur l'onglet Pilote, puis sur Détails du pilote. La fenêtre suivante s'affiche :

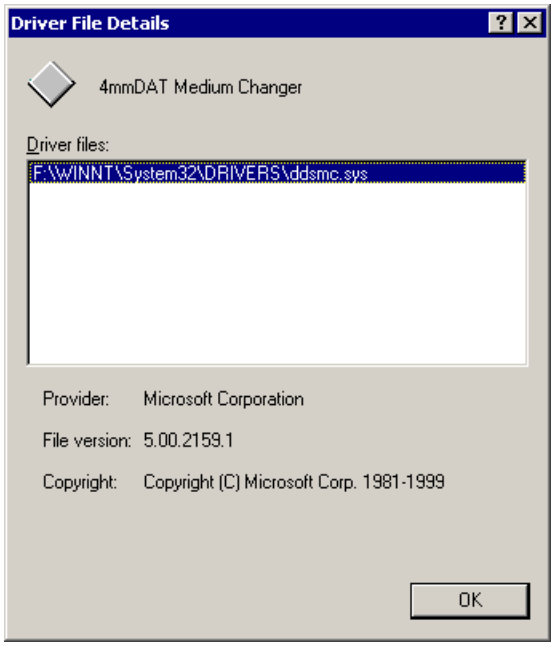

Figure 73 - Propriétés du changeur de support

Pour désactiver le pilote de robots natif, cliquez avec le bouton droit de la souris sur Changeur de support DDS 4mm, puis sélectionnez Désactiver.

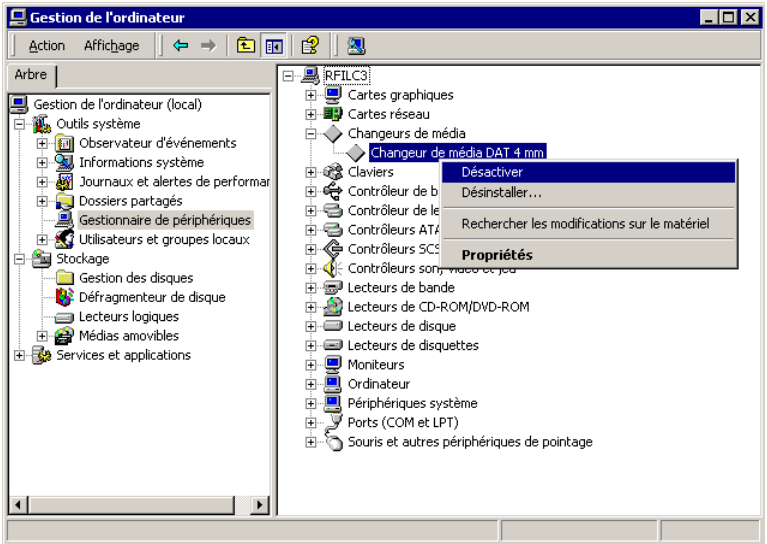

Figure 74 - Désactivation des pilotes de robots

5. Redémarrez le système pour appliquer les modifications. Vous pouvez alors configurer le robot avec Data Protector.

Création de fichiers de périphérique (adresses SCSI) sous Windows

La syntaxe à utiliser pour le fichier du périphérique à bandes est différente si le pilote de bandes natif a été chargé (`tapeN:B:T:L`) ou s'il a été déchargé (`scsiP:B:T:L`) pour un lecteur de bandes.

Windows avec le pilote de bandes natif

Pour créer un fichier de périphérique pour un lecteur de bande connecté à un système Windows utilisant le pilote de bandes natif, procédez comme suit :

1. Dans le Panneau de configuration Windows, cliquez deux fois sur Outils d'administration.
2. Dans la fenêtre Outils d'administration, cliquez deux fois sur Gestion de l'ordinateur. Développez Supports amovibles, puis Emplacements physiques. Cliquez avec le bouton droit de la souris sur le lecteur de bandes, puis sélectionnez Propriétés.
3. Si le pilote de bandes d'origine est chargé, le nom du fichier du périphérique s'affiche dans la page des propriétés générales. Sinon, vous pouvez trouver les informations utiles dans la page de propriétés Informations sur le périphérique. Reportez-vous à la Figure 75 à la page 407.

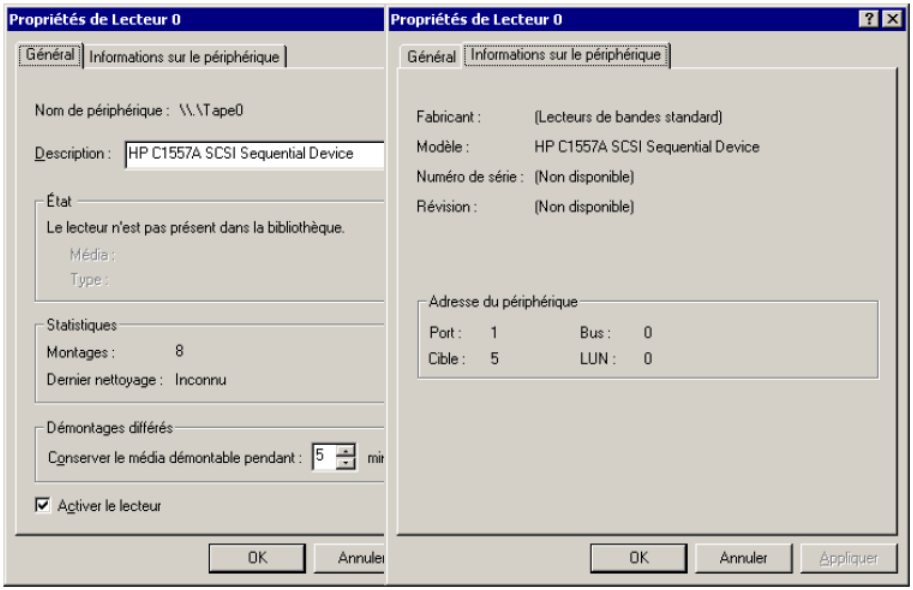

Figure 75 - Propriétés du lecteur de bande

Le nom de fichier pour le lecteur de bandes présenté dans la Figure 75 à la page 407 est créé comme suit :

Pilote de bandes natif utilisé	`Tape0` ou `Tape0:0:5:0`
Pilote de bandes natif NON utilisé	`scsii1:0:5:0`

Périphériques magnéto-optiques

Si vous connectez un périphérique magnéto-optique à un système Windows, une lettre de lecteur lui est attribuée après le réamorçage du système. Cette lettre est ensuite utilisée lorsque vous créez le fichier du périphérique. Par exemple, `E:` est le fichier de périphérique créé pour un lecteur magnéto-optique auquel la lettre de lecteur `E` a été attribuée.

Configuration de robot SCSI sous HP-UX

Sur les systèmes HP-UX, un pilote de passage SCSI est utilisé pour gérer le contrôleur SCSI *et* le périphérique de contrôle (appelé également robot ou sélectionneur) des périphériques de bibliothèque de bandes (tels que HP StorageWorks 12000e). Dans une bibliothèque, le périphérique de contrôle est utilisé pour charger/décharger les supports vers/depuis les lecteurs et importer/exporter les supports vers/depuis un périphérique de ce type.

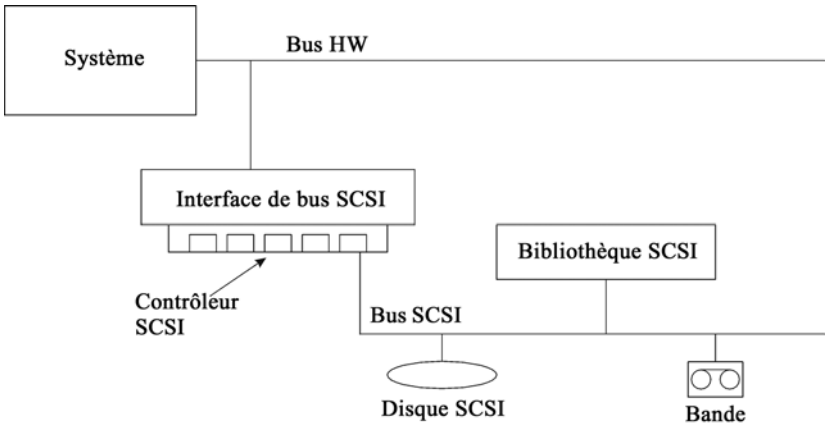

Figure 76 - Périphériques SCSI contrôlés

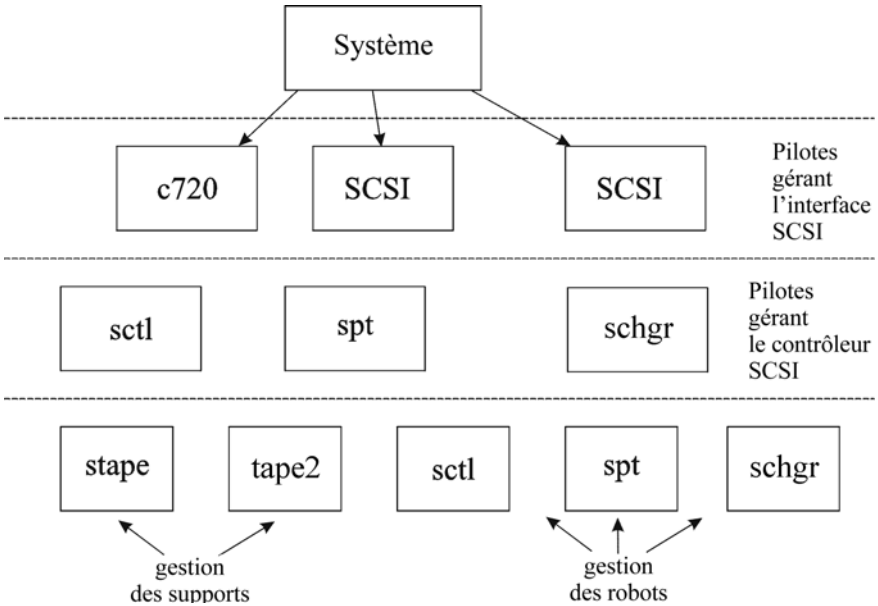

Figure 77 - Gestion des périphériques

Le type de pilote de robot SCSI utilisé dépend du matériel. Les systèmes équipés du bus `GSC/HSC` ou `PCI` sont dotés du pilote de changeur automatique SCSI nommé `schgr`, tandis que les systèmes équipés du bus `EISA` possèdent le pilote de passage SCSI nommé `sctl`, lequel est déjà intégré dans le noyau. En revanche, le pilote de passage

SCSI utilisé sur les serveurs HP avec un bus NIO est nommé `spt`. Il est installé sur le système sans être intégré par défaut au noyau.

Si le pilote de robot SCSI n'a pas encore été relié à votre noyau actuel, vous devez l'ajouter manuellement et l'attribuer au robot des bibliothèques de bandes connectées.

Pour ajouter *manuellement* le pilote de robot SCSI au noyau et en recréer un autre manuellement, suivez la procédure ci-dessous.

CONSEIL :

Sur la plate-forme HP-UX, vous pouvez également créer le noyau à l'aide de l'utilitaire *HP System Administration Manager (SAM)*. Reportez-vous à la section "Installation de clients HP-UX" à la page 94 du Chapitre 2.

Utilisez la commande `/opt/omni/sbin/ioscan -f` pour savoir si le pilote de robot SCSI est attribué à la bibliothèque que vous souhaitez configurer.

```
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
```

Figure 78 - Etat du pilote de passage SCSI (sctl)

La Figure 78 à la page 409 vous indique le pilote de passage SCSI `sctl` affecté au périphérique de contrôle du périphérique à bandes Exabyte. Le chemin matériel correspondant (H/W Path) est `8/12.2.0`. (SCSI=2, LUN=0).

Un lecteur de bandes est connecté au même bus SCSI, mais le pilote qui le contrôle est `stape`. Le chemin de matériel correspondant (H/W Path) est `8/12.1.0`. (SCSI=0, LUN=0)

IMPORTANT :

L'adresse SCSI 7 est toujours utilisée par les contrôleurs SCSI, bien que la ligne correspondante n'apparaisse pas forcément dans les résultats de la commande `ioscan -f`. Dans cet exemple, le contrôleur est géré par `sctl`.

```
# 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
#
```

Figure 79 - Etat du pilote de passage SCSI - spt

La Figure 79 à la page 410 donne un exemple de périphérique à bandes connecté, avec un robot contrôlé par le pilote de passage SCSI `spt`. Le périphérique en question est un périphérique de bibliothèque de bandes HP StorageWorks 12000e qui utilise l'adresse SCSI 4 et est connecté au bus SCSI avec le chemin matériel 52. Le chemin matériel correspondant est 52.4.1. Le robot est correctement affecté au pilote de passage SCSI `spt`.

Si le pilote `sctl`, `spt` ou `schgr` n'est pas affecté au robot, vous devez ajouter le chemin matériel du robot à l'instruction du pilote dans le fichier `system`, puis recréer le noyau. Pour cela, suivez la procédure ci-dessous.

Pour ajouter *manuellement* un pilote de robot SCSI au noyau, l'affecter au robot, puis recréer manuellement un nouveau noyau, procédez comme suit :

1. Connectez-vous comme utilisateur *root*, puis basculez vers le répertoire build :

   ```
   cd /stand/build
   ```

2. Créez un fichier système à partir du noyau existant :

   ```
   /usr/lbin/sysadm/system_prep -s system
   ```

3. Vérifiez quel pilote de robot SCSI est déjà intégré au kernel en cours. A partir du répertoire `/stand`, tapez la commande suivante :

   grep *`pilote de robot SCSI`*system

   où *`pilote de robot SCSI`* peut être `spt`, `sctl` ou `schgr`. Le système affiche alors la ligne correspondante si le pilote est déjà intégré au noyau en cours.

4. Utilisez un éditeur pour ajouter une instruction de pilote :

   `driver` *`chemin matériel`* `spt`

   au fichier `/stand/build/system`, où *`chemin matériel`* correspond au chemin matériel complet du périphérique.

   Pour la bibliothèque de bandes HP StorageWorks 12000e de l'exemple précédent, vous auriez saisi :

   ```
   driver 52.4.1 spt
   ```

   Si plusieurs bibliothèques sont connectées au même système, vous devez ajouter une ligne de pilote pour chaque robot de bibliothèque, avec le chemin matériel approprié.

   Lorsque vous configurez le pilote `schgr`, ajoutez la ligne suivante à l'instruction de pilote :

   ```
   schgr
   ```

5. Tapez la commande `mk_kernel -s./system` pour construire un nouveau noyau.

6. Enregistrez l'ancien fichier system sous un autre nom et renommez le nouveau fichier system avec le nom initial pour qu'il devienne le fichier en vigueur :

   ```
   mv /stand/system /stand/system.prev
   mv /stand/build/system /stand/system
   ```

7. Enregistrez l'ancien kernel sous un autre nom et renommez le nouveau kernel avec le nom initial pour qu'il deviennent le kernel en vigueur :

   ```
   mv /stand/vmunix /stand/vmunix.prev
   mv /stand/vmunix_test /stand/vmunix
   ```

8. Réamorcez le système à partir du nouveau noyau en tapant la commande suivante:

   ```
   shutdown -r 0
   ```

9. Après le réamorçage du système, vérifiez vos modifications à l'aide de la commande /usr/sbin/ioscan -f.

Création de fichiers de périphérique sous HP-UX

Configuration système requise

Avant de créer un fichier de périphérique, le périphérique de sauvegarde doit être connecté au système. Utilisez la commande `/usr/sbin/ioscan -f`. pour vérifier que le périphérique est correctement connecté. Utilisez la commande `/usr/sbin/infs -e` pour créer automatiquement les fichiers de périphérique pour certains périphériques de sauvegarde.

Si les fichiers de périphérique correspondant à un périphérique de sauvegarde particulier n'ont pas été créés lors de l'initialisation du système (processus d'amorçage) ou après exécution de la commande `infs -e`, vous devez les créer manuellement. Cela concerne notamment les fichiers de périphérique requis pour la gestion du périphérique de contrôle de bibliothèque (robot de bibliothèque).

Prenons l'exemple de la création d'un fichier de périphérique pour le robot du périphérique de bibliothèque HP StorageWorks 12000e connecté à un système HP-UX. Le fichier de périphérique correspondant au lecteur de bandes a déjà été créé automatiquement après la réinitialisation du système, tandis que le fichier de périphérique correspondant au périphérique de contrôle doit être créé manuellement.

La Figure 79 à la page 410 vous présente les résultats de la commande `ioscan -f` sur le système HP-UX sélectionné.

```
# 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
#
```

Figure 80 - Liste des périphériques connectés

L'interface du bus SCSI est contrôlée par le pilote système `scsi1`. Il s'agit d'une interface `SCSI NIO`. Pour accéder au robot de bibliothèque sur le bus `SCSI NIO`, il faut utiliser le pilote de passage SCSI `spt` qui est déjà installé et affecté au robot du périphérique à bandes HP StorageWorks 12000e, lequel utilise le chemin matériel `52.4.1`.

REMARQUE :

Si vous n'utilisez pas une interface de bus basée sur `SCSI NIO`, le pilote `spt` n'est pas nécessaire, mais le pilote `sctl` est utilisé à sa place.

Pour créer un fichier de périphérique, vous devez connaître le *numéro majeur* du pilote de passage SCSI et le *numéro mineur*, qui ne dépend pas du pilote de passage SCSI que vous utilisez.

Pour obtenir le *numéro majeur* correspondant au `spt`, exécutez la commande suivante :

```
lsdev -d spt
```

Dans notre exemple (voir la Figure 80 à la page 412), la commande renvoie le *numéro majeur* `75`.

Pour obtenir le *numéro majeur* correspondant au `sctl`, exécutez la commande suivante :

```
lsdev -d sctl
```

Dans notre exemple, la commande renvoie le *numéro majeur* `203`.

Le *numéro mineur*, indépendamment du pilote de passage SCSI utilisé, se présente sous la forme suivante :

```
0xIITL00
```

`II` -> *Numéro d'instance* de l'interface du bus SCSI (PAS celui du périphérique) consigné dans les résultats de la commande `ioscan -f` et se trouvant dans la deuxième colonne libellée `I`. Dans cet exemple, le numéro d'instance est `0`, il faut donc entrer deux chiffres hexadécimaux : 00.

`T` -> L'adresse SCSI du robot de bibliothèque. Dans cet exemple, l'adresse SCSI est `4` ; il faut donc entrer `4`.

`L` -> Numéro LUN du robot de bibliothèque. Dans cet exemple, le numéro LUN est `1` ; il faut donc entrer `1`.

`00` -> Deux zéros hexadécimaux.

Création du fichier de périphérique

Pour créer le fichier de périphérique, utilisez la commande suivante :

```
mknod /dev/spt/nom_fichier_périphérique c Num_majeur Num_mineur
```

Les fichiers de périphérique `spt` se trouvent généralement dans le répertoire `/dev/spt` ou `/dev/scsi`. Dans cet exemple, nous appelons le fichier du périphérique de contrôle `/dev/spt/SS12000e`.

Par conséquent, la commande complète à utiliser pour la création d'un fichier de périphérique nommé `SS12000e` dans le répertoire `/dev/spt` est la suivante :

```
mknod /dev/spt/SS12000e c 75 0x004100
```

Pour créer un fichier de périphérique correspondant à `sctl`, nommé SS12000e et situé dans le répertoire `/dev/scsi`, la commande complète à utiliser est la suivante :

```
mknod /dev/scsi/SS12000e c 203 0x004100
```

Configuration des paramètres du contrôleur SCSI

Data Protector permet de modifier la taille de bloc du périphérique. Pour ce faire, vous devez procéder à une configuration supplémentaire de certains contrôleurs SCSI : pour permettre l'écriture de tailles de bloc supérieures à 64 Ko, la configuration des paramètres de certains contrôleurs SCSI doit être modifiée.

Pour définir les paramètres de contrôleur SCSI sur un système Windows, vous devez modifier la valeur de registre des contrôleurs SCSI Adaptec et de certains contrôleurs dotés de chipsets Adaptec :

1. Définissez la valeur de registre suivante : `\\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aic78xx\Parameters\Device0\MaximumSGList`
2. Saisissez une valeur `DWORD` contenant le nombre de blocs de 4 Ko augmenté de un.

   ```
   MaximumSGList = (OBBlockSize en Ko / 4) + 1
   ```

   Par exemple, pour permettre l'écriture de blocs dont la taille peut atteindre 260 Ko, `MaximumSGList` doit être au moins égal à `(260 / 4) + 1 = 66`.
3. Redémarrez le système.

REMARQUE :

La valeur de registre définit la limite supérieure de la taille de bloc. Pour configurer la taille de bloc en cours pour un périphérique, vous devez utiliser l'interface graphique utilisateur de Data Protector.

Recherche des adresses SCSI non utilisées sous HP-UX

Le contrôle et l'accès à un périphérique de sauvegarde connecté à un système HP-UX se font via un fichier de périphérique qui doit se trouver sur chaque périphérique physique. Avant de créer le fichier de périphérique, vous devez rechercher quelles adresses SCSI (ports) restent inutilisées et disponibles pour un nouveau périphérique.

Sous HP-UX, utilisez la commande système `/usr/sbin/ioscan -f` pour afficher la liste des adresses SCSI déjà occupées. Les adresses qui ne figurent pas dans la liste obtenue par la commande `/usr/sbin/ioscan -f` sont par conséquent inutilisées.

La Figure 81 à la page 415 présente les résultats de la commande `/usr/sbin/ioscan -f` sur un système HP-UX 11.x.

```
# 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
#
```

Figure 81 - Résultats de ioscan -f sur un système HP-UX

Seules la troisième `(chemin H/W)` et la cinquième `(état S/W)` colonnes sont utiles pour déterminer les adresses SCSI disponibles. Un format de `(chemin H/W)` démembré se présenterait sous la forme suivante :

`Chemin_H/W_bus_SCSI.adresse_SCSI.numéro_LUN`

Dans ce cas particulier, il n'y a qu'un bus SCSI, qui utilise le chemin H/W 52. Pour ce bus, vous pouvez utiliser les adresses SCSI `0` et 3, puisqu'elles ne figurent pas dans la liste.

La Figure 81 à la page 415 vous indique quelles sont les adresses du bus SCSI sélectionné qui sont déjà occupées :

- L'adresse SCSI 1 est occupée par un disque SCSI.
- L'adresse SCSI 2 est occupée par un CD-ROM.
- L'adresse SCSI 4, LUN 0, est occupée par un lecteur de bandes.
- L'adresse SCSI 4, LUN 1, est occupée par la bibliothèque de bandes.
- L'adresse SCSI 5 est occupée par un disque SCSI.
- L'adresse SCSI 6 est occupée par un disque SCSI.
- L'adresse SCSI 7 est occupée par un contrôleur SCSI.

REMARQUE :

Bien que l'adresse SCSI numéro 7 *ne* figure *pas* dans la liste, elle est occupée par défaut par le contrôleur SCSI.

Pour tous les périphériques, la valeur `Etat S/W` est définie à `UTILISE` (CLAIMED) et la valeur `Type H/W` est définie à `PERIPHERIQUE` (H/W DEVICE) ce qui signifie que les périphériques sont actuellement connectés. Si une valeur `INUTILISE` (UNCLAIMED) figurait dans la colonne `Etat S/W` ou `AUCUN PERIPHERIQUE` (NO H/W) dans la colonne `Type H/W`, cela signifierait que le système ne peut pas accéder au périphérique.

L'adresse SCSI 4 est demandée par la bibliothèque de bandes, dotée du lecteur de bandes avec le LUN 0 et du robot avec le LUN 1. Le lecteur est contrôlé par le pilote `tape2` et le robot par le pilote de passage SCSI `spt`. Dans la description, vous pouvez constater que le périphérique est une bibliothèque HP StorageWorks 12000e ; celle-ci est facilement reconnaissable parmi les autres bibliothèques SCSI car elle utilise la même adresse SCSI pour le lecteur de bandes et le robot, mais avec des LUN différents.

Tout le bus SCSI est contrôlé par le module d'interface `scsi1`.

Recherche des ID SCSI cibles inutilisés sous Solaris

L'accès et le contrôle d'un périphérique de sauvegarde connecté à un système Solaris se fait via un fichier de périphérique. Ce fichier de périphérique est automatiquement créé par le système d'exploitation Solaris dans le répertoire `/dev/rmt`, au moment de la connexion du périphérique de sauvegarde et de la mise sous tension du système client et du périphérique de sauvegarde.

Toutefois, avant de connecter le périphérique de sauvegarde, les adresses SCSI disponibles doivent être vérifiées et l'adresse du périphérique de sauvegarde doit être établie sur une adresse non encore allouée.

Pour répertorier les adresses SCSI disponibles sur un système Solaris, procédez comme suit :

1. Arrêtez le système en appuyant sur Stop et A.
2. A l'invite ok, exécutez la commande probe-scsi-all :

   probe-scsi-all

   Le système peut vous demander de lancer la commande `reset-all` avant d'exécuter la commande `probe-scsi-all`.
3. Pour revenir au fonctionnement normal, tapez go à l'invite `ok` :

   `go`

Après avoir répertorié les adresses disponibles et choisi celle que vous souhaitez utiliser pour votre périphérique de sauvegarde, vous devez mettre à jour les fichiers de configuration appropriés avant de connecter et de démarrer le périphérique. Reportez-vous à la section suivante pour obtenir des instructions sur la mise à jour des fichiers de configuration.

Mise à jour de la configuration des périphériques et pilotes sur un système Solaris

Mise à jour des fichiers de configuration

Les fichiers de configuration suivants servent à la configuration du périphérique et du lecteur. Ils doivent être vérifiés, et modifiés le cas échéant, avant que les périphériques connectés ne puissent être utilisés :

- `st.conf`
- `sst.conf`

st.conf : tous les périphériques

Ce fichier est requis sur tout client Solaris Data Protector auquel est connecté un périphérique à bandes. Il doit contenir des informations sur le périphérique et une ou plusieurs adresses SCSI pour chaque périphérique de sauvegarde connecté au client. Une seule entrée SCSI est requise pour un périphérique à lecteur unique, tandis qu'il en faut plusieurs pour un périphérique de bibliothèque multi-lecteurs.

1. Vérifiez quelles sont les adresses SCSI inutilisées sur le client, tel que le décrit la section précédente, et choisissez une adresse pour le périphérique à connecter.
2. Définissez les adresses SCSI choisies sur le périphérique de sauvegarde.
3. Eteignez le système client.
4. Connectez le périphérique de sauvegarde.
5. Remettez le périphérique sous tension, puis le système client.
6. Arrêtez le système en appuyant sur `Stop` et `A`.
7. A l'invite `ok`, tapez la commande probe-scsi-all :

   ```
   probe-scsi-all
   ```

   Cela permet de fournir des informations sur les périphériques SCSI connectés, notamment la chaîne d'identification correcte du périphérique de sauvegarde nouvellement connecté.
8. Revenez en fonctionnement normal :

   ```
   go
   ```

9. Modifiez le fichier `/kernel/drv/st.conf`. Ce fichier est utilisé par le pilote (bande SCSI) `st` de Solaris. Il contient une liste des périphériques officiellement pris en charge par Solaris, ainsi qu'un ensemble de saisies de configuration pour des périphériques tiers. Si vous utilisez un périphérique non pris en charge, il devrait être possible de le connecter et de l'utiliser sans configuration supplémentaire. Sinon, vous pouvez ajouter les types d'entrée suivants dans le fichier `st.conf` :

   - Une entrée de liste de configuration de bande (plus une définition de variable de données de bandes). Des exemples d'entrées, accompagnés de commentaires, sont fournis dans le fichier. Si l'un d'eux vous convient, vous pouvez l'utiliser ; vous pouvez également les modifier pour les adapter à vos besoins.
     L'entrée doit venir avant la première entrée `name=` du fichier et le format requis est le suivant :
     tape-config-list= "*`périphérique à bandes`*", "*`nom de référence du périphérique à bandes`*", "*`données de bandes`*";
     où :

`périphérique à bande`	Chaîne d'identification du fournisseur et du produit pour le périphérique à bandes. Celui-ci doit être correctement spécifié, en conformité avec la documentation du constructeur du périphérique.
`nom de référence du périphérique à bandes`	Nom que vous choisissez, par lequel le système identifiera le périphérique à bandes. Ce nom ne modifie pas l'identification du produit mais, lorsque le système démarre, c'est le nom de référence qui s'affiche la liste des périphériques reconnus par le système.
`données de bandes`	Variable qui fait référence à des éléments supplémentaires de configuration du périphérique à bandes. La définition de la variable doit elle aussi être indiquée correctement, conformément aux dispositions de la documentation du constructeur du périphérique.

     Par exemple :

```
tape-config-list= ""Quantum DLT4000", "Quantum DLT4000",
"DLT-data";
DLT-data = 1,0x38,0,0xD639,4,0x80,0x81,0x82,0x83,2;
```

Le deuxième paramètre, `0x38`, désigne le type de bande DLT comme "autre lecteur SCSI". La valeur spécifiée ici doit être définie dans `/usr/include/sys/mtio.h`.

REMARQUE :

Assurez-vous que la dernière entrée de la ligne tape-config-list se termine par un point-virgule (;).

- Pour les périphériques multi-lecteurs, ciblez les saisies comme suit :

  ```
  name="st" class="scsi"
  target=X lun=Y;
  ```

  où :

  X correspond au port SCSI affecté au lecteur de données (ou mécanisme du robot).

  Y est la valeur de l'unité logique.

  Par exemple :

  ```
  name="st" class="scsi"
  target=1 lun=0;
  name="st" class="scsi"
  target=2 lun=0
  ```

  Normalement, les entrées cibles sont requises dans le fichier `st.conf` pour les lecteurs uniquement, et non pour le mécanisme du robot, qui est présent sur une autre cible. Elles sont généralement fournies dans le fichier `sst.conf` (voir ci-dessous). En revanche, il existe certains périphériques, tel que le HP StorageWorks 24x6, qui traitent le mécanisme du robot de la même manière qu'un autre lecteur. Dans ce cas, deux entrées avec la même cible sont requises (l'une pour le lecteur, l'autre pour le robot), mais avec des LUN différents.

  Par exemple :

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

sst.conf : périphériques de bibliothèque

Ce fichier requis sur chaque client Solaris Data Protector auquel un périphérique de bibliothèque multi-lecteurs est connecté. D'une manière générale, il requiert une entrée pour l'adresse SCSI du mécanisme de robot de chacun des périphériques de

bibliothèque connectés au client. Il existe cependant quelques exceptions, à l'instar du HP StorageWorks 24x6 mentionné dans la section précédente.

1. Copiez le pilote (module) `sst` et le fichier de configuration `sst.conf` dans le répertoire requis :
   - Pour les systèmes d'exploitation 32 bits :
     ```
     $cp /opt/omni/spt/sst /usr/kernel/drv/sst
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```
   - Pour les systèmes d'exploitation 64 bits :
     ```
     $cp /opt/omni/spt/sst.64bit /usr/kernel/drv/sparcv9 /sst
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```
2. Modifiez le fichier `sst.conf` et ajoutez l'entrée suivante :

   name="sst" class="scsi" target=*X* lun=*Y*;

   où :

   X correspond à l'adresse SCSI du mécanisme du robot.

   Y est l'unité logique.

   Par exemple :

   ```
   name="sst" class="scsi" target=6 lun=0;
   ```
3. Ajoutez le pilote au noyau Solaris :

   ```
   add_drv sst
   ```

Création et vérification de fichiers de périphérique

Après avoir défini les fichiers de configuration et installé les pilotes, vous pouvez créer de nouveaux fichiers de périphérique comme suit :

1. Supprimez tous les fichiers de périphérique existants du répertoire `/dev/rmt` :

   ```
   cd /dev/rmt rm *
   ```
2. Tapez la commande suivante pour arrêter le système :

   ```
   shutdown -i0 -g0
   ```

3. Relancez le système :

   `boot -rv`

   Le commutateur `r` de la commande `boot` permet une compilation du noyau et inclut la création de fichiers de périphérique spéciaux utilisés pour la communication avec le périphérique à bandes. Le commutateur `v` active l'affichage en mode prolixe (verbose) du démarrage du système. Avec le mode prolixe, le système indique que le périphérique est connecté en affichant la chaîne *`nom de référence du périphérique à bandes`* que vous avez sélectionnée lors de la phase de l'initialisation relative à la configuration du répertoire `/devices`.

4. Tapez la commande suivante pour vérifier l'installation :

   `mt -t /dev/rmt/0 status`

   La sortie de cette commande dépend du lecteur configuré. Elle se présente de la manière suivante :

   ```
   Quantum DLT7000 tape drive: sense key(0x6)= Unit Attention
   residual= 0 retries= 0 file no= 0 block no= 0
   ```

5. Une fois que la réinitialisation est terminée, vous pouvez vérifier les fichiers de périphérique qui ont été créés à l'aide de la commande `ls -all`. Pour un périphérique de bibliothèque, le résultat de cette commande peut être le suivant :

/dev/rmt/0hb	pour un premier lecteur de bandes
/dev/rmt/1hb	pour un deuxième lecteur de bandes
/dev/rsst6	pour un lecteur de robot

Recherche des ID SCSI cibles inutilisés sur un système Windows

Pour déterminer quels sont les ID SCSI cibles (adresses SCSI) inutilisés sur un système Windows, procédez comme suit :

1. Dans le Panneau de configuration Windows, cliquez deux fois sur Adaptateurs SCSI.
2. Vérifiez les propriétés de chaque périphérique connecté à une carte SCSI de la liste. Cliquez deux fois sur le nom d'un périphérique, puis sélectionnez Paramètres pour ouvrir sa page de propriétés. Reportez-vous à la Figure 82 à la page 422.

   Notez les `ID SCSI cibles` et les `LUN (Numéros d'unité logique)` affectés au périphérique. Vous pouvez ainsi savoir quels sont les `ID SCSI cibles` et `LUN` déjà occupés.

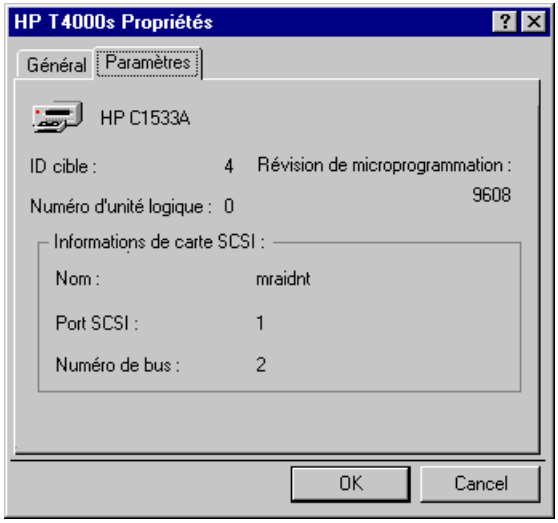

Figure 82 - Paramètres du périphérique

Configuration des ID SCSI sur une bibliothèque HP StorageWorks 330fx

Une fois que vous avez choisi les ID SCSI pour le robot et les lecteurs, vous pouvez les vérifier et les configurer à l'aide du panneau de configuration de la bibliothèque.

EXEMPLE : si vous disposez d'une bibliothèque HP StorageWorks 330fx, procédez comme suit pour trouver les ID SCSI configurés :

1. Depuis l'état PRET, appuyez sur SUIVANT. `ADMIN*` apparaît.
2. Appuyez sur ENTREE. Vous êtes invité à saisir le mot de passe. Saisissez le mot de passe.
3. `TEST*` apparaît ; appuyez sur SUIVANT jusqu'à ce que l'option `ID SCSI*` apparaisse.
4. Appuyez sur ENTREE. `VIEW IDs*` apparaît.
5. Appuyez sur ENTREE. `JKBX ID 6 LUN 0` s'affiche.
6. Appuyez sur SUIVANT. `DRV 1 ID 5 LUN 0` s'affiche.
7. Appuyez sur SUIVANT. `DRV 2 ID 4 LUN 0` s'affiche, etc.

Vous pouvez revenir à l'état `PRET` en appuyant sur ANNULER plusieurs fois.

Connexion de périphériques de sauvegarde

Pour connecter un périphérique de sauvegarde à un système HP-UX, Solaris, Linux ou Windows, suivez la procédure générale ci-dessous.

1. Sélectionnez le client auquel vous souhaitez connecter le périphérique de sauvegarde.
2. Installez un Agent de support sur le système sélectionné. Reportez-vous à la section "Installation distante de clients Data Protector" à la page 78.
3. Déterminez l'adresse SCSI non occupée pouvant être utilisée par le périphérique. Pour les systèmes HP-UX, reportez-vous à la section "Recherche des adresses SCSI non utilisées sous HP-UX" à la page 414. Pour les systèmes Solaris, reportez-vous à la section "Recherche des ID SCSI cibles inutilisés sous Solaris" à la page 416. Pour les systèmes Windows, reportez-vous à la section "Recherche des ID SCSI cibles inutilisés sur un système Windows" à la page 421.
   - Pour la connexion à un système HP-UX, vérifiez que les pilotes requis sont *installés* et *intégrés* au noyau en cours. Reportez-vous à la section "Vérification de la configuration du noyau sous HP-UX" à la page 95.
     Si vous devez configurer un pilote de passage SCSI, reportez-vous à la section "Configuration de robot SCSI sous HP-UX" à la page 407.
   - Pour la connexion à un système Solaris, vérifiez que les pilotes requis sont installés et que les fichiers de configuration sont à jour pour l'installation du périphérique. Reportez-vous à la section "Mise à jour de la configuration des périphériques et pilotes sur un système Solaris" à la page 417. Celle-ci vous indique également comment mettre à jour le fichier `sst.conf` si vous devez configurer un pilote de passage SCSI.
   - Si le périphérique est connecté à un client Windows, le lecteur de bande d'origine peut être chargé ou désactivé, selon la version du système Windows. Reportez-vous à la section "Utilisation de pilotes de bandes et de pilotes de robots sous Windows" à la page 402.
     Si vous chargez le pilote de bandes natif pour un périphérique déjà configuré dans Data Protector qui n'utilisait pas le pilote de bandes natif, n'oubliez pas de renommer les fichiers de périphérique pour tous les périphériques logiques Data Protector configurés qui se rapportent au périphérique en question (par exemple, remplacez `scsi1:0:4:0` par `tape3:0:4:0`).
     Pour plus d'informations concernant l'attribution d'un nom de fichier de périphérique correct, reportez-vous à la section "Création de fichiers de périphérique (adresses SCSI) sous Windows" à la page 406.

4. Définissez les adresses SCSI (ID) sur le périphérique. En fonction du type de périphérique, vous pouvez généralement effectuer cette opération avec les commutateurs du périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.

   Si vous souhaitez voir un exemple, reportez-vous à la section "Configuration des ID SCSI sur une bibliothèque HP StorageWorks 330fx" à la page 422.

   Pour obtenir des informations détaillées sur les périphériques pris en charge, reportez-vous à la page http://www.hp.com/support/manuals.

REMARQUE :

Sur un système Windows NT doté d'une carte SCSI Adaptec et auquel est connecté un périphérique SCSI, vous devez activer l'option `Carte hôte BIOS` afin que le système n'ait pas de problème pour émettre les commandes SCSI.

Pour définir l'option Carte hôte BIOS, appuyez sur Ctrl+A pendant l'initialisation du système pour accéder au menu Carte SCSI, puis sélectionnez Configurer/Afficher les paramètres de la carte hôte -> Options de configuration avancées, et enfin activez Carte hôte BIOS.

5. Allumez d'abord le périphérique, puis l'ordinateur, et attendez que le processus d'initialisation soit terminé. Vérifiez que le système reconnaît bien le nouveau périphérique de sauvegarde.

   - Sur un système HP-UX, servez-vous de l'utilitaire `ioscan`
     `/usr/sbin/ioscan -fn`
     pour afficher la liste des périphériques connectés, avec les chemins matériels et les fichiers de périphérique correspondants, dans laquelle vous devez trouver le nouveau périphérique connecté avec les adresses SCSI correctes. Si un fichier de périphérique n'a pas été créé automatiquement durant le processus d'initialisation, vous devez le créer manuellement. Reportez-vous à la section "Création de fichiers de périphérique sous HP-UX" à la page 412.
   - Sur un système Solaris, exécutez l'utilitaire `ls -all` dans le répertoire `/dev/rmt` pour afficher la liste des périphériques connectés, avec les chemins matériels et les fichiers de périphérique correspondants, dans laquelle vous devez trouver le nouveau périphérique connecté avec les adresses SCSI correctes.
   - Sur un système Solaris, exécutez l'utilitaire `ls -all` dans le répertoire `/dev/rmt` pour afficher la liste des périphériques connectés, avec les chemins matériels et les fichiers de périphérique correspondants, dans laquelle vous devez trouver le nouveau périphérique connecté avec les adresses SCSI correctes.
   - Sur un système Windows, vous pouvez vérifier que le système reconnaît correctement le nouveau périphérique de sauvegarde à l'aide de l'utilitaire

`devbra`. Dans le répertoire *`répertoire_Data_Protector`*`\bin`, exécutez :

```
devbra -dev
```

Dans les résultats de la commande `devbra`, vous trouverez pour chaque périphérique connecté et correctement reconnu les lignes suivantes :

```
spécification du périphérique de sauvegarde
chemin_matériel
type_support
...........
```

Par exemple, les résultats suivants :

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

signifient qu'un périphérique à bandes HP DDS (le pilote de bandes natif étant chargé) a le numéro d'instance du lecteur 3, et est connecté au bus SCSI 0, à l'ID SCSI cible 4 et au numéro LUN 0.

Tandis que les résultats suivants :

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

signifient qu'un périphérique à bandes HP DDS (le pilote de bandes d'origine étant déchargé) est connecté au port SCSI 1, au bus SCSI 0 et que le lecteur de bandes a l'ID SCSI cible 4 et le numéro LUN 0.

- Sur un système AIX, servez-vous de l'utilitaire `lsdev`

  ```
  lsdev -C
  ```

  pour afficher la liste des périphériques connectés et les noms de périphérique correspondants.

Compression matérielle

La plupart des périphériques de sauvegarde récents proposent une compression matérielle intégrée pouvant être activée lors de la création d'un fichier de périphérique ou d'une adresse SCSI pendant la procédure de configuration du périphérique. Reportez-vous à l'aide en ligne pour connaître la procédure détaillée.

La compression matérielle est effectuée par un périphérique qui reçoit les données originales d'un Agent de support et les écrit sur la bande sous forme compressée. Ce procédé permet d'augmenter la vitesse à laquelle un lecteur de bande reçoit les données car le volume de données écrit sur la bande est moins important.

Lorsque la compression logicielle est utilisée et la compression matérielle désactivée, les données sont compressées par l'Agent de disque et envoyées sous forme compressée à un Agent de support. L'algorithme de compression peut faire appel à une quantité de

ressources de l'Agent de disque considérable si la compression logicielle est utilisée, mais cela réduit la charge réseau.

Pour activer la compression matérielle sous Windows, ajoutez "C" à la fin des adresses SCSI de périphérique/lecteur, par exemple : scsi:0:3:0C (ou tape2:0:1:0C si le pilote du lecteur de bandes est chargé). Si le périphérique prend en charge la compression matérielle, celle-ci sera utilisée ; sinon, l'option C sera ignorée.

Pour désactiver la compression matérielle sous Windows, ajoutez "N" à la fin des adresses SCSI de périphérique/lecteur, par exemple : scsi:0:3:0:N.

Pour activer/désactiver la compression matérielle sous UNIX, sélectionnez un fichier de périphérique approprié. Consultez la documentation du périphérique et du système d'exploitation pour plus de détails.

Etape suivante

A ce stade de la procédure, les périphériques de sauvegarde doivent être connectés afin que vous puissiez les configurer ainsi que les pools de supports. Dans l'index de l'aide en ligne, recherchez : "configuration, périphériques de sauvegarde" pour plus d'informations sur les tâches de configuration supplémentaires.

Un Agent de support doit être installé sur votre système. Pour connaître la procédure, reportez-vous à la section "Installation distante de clients Data Protector" à la page 78.

Les sections suivantes décrivent la procédure de connexion d'un périphérique à bandes autonome HP StorageWorks 24, d'une bibliothèque HP StorageWorks 12000e et d'une bibliothèque DLT 28/48 logements HP StorageWorks à des systèmes HP-UX et Windows.

Connexion d'un périphérique autonome HP StorageWorks 24

Le périphérique de sauvegarde DDS StorageWorks 24 est un lecteur de bandes autonome basé sur la technologie DDS3.

Connexion à un système HP-UX

Pour connecter un périphérique autonome HP StorageWorks 24 à un système HP-UX, procédez comme suit :

1. Vérifiez que les pilotes nécessaires (`stape` ou `tape2`) sont *installés* et *intégrés* au noyau actuel. Reportez-vous à la section "Vérification de la configuration du noyau sous HP-UX" à la page 95.
2. Définissez une adresse SCSI non occupée pouvant être utilisée par le lecteur de bandes. Reportez-vous à la section "Recherche des adresses SCSI non utilisées sous HP-UX" à la page 414.

3. Définissez les adresses SCSI (ID) sur le périphérique. Utilisez les commutateurs situés à l'arrière du périphérique.

   Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.

4. Allumez d'abord le périphérique, puis l'ordinateur, et attendez que le processus d'initialisation soit terminé.

5. Vérifiez que le système reconnaît correctement le nouveau lecteur de bandes connecté. Servez-vous de l'utilitaire `ioscan` :

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

   pour afficher la liste des périphériques connectés avec les chemins matériels et les fichiers de périphérique correspondants, dans laquelle vous devez trouver le nouveau lecteur de bandes connecté avec l'adresse SCSI correcte. Le fichier de périphérique du lecteur a été créé lors du processus d'amorçage.

Etape suivante

Une fois que le périphérique est correctement connecté, recherchez : "configuration, périphériques de sauvegarde" dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

Connexion à un système Windows

Pour connecter un périphérique autonome HP StorageWorks 24 à un système Windows, procédez comme suit :

1. Définissez une adresse SCSI (ID cible) non occupée pouvant être utilisée par le lecteur de bandes. Reportez-vous à la section "Recherche des ID SCSI cibles inutilisés sur un système Windows" à la page 421.

2. Définissez les adresses SCSI (ID) sur le périphérique. Utilisez les commutateurs situés à l'arrière du périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.

3. Allumez d'abord le périphérique, puis l'ordinateur, et attendez que le processus d'initialisation soit terminé.

4. Vérifiez que le système reconnaît correctement le nouveau lecteur de bandes connecté. Exécutez la commande `devbra` à partir du répertoire *`répertoire_Data_Protector`*`\bin`. Tapez

   ```
   devbra -dev
   ```

   Dans les résultats de la commande `devbra`, vous devez trouver le nouveau lecteur de bandes connecté du périphérique autonome HP StorageWorks 24.

Etape suivante

Une fois que le périphérique est correctement connecté, recherchez : "configuration, périphériques de sauvegarde" dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

Connexion d'un chargeur automatique DAT HP StorageWorks

Les bibliothèques HP StorageWorks 12000e et StorageWorks DAT 24x6 sont toutes deux dotées d'un logement pour six cartouches, d'un lecteur et d'un bras robotisé utilisé pour déplacer les cartouches du/vers le lecteur. Les deux bibliothèques sont également équipées d'un système de détection de bande encrassée.

Connexion à un système HP-UX

Pour connecter le périphérique de bibliothèque HP StorageWorks 12000e à un système HP-UX, procédez comme suit :

1. A l'arrière du chargeur automatique, mettez le commutateur de mode sur `6`.
2. Vérifiez que les pilotes nécessaires (`stape` ou `tape2`) sont *installés* et *intégrés* au noyau actuel. Reportez-vous à la section "Vérification de la configuration du noyau sous HP-UX" à la page 95.
3. Vérifiez que les pilotes de passage SCSI (`sctl` ou `spt`) sont *installés* et *intégrés* au noyau actuel. Reportez-vous à la section "Configuration de robot SCSI sous HP-UX" à la page 407.
4. Déterminez une adresse SCSI non occupée pouvant être utilisée par le lecteur de bandes et le robot. Reportez-vous à la section "Recherche des adresses SCSI non utilisées sous HP-UX" à la page 414.

REMARQUE :

La bibliothèque HP StorageWorks 12000e utilise la même adresse SCSI pour le lecteur de bandes et le robot, mais avec différents numéros LUN.

5. Définissez les adresses SCSI (ID) sur le périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.
6. Allumez d'abord le périphérique, puis l'ordinateur, et attendez que le processus d'initialisation soit terminé.

7. Vérifiez que le système reconnaît correctement le nouveau lecteur de bandes connecté. Servez-vous de l'utilitaire `ioscan`

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

   pour afficher la liste des périphériques connectés avec les chemins matériels et les fichiers de périphérique correspondants, dans laquelle vous devez trouver le nouveau lecteur de bandes connecté avec l'adresse SCSI correcte.

8. Le fichier de périphérique du lecteur a été créé lors du processus d'amorçage, mais vous devez créer celui du robot manuellement. Reportez-vous à la section "Création de fichiers de périphérique sous HP-UX" à la page 412.

9. Vérifiez que le système reconnaît correctement le nouveau fichier de périphérique du robot de bibliothèque. Servez-vous de l'utilitaire `ioscan` :

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

   Le nouveau fichier de périphérique doit apparaître dans les résultats de la commande.

Etape suivante

Une fois que le périphérique de bibliothèque est correctement connecté, recherchez : "configuration, périphériques de sauvegarde" dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

Connexion à un système Windows

Pour connecter le périphérique de bibliothèque HP StorageWorks 12000e à un système Windows, procédez comme suit :

1. A l'arrière du chargeur automatique, mettez le commutateur de mode sur `6`.

2. Déterminez une adresse SCSI non occupée pouvant être utilisée par le lecteur de bandes et le robot. Reportez-vous à la section "Recherche des ID SCSI cibles inutilisés sur un système Windows" à la page 421.

3. Définissez les adresses SCSI (ID) sur le périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.

   REMARQUE :

   La bibliothèque HP StorageWorks 12000e utilise la même adresse SCSI pour le lecteur de bandes et le robot, mais avec différents numéros LUN.

4. Allumez d'abord le périphérique, puis l'ordinateur, et attendez que le processus d'initialisation soit terminé.

5. Vérifiez que le système reconnaît correctement le nouveau lecteur de bandes connecté et le robot. Dans le répertoire *répertoire_Data_Protector*\bin, exécutez :

   ```
   devbra -dev
   ```

   Dans les résultats de la commande devbra, vous devez trouver le nouveau lecteur de bandes connecté et le robot du périphérique de bibliothèque HP StorageWorks 12000e.

Etape suivante

Une fois que le périphérique de bibliothèque est correctement connecté, recherchez : "configuration, périphériques de sauvegarde" dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

Connexion d'une bibliothèque DLT 28/48 logements HP StorageWorks

La bibliothèque DLT 28/48 logements HP StorageWorks est une bibliothèque multi-lecteurs destinée aux environnements d'entreprise ayant de 80 à 600 Go à sauvegarder. Elle est équipée de quatre lecteurs DLT 4000 ou DLT 7000 dotés de plusieurs canaux de données, d'un logement de bande et d'un lecteur de codes-barres.

Connexion à un système HP-UX

Pour connecter la bibliothèque DLT 28/48 logements HP StorageWorks à un système HP-UX, procédez comme suit :

1. Vérifiez que les pilotes nécessaires (stape ou tape2) sont *installés* et *intégrés* au noyau en cours. Reportez-vous à la section "Vérification de la configuration du noyau sous HP-UX" à la page 95.
2. Vérifiez que les pilotes de passage SCSI (sctl ou spt) sont *installés* et *intégrés* au noyau actuel. Reportez-vous à la section "Configuration de robot SCSI sous HP-UX" à la page 407.

3. Déterminez une adresse SCSI non occupée pouvant être utilisée par le lecteur de bandes et le robot. Reportez-vous à la section "Recherche des adresses SCSI non utilisées sous HP-UX" à la page 414.

REMARQUE :

La bibliothèque DLT 28/48 logements HP StorageWorks est dotée de quatre lecteurs de bande et d'un robot, vous devez donc disposer de cinq adresses SCSI inutilisées au cas où tous les lecteurs de bandes devraient être utilisés. Les lecteurs de bandes et le robot doivent utiliser des adresses SCSI différentes.

4. Définissez les adresses SCSI (ID) sur le périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.
5. Allumez le périphérique, puis l'ordinateur, et attendez que le processus d'amorçage soit terminé.
6. Vérifiez que le système reconnaît correctement les nouveaux lecteurs de bandes connectés. Servez-vous de l'utilitaire `ioscan`

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

   pour afficher la liste des périphériques connectés avec les chemins matériels et les fichiers de périphérique correspondants, dans laquelle vous devez trouver les nouveaux lecteurs de bandes connectés avec les adresses SCSI correctes.
7. Les fichiers de périphérique des lecteurs ont été créés lors du processus d'initialisation, mais vous devez créer celui du robot manuellement. Reportez-vous à la section "Création de fichiers de périphérique sous HP-UX" à la page 412.
8. Vérifiez que le système reconnaît correctement le nouveau fichier de périphérique du robot de bibliothèque. Servez-vous de l'utilitaire `ioscan` :

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

   Le nouveau fichier de périphérique doit apparaître dans les résultats de la commande.

Etape suivante

Une fois le périphérique de la bibliothèque DLT 28/48 logements HP StorageWorks correctement connecté, recherchez : "configuration, périphériques de sauvegarde" dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

Connexion à un système Solaris

Pour configurer le périphérique de bibliothèque HP C5173-7000 sur un système Solaris, exécutez la procédure décrite ci-dessous. Cet exemple suppose que deux lecteurs sont alloués à Data Protector :

1. Copiez le pilote (module) `sst` et le fichier de configuration `sst.conf` dans le répertoire requis :
   - Pour les systèmes d'exploitation 32 bits :
     ```
     $cp /opt/omni/spt/sst /usr/kernel/drv/sst
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```
   - Pour les systèmes d'exploitation 64 bits :
     ```
     $cp /opt/omni/spt/sst.64 /usr/kernel/drv/sparcv9 /sst
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv
     /sparcv9/sst.conf
     ```
2. Ajoutez le pilote au noyau Solaris :

   ```
   add_drv sst
   ```
3. Supprimez tous les fichiers de périphérique existants du répertoire `/dev/rmt` :

   ```
   cd /dev/rmt rm *
   ```
4. Arrêtez le système en appuyant sur Stop et A.
5. Exécutez la commande `probe-scsi-all` à l'invite "`ok`" pour vérifier quelles sont les adresses SCSI disponibles.

   ```
   ok probe-scsi-all
   ```

   Le système peut vous demander de lancer la commande `reset-all` avant d'exécuter la commande `probe-scsi-all`.

   Dans le cas présent, nous utiliserons le port 6 pour le périphérique de contrôle SCSI, le port 2 pour le premier lecteur et le port 1 pour le deuxième lecteur ; le numéro LUN est 0.
6. Revenez en fonctionnement normal :

   ```
   ok go
   ```
7. Copiez le fichier de configuration `st.conf` dans le répertoire requis :

   ```
   $cp /opt/omni/spt/st.conf /kernel/drv/st.conf
   ```

   Le fichier `st.conf` est présent sur chaque client Data Protector Solaris et contient les adresses SCSI de chaque périphérique de sauvegarde connecté au client.

8. Modifiez le fichier `/kernel/drv/st.conf` et ajoutez les lignes suivantes :

```
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;
```

Ces entrées fournissent les adresses SCSI pour le lecteur 1, le lecteur 2 et le robot.

9. Modifiez le fichier `sst.conf` (que vous avez copié à l'Étape 1 à la page 432) et ajoutez la ligne suivante :

```
name="sst" class="scsi" target=6 lun=0;
```

REMARQUE :

Cette entrée doit être identique à celle du robot dans le fichier `st.conf`. Reportez-vous à l'Étape 8 à la page 433 ci-dessus.

10. Arrêtez le système client et connectez le périphérique de bibliothèque.

11. Remettez le périphérique de bibliothèque sous tension, puis le système client.

Le système s'initialise alors et crée automatiquement les fichiers de périphérique pour le robot et les lecteurs de bandes. Vous pouvez répertorier ceux-ci à l'aide de la commande `ls -all`. Dans le cas présent :

/dev/rmt/0hb	pour un premier lecteur de bandes
/dev/rmt/1hb	pour un deuxième lecteur de bandes
/dev/rsst6	pour un lecteur de robot

Etape suivante

Une fois le périphérique de la bibliothèque DLT 28/48 logements HP StorageWorks correctement connecté, recherchez : "configuration, périphériques de sauvegarde" dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un

périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

Connexion à un système Windows

Pour connecter le périphérique de bibliothèque DLT 28/48 logements HP StorageWorks à un système Windows, procédez comme suit :

1. Déterminez les adresses SCSI (ID cibles) non occupées pouvant être utilisées par le lecteur de bandes et le robot. Reportez-vous à la section "Recherche des ID SCSI cibles inutilisés sur un système Windows" à la page 421.
2. Définissez les adresses SCSI (ID cibles) sur le périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.

REMARQUE :

La bibliothèque DLT 28/48 logements HP StorageWorks est dotée de quatre lecteurs de bande et d'un robot, vous devez donc disposer de cinq adresses SCSI inutilisées au cas où tous les lecteurs de bandes devraient être utilisés. Les lecteurs de bande et le robot doivent utiliser des ID SCSI cibles différents.

3. Allumez d'abord le périphérique, puis l'ordinateur, et attendez que le processus d'amorçage soit terminé.
4. Vérifiez que le système reconnaît correctement les nouveaux lecteurs de bandes connectés et le robot. Dans le répertoire `répertoire_Data_Protector\bin`, exécutez :

   ```
   devbra -dev
   ```

   Dans le résultat de la commande `devbra`, vous devez trouver les nouveaux lecteurs de bandes connectés et le robot du périphérique de bibliothèque DLT 28/48 logements HP StorageWorks.

Etape suivante

Une fois le périphérique de la bibliothèque DLT 28/48 logements HP StorageWorks correctement connecté, recherchez : "configuration, périphériques de sauvegarde" dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

Connexion d'un lecteur de bandes Seagate Viper 200 LTO Ultrium

Le lecteur de bandes Seagate Viper 200 LTO Ultrium est un périphérique autonome pour les environnements d'entreprise avec 100 à 200 Go à sauvegarder.

Connexion à un système Solaris

Pour configurer le lecteur de bandes Seagate Viper 200 LTO Ultrium sur un système Solaris, procédez comme suit :

1. Déterminez les adresses SCSI non occupées pouvant être utilisées par le lecteur de bandes. Exécutez la commande `modinfo` ou `dmesg` pour rechercher les contrôleurs SCSI en cours d'utilisation et les périphériques SCSI cibles installés :

   ```
   dmesg | egrep "target" | sort | uniq
   ```

   Le résultat suivant doit être obtenu :

   ```
   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
   ```

   REMARQUE :

   Il est recommandé d'utiliser le contrôleur SCSI `glm` ou `isp` lorsque vous connectez un périphérique Viper 200 LTO à un système Solaris. De même, il est préférable d'utiliser les contrôleurs Ultra2 SCSI ou Ultra3 SCSI.

2. Modifiez le fichier `/kernel/drv/st.conf` et ajoutez les lignes suivantes :

   ```
   tape-config-list =
   "SEAGATE ULTRIUM06242-XXX" , "SEAGATE LTO" , \
   "SEAGATE_LTO";
   SEAGATE_LTO = 1, 0x7a, 0, 0x1d679, 4, 0x00, 0x00, 0x00, \
   0x00, 1;
   ```

3. Arrêtez le système client et connectez le périphérique.
4. Remettez le périphérique sous tension, puis le système client.

   Le système s'initialise alors et crée automatiquement les fichiers de périphérique pour le lecteur de bandes. Vous pouvez répertorier ceux-ci à l'aide de la commande `ls -all`.

Etape suivante

Une fois le lecteur de bandes Seagate Viper 200 LTO Ultrium correctement connecté, recherchez : "configuration, périphériques de sauvegarde" dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

Connexion à un système Windows

Pour connecter le lecteur de bandes Seagate Viper200 LTO Ultrium à un système Windows, procédez comme suit :

1. Déterminez les adresses SCSI (ID cibles) non occupées pouvant être utilisées par le lecteur de bandes. Reportez-vous à la section "Recherche des ID SCSI cibles inutilisés sur un système Windows" à la page 421.
2. Définissez les adresses SCSI (ID cibles) sur le périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.
1. Allumez d'abord le périphérique, puis l'ordinateur, et attendez que le processus d'amorçage soit terminé.
2. Vérifiez que le système reconnaît correctement les nouveaux lecteurs de bandes connectés et le robot. Dans le répertoire *répertoire_Data_Protector*\bin, exécutez :

   ```
   devbra -dev
   ```

   Dans les résultats de la commande `devbra`, vous devez trouver le nouveau lecteur de bandes connecté du lecteur de bandes Seagate Viper 200 LTO Ultrium.

Etape suivante

Une fois le lecteur de bandes Seagate Viper 200 LTO Ultrium correctement connecté, recherchez : "configuration, périphériques de sauvegarde" dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

REMARQUE :

Lorsque vous configurez le lecteur de bandes Seagate Viper 200 LTO Ultrium avec Data Protector, assurez-vous que le mode de compression est activé. Pour cela, spécifiez le paramètre `C` après l'adresse SCSI du lecteur, par exemple :

```
scsi2:0:0:0C
```

Vérification de l'installation de l'Agent général de support sous Novell NetWare

Après avoir effectué l'installation de l'Agent général de support sur la plateforme Novell NetWare, vous devez la contrôler en procédant comme suit :

- Identifiez le périphérique de stockage.
- Testez le démarrage de l'Agent général de support sur la console du serveur Novell NetWare.

- Testez le démarrage de `HPUMA.NLM` et de `HPDEVBRA.NLM` sur la console du serveur Novell NetWare.

Identification du périphérique de stockage

Utilisez la convention suivante pour identifier un périphérique de stockage dans l'environnement Novell NetWare :

numéro d'identification de la carte: *numéro d'identification cible*: *numéro d'unité logiquecompression*

Par exemple, la chaîne "`0:2:0N`" identifie un périphérique de stockage avec comme ID de carte 0, comme ID cible 2, un numéro d'unité logique (LUN) 0 et aucune compression.

Autre exemple : la chaîne "`1:1:0C`" identifie un périphérique de stockage avec comme ID de carte 1, comme ID cible 1, un numéro d'unité logique (LUN) 0 et la compression activée.

Test de démarrage de l'Agent général de support

Une fois l'Agent général de support installé sur le système Novell NetWare, vous pouvez tester le démarrage d'un Agent de support de sauvegarde `HPBMA.NLM` sur la console du serveur Novell NetWare.

Dans l'exemple ci-après, la carte bus hôte `Adaptec`, `AHA-2940`, est utilisée pour accéder au périphérique à bandes échangeur de la bibliothèque de bandes HP StorageWorks 12000e.

Avant de démarrer tout composant `*.NLM` de Data Protector, vous devez satisfaire aux conditions suivantes :

- `HPINET` doit être en cours d'exécution.
- Le pilote de carte hôte SCSI `Adaptec` doit être en cours d'exécution.
- Le logiciel de l'Agent général de support doit se trouver dans le répertoire `SYS:USR\OMNI\BIN`.
- Le périphérique de stockage doit être correctement installé et connecté.
- La carte bus hôte Adaptec et le protocole de communication TCP/IP doivent être correctement installés et en cours d'exécution.

Une fois ces conditions remplies, procédez comme suit :

1. Pour charger `HPBMA.NLM`, tapez :

   `LOAD HPBMA -name testbma -type` *`numéro_type`* `-policy` *`numéro_mode`* `-ioctl` *`périphérique_contrôle`* `-dev` *`périphérique_données`* `-tty` *`numéro_port_TCP`*

   L'option `type` *`numéro_type`* correspond au type de périphérique Data Protector. Les valeurs possibles pour *`numéro_type`* sont les suivantes :

   - 1=DAT/DDS

- 2 = QIC (cartouche d'un quart de pouce)
- 3 = Exabyte 8mm
- 9 = périphérique générique à bandes magnétiques
- 10 = bande linéaire numérique (DLT)

L'option `policy` *`numéro_mode`* correspond au mode d'utilisation du périphérique par Data Protector. Les valeurs possibles sont les suivantes :

- 1= périphérique autonome
- 10= bibliothèque SCSI - II

L'option `ioctl` *`périphérique_contrôle`* définit l'adresse SCSI du contrôle du robot. Elle se présente sous la forme suivante :

`numéro_identification_adaptateur`:*`numéro_identification_cible`*:*`numéro_unité_logique`*

Par exemple :

- `0:1:1` =>Le périphérique de contrôle (robot) utilise la carte SCSI 0, possède l'adresse SCSI 1 et le LUN 1.

L'option `dev` *`périphérique_données`* définit l'adresse SCSI du contrôle du robot. Elle se présente sous la forme suivante :

`numéro_identification_adaptateur`:*`numéro_identification_cible`*:*`numéro_unité_logiquecompression`*

Par exemple :

- `0:1:1C` =>Le périphérique de contrôle (robot) utilise la carte SCSI 0, possède l'adresse SCSI 1 et le LUN 1. La compression de données est activée.

L'option `-tty` *`numéro_port_TCP`* correspond au numéro de port du protocole de communication TCP/IP.

L'Agent de support de la console, `HPCONMA.NLM`, démarre et l'écran suivant s'affiche :

```
*** MA listening on port : numéro

SLOT: [Load(2), Peek(2), Stop(0), Abort(0)]

SLOT: _
```

Les commandes actuellement disponibles sont les suivantes :

`Load(2)` - Cette commande permet de charger la bande dans le lecteur et requiert deux arguments :

`Load` *`numéro d'emplacementindicateur de permutation`*

L'indicateur de permutation peut être défini soit à 0 soit à 1, ce qui signifie que le support ne permute pas si la valeur est 0 ou qu'il permute si la valeur est 1.

`Stop(0)` - Termine normalement la session en cours.

`Abort(0)` - Abandonne la session en cours.

Dans cet exemple, vous chargez la bande à partir de l'emplacement 3 (`SLOT 3`) sans permutation du support.

2. Tapez la commande permettant de charger la bande à partir de l'emplacement 3 (`SLOT 3`) sans permutation du support.

   ```
   SLOT:LOAD 3 0
   ```

   Une fois la bande chargée dans le lecteur, le message suivant s'affiche :

   ```
   CHECK: [Deny(0), Init(1), Seek(2), Abort(0)]
   CHECK: _
   ```

   Les commandes disponibles sont les suivantes :

   `Deny(0)` - Refuse l'action en cours.

   `Init(1)` - Initialise la bande chargée et requiert un paramètre :

   `Init(1)` *`ID_support`*

   `Seek(2)` - Effectue une recherche à la position requise. La chaîne d'arguments est la suivante :

   `Seek`*`numéro_segmentnuméro de bloc`*

   `Abort(0)` - Abandonne la session en cours.

3. Pour initialiser la bande, tapez

   ```
   CHECK: Init test
   ```

4. Basculez de l'écran de l'Agent général de support de sauvegarde à la console Novell NetWare et démarrez la session de sauvegarde à l'aide de la commande d'action/de requête de l'Agent de support.

REMARQUE :

Vous devez démarrer l'Agent de disque Data Protector sur l'hôte sélectionné en entrant `load -ma` *`hôte port`* pour permettre une communication correcte entre l'Agent général de support et l'Agent de disque et afficher le bon numéro de port des opérations de la session de sauvegarde lorsque `HPCONMA.NLM` démarre. Une fois la session de sauvegarde terminée correctement, un message s'affiche.

5. Pour quitter correctement l'Agent de support de sauvegarde, appuyez sur CTRL-C lorsque l'écran de l'Agent de support de sauvegarde s'affiche. L'invite `Requête d'intervention sur la console` s'affiche au bout de quelques secondes :

   `ATT:[Stop(0), Abort(0), Disconnect(1)]` Exécutez la commande `Stop` pour terminer la session.

Test du démarrage de HPUMA.NLM et de HPDEVBRA.NLM

Le chargement de `HPUMA.NLM` sur la console du serveur permet de tester manuellement les commandes SCSI.

Chargez `HPUMA.NLM` à l'aide de la commande suivante :

`LOAD HPUMA.NLM -ioctl` *`périphérique_contrôle`* `-dev` *`périphérique_données`*

`-tty`

L'option `ioctl` *`périphérique_contrôle`* définit l'adresse SCSI du contrôle du robot. Elle se présente sous la forme suivante :

`numéro_identification_adaptateur`:*`numéro_identification_cible`*:*`numéro_unité_logique`*

Par exemple :

- `0:1:1` =>Le périphérique de contrôle (robot) utilise la carte SCSI 0, possède l'adresse SCSI 1 et utilise le LUN 1.

L'option `dev` *`périphérique_données`* définit l'adresse SCSI du contrôle du robot. Elle se présente sous la forme :

`numéro_identification_adaptateur`:*`numéro_identification_cible`*:*`numéro_unité_logique`*:*`compression`*

Par exemple :

- `0:1:1C` =>Le périphérique de contrôle (robot) utilise la carte SCSI 0, possède l'adresse SCSI 1 et le LUN 1. La compression de données est activée.

L'option `-tty` est nécessaire pour interagir avec la console du serveur Novell NetWare.

HPUMA démarre et l'écran suivant s'affiche :

`prompt`

où "prompt" se présente sous la forme suivante : `numéro_identification_adaptateur :numéro_identification_cible : numéro_unité_logique` Par exemple,

`0:2:1`

Pour afficher les commandes actuellement disponibles, tapez la commande `HELP` dans l'écran HPUMA. Par exemple, tapez `STAT` à l'invite pour voir si les logements et le ou les lecteurs sont occupés ou vides.

Lorsque vous avez terminé, tapez `BYE` pour fermer l'écran HPUMA.

Le chargement de `HPDEVBRA.NLM` vous permet localement d'obtenir des informations sur les périphériques à la fois installés et détectés sur le serveur Novell NetWare.

Pour charger `HPDEVBRA.NLM` sur la console du serveur, entrez la commande suivante :

```
LOAD HPDEVBRA.NLM -dev
```

où l'option `-dev` est nécessaire pour répertorier tous les périphériques associés au serveur Novell NetWare.

Pour afficher les commandes disponibles, chargez `HPDEVBRA.NLM` avec l'option `HELP` :

```
LOAD HPDEVBRA -HELP
```

Installation de Data Protector sur Microsoft Cluster avec Veritas Volume Manager

Pour installer Data Protector sur Microsoft Cluster Server (MSCS) avec Veritas Volume Manager, commencez par suivre la procédure d'installation de Data Protector sur MSCS. Reportez-vous à la section "Installation de Data Protector sur Microsoft Cluster Server" à la page 187.

Une fois que vous avez terminé l'installation, certaines étapes supplémentaires sont requises pour activer le service `Data ProtectorInet Data Protector` permettant de distinguer, entre les ressources disque de cluster et les ressources disque locales, celles qui utilisent leurs propres ressources et non le pilote de ressources Microsoft :

1. Exécutez la commande `omnisv -stop` sur le Gestionnaire de cellule pour arrêter les services et processus Data Protector :*répertoire_Data_Protector*`\bin\omnisv -stop`

2. Définissez une nouvelle variable d'environnement système

   `OB2CLUSTERDISKTYPES` avec `Volume Manager Disk Group` en tant que valeur, ou définissez la variable `omnirc` sur les deux nœuds de cluster comme suit :

   ```
   OB2CLUSTERDISKTYPES=Volume Manager Disk Group
   ```

   Si vous souhaitez spécifier des ressources disque propriétaires supplémentaires, telles qu'un disque NetRAID4, ajoutez simplement le nom du type de la ressource à la valeur de la variable d'environnement

   `OB2CLUSTERDISKTYPES` :

   ```
   OB2CLUSTERDISKTYPES=Volume Manager Disk Group;NETRaid4M
   Diskset
   ```

   Pour plus d'informations sur l'utilisation des variables de fichier `omnirc`, reportez-vous au *Guide de dépannage HP Data Protector*.

3. Exécutez la commande `omnisv -start` pour démarrer les services/processus :
   `répertoire_Data_Protector``\bin\omnisv -start`

Modification du chemin des fichiers de configuration dans Data Protector A.06.10

Les chemins par défaut de certains fichiers de configuration, fichiers journaux et de base de données (sous UNIX) ont été modifiés dans Data Protector A.05.50 et versions ultérieures. Certains fichiers figurant dans les répertoires `server` et `client` sont désormais divisés.

Si vous effectuez une mise à niveau à partir de Data Protector A.05.10, consultez les tableaux suivants pour prendre connaissance des changements et modifiez les chemins, le cas échéant.

Fichiers de configuration sous UNIX

Fichiers de configuration client

Le tableau suivant indique les fichiers et le répertoire qui ont été déplacés du répertoire `/etc/opt/omni` au répertoire `/etc/opt/omni/client` pendant la mise à niveau.

Tableau 31 - Contenu du nouveau répertoire /etc/opt/omni/client

Ancien chemin	Chemin actuel
/etc/opt/omni/cell/cell_server	/etc/opt/omni/client/cell_server
/etc/opt/omni/cell/omni_format	/etc/opt/omni/client/omni_format
/etc/opt/omni/cell/omni_info	/etc/opt/omni/client/omni_info
/etc/opt/omni/cell/allow_hosts	/etc/opt/omni/client/allow_hosts
/etc/opt/omni/cell/deny_hosts	/etc/opt/omni/client/deny_hosts
/etc/opt/omni/customize	/etc/opt/omni/client/customize

Fichiers de configuration et fichiers journaux du Gestionnaire de cellule

Le reste du contenu du répertoire /etc/opt/omni a été déplacé vers le répertoire /etc/opt/omni/server. Par exemple, le fichier /etc/opt/omni/cell/cell_info se trouve désormais dans le répertoire /etc/opt/omni/server/cell.

Le tableau suivant indique les fichiers et le répertoire qui ont été déplacés du répertoire /var/opt/omni vers le répertoire /var/opt/omni/server pendant la mise à niveau.

Tableau 32 - Contenu du nouveau répertoire /var/opt/omni/server

Ancien chemin	Chemin actuel
/var/opt/omni/db40	/var/opt/omni/server/db40
/var/opt/omni/sessions	/var/opt/omni/server/sessions
/var/opt/omni/log/log_file	/var/opt/omni/server/log/*fichier_journal*

où fichier_journal représente n'importe lequel des fichiers suivants : HealthCheck.log, Check_*.txt, Ob2Event*, lic.log, omnisv.log, media.log, sm.log, crsevents.log, security.log, purge.log, readascii.log, cleaning.log, upgrade.log, trace.log et cluster.log.

Tous les autres répertoires (par exemple, /var/opt/omni/tmp, /var/opt/omni/windu ou /var/opt/omni/emc) ainsi que les fichiers journaux (par exemple, /var/opt/omni/log/debug.log) n'ont pas été déplacés.

Fichiers de configuration sous Windows

Fichiers de configuration client

Le tableau suivant représente les fichiers et répertoires qui ont été déplacés du répertoire *répertoire_Data_Protector*\Config vers les répertoires *répertoire_Data_Protector*\Config\client et *répertoire_Data_Protector*\tmp pendant la mise à niveau.

Tableau 33 - Contenu du nouveau répertoire répertoire_Data_Protector\Config\client

Ancien chemin	Chemin actuel
répertoire_Data_Protec-tor\Config\cell\cell_server	*répertoire_Data_Protec-tor*\Config\client\cell_server
répertoire_Data_Protec-tor\Config\cell\omni_format	*répertoire_Data_Protec-tor*\Config\client\omni_format
répertoire_Data_Protec-tor\Config\cell\omni_info	*répertoire_Data_Protec-tor*\Config\client\omni_info
répertoire_Data_Protec-tor\Config\cell\allow_hosts	*répertoire_Data_Protec-tor*\Config\client\allow_hosts
répertoire_Data_Protec-tor\Config\cell\deny_hosts	*répertoire_Data_Protec-tor*\Config\client\deny_hosts
répertoire_Data_Protec-tor\Config\EMC	*répertoire_Data_Protec-tor*\Config\client\EMC
répertoire_Data_Protec-tor\Config\tmp\EMC	*répertoire_Data_Protec-tor*\tmp\EMC

Fichiers de configuration Gestionnaire de cellule

Le reste du contenu du répertoire *répertoire_Data_Protector*\Config a été déplacé vers le répertoire *répertoire_Data_Protector*\Config\Server. Par exemple, le fichier *répertoire_Data_Protector*\Config\cell\cell_info se trouve désormais dans le répertoire *répertoire_Data_Protec-tor*\Config\Server\cell.

Fichiers journaux

Les fichiers suivants ont été déplacés du répertoire *répertoire_Data_Pro-tector*\log vers le répertoire *répertoire_Data_Protector*\log\server : HealthCheck.log, Check_*.txt, Ob2Event*, lic.log, omnisv.log, media.log, sm.log, crsevents.log, security.log, purge.log, readascii.log, cleaning.log, upgrade.log, trace.log et cluster.log.

Tous les autres fichiers journaux (par exemple, *répertoire_Data_Protector*\log\debug.log) ne sont pas déplacés.

Modifications de la ligne de commande après la mise à niveau vers Data Protector A.06.10

Les commandes répertoriées dans ce chapitre ont été modifiées ou proposent des fonctionnalités étendues concernant de nouvelles options dans Data Protector A.06.10. Vérifiez et modifiez les scripts utilisant les anciennes commandes. Pour les synopsis d'utilisation, consultez la Guide de rfrence de l'interface de ligne de commande HP Data Protector ou les pages correspondantes du manuel.

Selon la version d'origine de la mise à niveau de votre Gestionnaire de cellule, reportez-vous au tableau correspondant :

- Pour la mise à niveau à partir de Data Protector A.05.10, reportez-vous au Tableau 34 à la page 445.
- Pour la mise à niveau à partir de Data Protector A.05.50, reportez-vous au Tableau 35 à la page 452.
- Pour la mise à niveau à partir de Data Protector A.06.00, reportez-vous au Tableau 36 à la page 457.
- Pour la mise à niveau à partir de Application Recovery Manager A.06.00, reportez-vous au Tableau 37 à la page 462.

Tableau 34 - Mise à niveau à partir de Data Protector A.05.10

Commande	Sous-commande/Option	Etat
cjutil		NOUVELLE COMMANDE
ob2install	sapdb	NOUVEAUX COMPOSANTS LOGICIELS
	smisa	
	vls_am	
	sps	
	vmware	
	acs	COMPOSANTS OBSOLETES DU LOGICIEL
	das	
	momgui	

Commande	Sous-commande/Option	Etat
omnib	-sapdb_list	NOUVELLES INTEGRATIONS
	-mssps_list	
	-vmware_list	
	-vss_list	OPTION OBSOLETE
	-msvssw_list	NOUVELLES OPTIONS
	-share_info	
	-miroir	
	-enh_incr	
	-async	
	-encode aes256	
	-iap	
	-clp	
omnicc	-check_licenses	NOUVELLES OPTIONS
	-detail	
	-update_all	
	-force_cs	
	-list_trusted_hosts	
	-secure_client	
	-unsecure_client	
	-trusted_hosts	
	–import_vls	
	–import_iap	
	–cert_mode	
	–cert_name	
	–add_certificate	
	–get_certificate	
	–list_certificates	
	–port	OPTIONS MODIFIEES
	–user	
	–passwd	
omnicjutil		NOUVELLE COMMANDE

Commande	Sous-commande/Option	Etat
omniclus	-applid	OPTION MODIFIEE
omnicreatedl	-smis	NOUVELLES OPTIONS POUR StorageWorks StorageWorks ENTERPRISE VIRTUAL ARRAY
	-instant_recovery	
	-snapshots *numéro*	
	-snapshot_type clone	
	-wait_clonecopy *numéro*	
	-replica_conf local	
	-replica_conf combined	
	-ca_failover_option follow_replica_direction	
	-ca_faiover_option maintain_replica_location	
omnidb	-sapdb	NOUVELLES INTEGRATIONS
	-mssps	
	-vmware	
	-copyid	NOUVELLES OPTIONS
	-listcopies	
	-auditing	
	-timeframe	
omnidbcheck	-keystore	NOUVELLES OPTIONS
	-summary	
omnidbeva		COMMANDE OBSOLETE
omnidbrestore	–keyfile	NOUVELLE OPTION
omnidbupgrade		NOUVELLE COMMANDE
omnidbvss		NOUVELLE COMMANDE

Commande	Sous-commande/Option	Etat
omnidbutil	-extendtblspace	NOUVELLES OPTIONS
	-free_cell_resources	
	-list_large_directories	
	-list_large_mpos	
	-list_mpos_without_overs	
	-readdb	OPTION MODIFIEE
omnidlc		NOUVELLE COMMANDE
omniinetpasswd		NOUVELLE COMMANDE
omnikeymigrate		NOUVELLE COMMANDE
omnikeytool		NOUVELLE COMMANDE
omnimigrate.pl		NOUVELLE COMMANDE
omnimcopy	-encrypt	NOUVELLE OPTION
omniminit	-[no]barcode_as_label	NOUVELLE OPTION
omnimm	-[no_]free_pool	OPTION MODIFIEE
	-create_free_pool	NOUVELLE OPTION
omnimcopy	-ams	NOUVELLE OPTION
	-copy	OPTIONS MODIFIEES
	-from	
	-pool	
omniinstlic		NOUVELLE COMMANDE
omniiso		NOUVELLE COMMANDE
omniobjcopy		NOUVELLE COMMANDE

Commande	Sous-commande/Option	Etat
`omniobjconsolidate`		NOUVELLE COMMANDE
`omnir`	`-sapdb`	NOUVELLES INTEGRATIONS
	`-mssps`	
	`-vmware`	
	`-newinstance`	NOUVELLES OPTIONS POUR SAP DB/MaxDB
	`-recover`	
	`-endlogs`	
	`-time`	
	`-nochain`	
	`-destination`	
	`-from_disk`	
	`-instance`	
	`-portal`	NOUVELLES OPTIONS POUR MS SPS
	`-ssodb`	
	`-doclib`	
	`-tohost`	
	`-instance`	
	`-as`	
	`-todir`	
	`-changemaster`	
	`-force_prp_replica`	NOUVELLE OPTION POUR HP StorageWorks ENTERPRISE VIRTUAL ARRAY
	`-instance` *`NomInstanceSource`*	NOUVELLES OPTIONS POUR MS SQL
	`-destinstance` *`NomInstanceDestination`*	
	`-asbase` *`NomNouvelleBDD`*	
	`-file` *`NomFichierLogique`*	
	`-oracle`	NOUVELLES OPTIONS DE RESTAURATION INSTANTANEE ORACLE ET SAP
	`-sap`	
	`-user`	

Commande	Sous-commande/Option	Etat
	-group	R/3
	-recover	
	-open	
	-resetlogs	
	-paralleism	
	-public	NOUVELLES OPTIONS POUR MS EXCHANGE SINGLE MAILBOX
	-originalfolder	
	-keep_msg	
	-overwrite_msg	
	-folder	
	-exclude	
	-instant_restore	NOUVELLES OPTIONS POUR RESTAURATION VSS
	-conf_check	
	-no_recovery	
	-use_vds	
	–no_copy_back	
	-copy_back	
	-diskarray_wait	
	-delete_replica	
	-no_diskarray_wait	
	-no_retain_source	
	–exch_check	
	-exch_throttle	
	-appsrv	
	-target_tree	
	–exch_RSG	
	-target_dir	
	-copyid	NOUVELLES OPTIONS
	-no_auto_dev	
	-omit_unrequired_object_versions	

Commande	Sous-commande/Option	Etat
	-omit_unrequired_object_versions	OPTION OBSOLETE Remplacée par -omit_unrequired _object_versions
omnirpt	-smtp	NOUVELLES OPTIONS
	-copylist_sch	
	-copylist_post	
	-no_copylist	
	-conslist_sch	
	-conslist_post	
	-no_conslist	
	-num_copies	
	obj_copies	NOUVEAUX RAPPORTS
	session_objcopies	
	session_errors	
	session_statistics	
	backup_errors	RAPPORTS OBSOLETES
	backup_statistics	
omniresolve		NOUVELLE COMMANDE
omnisetup.sh	-CM	NOUVELLES OPTIONS
	-IS	
	-autopass	
	smisa	NOUVEAUX COMPOSANTS LOGICIELS
	sapdb	
	docs	
	javagui	
	vmware	
	vls_am	

Commande	Sous-commande/Option	Etat
	acs	COMPOSANTS OBSOLETES DU LOGICIEL
	das	
	momgui	
omnistoreap-putil		NOUVELLE COMMANDE
omniusers		NOUVELLE COMMANDE
sanconf	-[no_]multipath	NOUVELLES OPTIONS
	-remove_hosts	
	-sanstableaddressing	
up-grade_cm_from_evaa		NOUVELLE COMMANDE
uma	-vls_address	NOUVELLES OPTIONS
	-vls_port	
	-vls_username	
	-vls_password	
winomnimi-grate.pl		NOUVELLE COMMANDE
uma	-vls_address	NOUVELLES OPTIONS
	-vls_port	
	-vls_username	
	-vls_password	

Tableau 35 - Mise à niveau à partir de Data Protector A.05.50

Commande	Sous-commande/Option	Etat
cjutil		NOUVELLE COMMANDE
ob2install	sps	NOUVEAU COMPOSANT LOGICIEL
	vmware	
	vls_am	
	momgui	COMPOSANT OBSOLETE DU LOGICIEL

Commande	Sous-commande/Option	Etat
omnib	-mssps_list	NOUVELLES INTEGRATIONS
	-vmware_list	
	-enh_incr	NOUVELLES OPTIONS
	-async	
	-encode aes256	
	-iap	
	-clp	
omnicc	-import_vls	NOUVELLES OPTIONS
	-import_iap	
	-cert_mode	
	-cert_name	
	-add_certificate	
	-get_certificate	
	-list_certificates	
	-port	OPTIONS MODIFIEES
	-user	
	-passwd	
omnicjutil		NOUVELLE COMMANDE
omnidb	-mssps	NOUVELLES INTEGRATIONS
	-vmware	
	-auditing	NOUVELLES OPTIONS
	-timeframe	
omnidbcheck	-keystore	NOUVELLES OPTIONS
	-summary	
omnidbsmis	-ssl	NOUVELLES OPTIONS
	-caconf	
	-init	
	-put *nom_de_fichier*	
	-get *nom_de_fichier*	
	-list *Nom EVA*	
	-check *Nom groupe RD*	

Commande	Sous-commande/Option	Etat
omnidbeva		COMMANDE OBSOLETE
omnidlc	-add_info	NOUVELLES OPTIONS
	-pack	
	-no_config	
	-any	
	-del_tracelog	
omnicreatedl	-replica_conf local	NOUVELLES OPTIONS POUR HP StorageWorks ENTERPRISE VIRTUAL ARRAY
	-replica_conf combined	
	-ca_failover_option follow_replica_direction	
	–ca_faiover_option maintain_replica_location	
omnidbrestore	–keyfile	NOUVELLE OPTION
omnidbutil	-extendtblspace	NOUVELLES OPTIONS
	-free_cell_resources	
	-list_large_directories	
	-list_large_mpos	
	-list_mpos_without_overs	
	-readdb	OPTION MODIFIEE
omnidbvss		NOUVELLE COMMANDE
omnidlc	-debug_loc	NOUVELLE OPTION
omniinetpasswd		NOUVELLE COMMANDE
omniiso	–autoinject -waik -inject_drivers	NOUVELLES OPTIONS
omnikeymigrate		NOUVELLE COMMANDE
omnikeytool		NOUVELLE COMMANDE
omnimigrate.pl		COMMANDE MISE A JOUR

Commande	Sous-commande/Option	Etat
omnimcopy	–encrypt	NOUVELLE OPTION
	-ams	
	-copy	OPTIONS MODIFIEES
	-from	
	-pool	
omnimm	-[no_]free_pool	OPTION MODIFIEE
	-create_free_pool	NOUVELLE OPTION
omniobjcopy	-mssps	NOUVELLES INTEGRATIONS
	-vmware	
	–encrypt	NOUVELLE OPTION
omniobjconsol-idate		NOUVELLE COMMANDE
omnir	-mssps	NOUVELLES INTEGRATIONS
	-vmware	
	-portal	NOUVELLES OPTIONS POUR MS SPS
	-ssodb	
	-doclib	
	-tohost	
	-instance	
	-as	
	-todir	
	-changemaster	
	-public	NOUVELLES OPTIONS POUR MS EXCHANGE SINGLE MAILBOX
	-originalfolder	
	-keep_msg	
	-overwrite_msg	
	-folder	
	-exclude	
	-instant_restore	NOUVELLES OPTIONS POUR RESTAURATION VSS
	-conf_check	
	-no_recovery	
	-use_vds	

Commande	Sous-commande/Option	Etat
	–no_copy_back -copy_back	
	-diskarray_wait	
	-delete_replica	
	-no_diskarray_wait	
	-no_retain_source	
	–exch_check	
	-exch_throttle	
	-appsrv	
	-target_tree	
	–exch_RSG	
	-target_dir	
	-no_auto_dev	NOUVELLES OPTIONS
	-omit_unrequired_object_ver-sions	
	-omit_unrequired_incrementals	OPTION OBSOLETE Remplacée par -omit_unre-quired _object_ver-sions
	-smtp	NOUVELLES OPTIONS
	-copylist_sch	
	-copylist_post	
	-no_copylist	
	-conslist_sch	
	-conslist_post	
	-no_conslist	
	-num_copies	
	obj_copies	NOUVEAUX RAPPORTS
	session_objcopies	
	session_errors	
	session_statistics	

Commande	Sous-commande/Option	Etat
	session_statistics backup_errors	
omnisetup.sh	docs	NOUVEAUX COMPOSANTS LOGICIELS
	javagui	
	vmware	
	vls_am	
	momgui	COMPOSANT OBSOLETE DU LOGICIEL
omnistoreap-putil		NOUVELLE COMMANDE
up-grade_cm_from_evaa		NOUVELLE COMMANDE
up-grade_cfg_from_evaa		COMMANDE OBSOLETE
winomnimi-grate.pl		NOUVELLE COMMANDE

Tableau 36 - Mise à niveau à partir de Data Protector A.06.00

Commande	Sous-commande/Option	Etat
cjutil	backup_statistics	NOUVELLE COMMANDE
ob2install	sps	NOUVEAUX COMPOSANTS LOGICIELS
	vmware	
	vls_am	
	momgui	COMPOSANT OBSOLETE DU LOGICIEL

Commande	Sous-commande/Option	Etat
omnib	-mssps_list	NOUVELLES INTEGRATIONS
	-vmware_list	
	-async	NOUVELLES OPTIONS
	-encode aes256	
	-iap	
	-clp	
omnicc	-import_vls	NOUVELLES OPTIONS
	-import_iap	
	–cert_mode	
	–cert_name	
	-add_certificate	
	-get_certificate	
	-list_certificates	
	-port	OPTIONS MODIFIEES
	-user	
	-passwd	
omnicjutil		NOUVELLE COMMANDE
omnidb	-mssps	NOUVELLES INTEGRATIONS
	-vmware	
	-auditing	NOUVELLES OPTIONS
	-timeframe	
omnidbcheck	-keystore	NOUVELLES OPTIONS
	-summary	
omnidbvss	–init –list session –list disk –get session –get disk –remove session –remove disk	NOUVELLES OPTIONS
	–get table –list table –remove table	OPTIONS OBSOLETES

Commande	Sous-commande/Option	Etat
omnidbrestore	-keyfile	NOUVELLE OPTION
omnidbutil	-free_cell_resources	NOUVELLES OPTIONS
	-list_large_directories	
	-list_large_mpos	
	-list_mpos_without_overs	
omnidlc	-add_info	NOUVELLES OPTIONS
	-pack	
	-no_config	
	-any	
	-del_tracelog	
omniinetpasswd		NOUVELLE COMMANDE
omniiso	-autoinject -waik -inject_drivers	NOUVELLES OPTIONS
omnikeymigrate		NOUVELLE COMMANDE
omnikeytool		NOUVELLE COMMANDE
omnimcopy	-encrypt	NOUVELLE OPTION
	-ams	
	-copy	OPTIONS MODIFIEES
	-from	
	-pool	
omniobjconsol-idate	-encrypt	NOUVELLE OPTION
omniobjcopy	-mssps	NOUVELLES INTEGRATIONS
	-vmware	
	-encrypt	NOUVELLE OPTION

Commande	Sous-commande/Option	Etat
omnir	-mssps	NOUVELLES INTEGRATIONS
	-vmware	
	-no_auto_dev	NOUVELLES OPTIONS
	-omit_unrequired_object_ver-sions	
	-omit_unrequired_incrementals	OPTION OBSOLETE Remplacée par -omit_unre-quired _object_ver-sions.
	-instant_restore	NOUVELLES OPTIONS POUR RESTAURATION VSS
	-conf_check	
	-no_recovery	
	-use_vds	
	–no_copy_back	
	-copy_back	
	-diskarray_wait	
	-delete_replica	
	-no_diskarray_wait	
	-no_retain_source	
	–exch_check	
	-exch_throttle	
	-appsrv	
	-target_tree	
	–exch_RSG	
	-target_dir	
	-delete_current	OPTION OBSOLETE

Commande	Sous-commande/Option	Etat
omnirpt	-copylist_sch	NOUVELLES OPTIONS
	-copylist_post	
	-conslist_sch	
	-conslist_post	
	-num_copies	
	-copylist	OPTIONS OBSOLETES
	-conslist	
	obj_copies	NOUVEAUX RAPPORTS
	session_objcopies	
	session_errors	
	session_statistics	
	backup_errors	RAPPORTS OBSOLETES
	backup_statistics	
omnisetup.sh	docs	NOUVEAUX COMPOSANTS LOGICIELS
	javagui	
	vmware	
	vls_am	
	momgui	COMPOSANT OBSOLETE DU LOGICIEL
	-IS1 -IS2	OPTIONS OBSOLETES
omnistoreap-putil		NOUVELLE COMMANDE
uma	-vls_address	NOUVELLES OPTIONS
	-vls_port	
	-vls_username	
	-vls_password	

Tableau 37 - Mise à niveau à partir de Application Recovery Manager A.06.00

Commande	Sous-commande/Option	Etat
`omnib`	`-disk_only`	NOUVELLE OPTION Nécessaire pour une sauvegarde ZDB sur disque
	Nouvelles options d'intégrations et de système de fichiers.	NOUVELLES OPTIONS
`omnidb`	Nouvelles options relatives à la gestion des supports et autre nouvelle fonctionnalité de Data Protector.	NOUVELLES OPTIONS
`omnidbutil`	Nouvelles options relatives à la gestion des supports et autre nouvelle fonctionnalité de Data Protector.	NOUVELLES OPTIONS
`omnir`	Nouvelles options d'intégrations et de système de fichiers. Les options d'Application Recovery Manager A.06.00 sont disponibles.	L'UTILISATION DE LA COMMANDE EST TRES MODIFIEE Reportez-vous à la section *Guide de rfrence de l'interface de ligne de commande HP Data Protector*.
`utild_cmd`	Nouvelles options d'intégrations et de système de fichiers.	NOUVELLES OPTIONS
`dbtool.pl`		COMMANDE OBSOLETE Remplacée par la sauvegarde de la base de données interne.
REMARQUE : La première partie de la table recense uniquement les modifications apportées aux commandes déjà disponibles dans Application Recovery Manager A.06.00 et qui peuvent affecter vos scripts. *Toutes les commandes introduites avec Data Protector* sont indiquées ci-dessous comme "NOUVELLE COMMANDE".		
`cjutil`		NOUVELLE COMMANDE
`NNMpost`		NOUVELLE COMMANDE

Commande	Sous-commande/Option	Etat
NNMpre		NOUVELLE COMMANDE
NNMscript		NOUVELLE COMMANDE
ob2install		NOUVELLE COMMANDE
omniamo		NOUVELLE COMMANDE
omnicjutil		NOUVELLE COMMANDE
omnicreatedl		NOUVELLE COMMANDE
omnidbrestore		NOUVELLE COMMANDE
omnidbupgrade		NOUVELLE COMMANDE
omnidbva		NOUVELLE COMMANDE
omnidbxp		NOUVELLE COMMANDE
omnidownload		NOUVELLE COMMANDE
omnidr		NOUVELLE COMMANDE
omniinetpasswd		NOUVELLE COMMANDE
omniiso		NOUVELLE COMMANDE
omnimcopy		NOUVELLE COMMANDE
omnimigrate.pl		NOUVELLE COMMANDE
omniminit		NOUVELLE COMMANDE
omnimlist		NOUVELLE COMMANDE

Commande	Sous-commande/Option	Etat
omnimm		NOUVELLE COMMANDE
omnimnt		NOUVELLE COMMANDE
omnimver		NOUVELLE COMMANDE
omniobjcopy		NOUVELLE COMMANDE
omniobjconsol-idate		NOUVELLE COMMANDE
omniofflr		NOUVELLE COMMANDE
omniresolve		NOUVELLE COMMANDE
omnirpt		NOUVELLE COMMANDE
omnisetup.sh		NOUVELLE COMMANDE
omnisrdupdate		NOUVELLE COMMANDE
omnistat		NOUVELLE COMMANDE
omnistoreap-putil		NOUVELLE COMMANDE
omniupload		NOUVELLE COMMANDE
sanconf		NOUVELLE COMMANDE
syb_tool		NOUVELLE COMMANDE
uma		NOUVELLE COMMANDE

Commande	Sous-commande/Option	Etat
`up-grade_cm_from_evaa`		NOUVELLE COMMANDE
`util_cmd`		NOUVELLE COMMANDE
`util_ora-cle8.pl`		NOUVELLE COMMANDE

Glossaire

ACSLS	*(terme propre à Windows)* Le service d'annuaire d'un réseau Windows. Il contient des informations sur les ressources du réseau et les rend accessibles aux utilisateurs et aux applications. Les services d'annuaire permettent de nommer, de décrire, de localiser, de consulter et de gérer les ressources de manière cohérente, quel que soit le système physique sur lequel elles résident.
Active Directory	Cryptage sur logiciel Data Protector basé sur l'algorithme de cryptage AES-CTR (Advanced Encryption Standard in Counter Mode) qui utilise des clés aléatoires d'une longueur de 256 bits. C'est la même clé qui est utilisée à la fois pour le cryptage et le décryptage. Avec le cryptage AES 256 bits, les données sont cryptées avant d'être transférées sur un réseau et d'être écrites sur un support.
adresse IP	*(terme propre à EMASS/GRAU)* Automated Mixed-Media library, bibliothèque de supports mixtes automatisée.
affichage de sauvegarde	Composant requis sur un client pour sauvegarder ou restaurer des intégrations de bases de données en ligne. *Voir aussi* Agent de disque.
agent d'application	*(terme propre à ZDB)* Système sur lequel tourne l'application ou la base de données. Les données de l'application ou de la base de données sont situées sur les volumes source. *Voir aussi* système de sauvegarde et volume source.
Agent de disque	*(terme propre à Oracle)* Egalement appelé journal de rétablissement hors ligne. Si la base de données Oracle fonctionne en mode ARCHIVELOG, chaque journal de rétablissement en ligne, lorsqu'il est plein, est copié dans un emplacement de destination des journaux archivés. Cette copie est appelée journal de rétablissement archivé. La présence ou l'absence d'un journal de rétablissement archivé est déterminée par le mode que la base de données utilise : • ARCHIVELOG - Les fichiers journaux de rétablissement en ligne pleins sont archivés avant d'être réutilisés. La base de données peut être récupérée en cas de défaillance d'un disque ou d'une instance. Vous ne pouvez effectuer

de sauvegarde "à chaud" que si la base de données fonctionne dans ce mode.

- NOARCHIVELOG - Les fichiers journaux de rétablissement en ligne pleins ne sont pas archivés.

Voir aussi journal de rétablissement en ligne.

Agent de support

(terme propre à Lotus Domino Server) Mode de la base de données Lotus Domino Server avec lequel les fichiers journaux de transactions sont seulement écrasés après avoir été sauvegardés.

Agent EMC Symmetrix (SYMA) *(terme propre à EMC Symmetrix)*

Ensemble de fichiers stockés sur plusieurs disquettes, nécessaires pour la reconfiguration appropriée du disque de rechange (partition du disque et configuration des volumes logiques), ainsi que pour la récupération automatique du système d'origine et des données utilisateur sauvegardées lors de la sauvegarde complète du client. Ces fichiers sont stockés comme fichier archive ASR sur le Gestionnaire de cellule (dans `répertoire_Data_ProtectorConfig\Server\dr\asr` sur un Gestionnaire de cellule Windows ou dans `/etc/opt/omni/server/dr/asr/` sur un Gestionnaire de cellule UNIX) ainsi que sur le support de sauvegarde. Le fichier archive ASR est extrait sur trois disquettes sur les systèmes Windows 32 bits, ou sur quatre disquettes sur les systèmes Windows 64 bits lorsqu'un sinistre a eu lieu. Ces disquettes sont nécessaires pour effectuer l'ASR.

Agent SMI-S HP StorageWorks EVA

Fichiers de données dans lesquels les informations d'audit sont stockées.

agent SSE

Sortie lisible par l'utilisateur d'informations d'audit créées à partir des données stockées dans les fichiers journaux d'audit.

agent Symmetrix (SYMA)

Données concernant chaque session de sauvegarde effectuée sur une période étendue et définie par l'utilisateur, sur l'ensemble de la cellule Data Protector.

Agents de disque simultanés

Voir bibliothèque.

AML

Voir bibliothèque.

analyse

(terme propre à Oracle) Il s'agit d'un gestionnaire de systèmes de fichiers et de volumes intégré à Oracle 10g/11g pour les fichiers de base de données Oracle. Il simplifie la gestion des données et des disques et fournit des fonctions de mise en miroir et de répartition sur plusieurs axes pour optimiser les performances.

analyser — *(terme propre à VLS)* Fonctionnalité qui permet de procéder initialement à la sauvegarde des données sur les bandes virtuelles des VLS, puis de les faire migrer vers des bandes physiques (une bande virtuelle émulant une bande physique) sans utiliser d'application de sauvegarde intermédiaire.
Voir aussi Système de bibliothèque virtuelle (VLS) et bande virtuelle.

API C Lotus — *(terme propre à SAP R/3)* Par le biais d'une interface ouverte, les programmes de sauvegarde SAP R/3 peuvent appeler l'interface backint Data Protector, laquelle leur permet de communiquer avec le logiciel Data Protector. En ce qui concerne la restauration et la sauvegarde, les programmes SAP R/3 émettent des ordres destinés à l'interface backint Data Protector.

API de sauvegarde — Programme Oracle servant d'interface entre l'utilitaire de sauvegarde/restauration d'Oracle et la couche de gestion des supports de sauvegarde/restauration. L'interface définit un ensemble de routines afin de permettre la lecture et l'écriture des données sur les supports de sauvegarde, ainsi que la création, la recherche et la suppression des fichiers de sauvegarde.

API Sybase Backup Server — *Voir* chaîne de restauration.

application compatible cluster — Périphérique configuré pour une utilisation avec Data Protector, capable d'écrire et de lire des données sur un support de stockage. Il peut s'agir, par exemple, d'un lecteur DDS/DAT autonome ou d'une bibliothèque.

archivage des journaux — Une génération de sauvegarde est constituée d'une sauvegarde complète, ainsi que de toutes les sauvegardes incrémentales effectuées jusqu'à la prochaine sauvegarde complète.

auto-migration — Identificateur d'un objet d'intégration qui correspond à l'ID de session de la sauvegarde de cet objet. L'ID de sauvegarde est conservé quand un objet est copié, exporté ou importé.

BACKINT — Unité de sauvegarde contenant tous les éléments sauvegardés d'un volume de disque (disque logique ou point de montage). Les éléments sauvegardés peuvent être des fichiers, des répertoires ou l'ensemble du disque ou du point de montage. En outre, un objet sauvegarde peut être une entité de base de données/d'application ou une image disque (rawdisk).
Un objet sauvegarde est défini comme suit :

- Nom de client : nom d'hôte du client Data Protector dans lequel l'objet sauvegarde est hébergé.
- Point de montage : pour des objets système de fichiers — point d'accès dans une structure de répertoires (lecteur sous Windows et point de montage sous UNIX) sur le client contenant l'objet sauvegarde. Pour des objets intégration — identificateur du flux de sauvegarde, indiquant les éléments base de données/application sauvegardés.
- Description : pour les objets système de fichiers — définit exclusivement les objets avec un nom de client et un point de montage identiques. Pour les objets d'intégration — affiche le type d'intégration (SAP ou Lotus, par exemple).
- Type : type de l'objet sauvegarde. Pour les objets système de fichiers — type de système de fichiers (WinFS, par exemple). Pour les objets d'intégration — "Bar".

bande virtuelle

Chaque objet sauvegarde de l'IDB a un propriétaire. Par défaut, il s'agit de l'utilisateur qui a lancé la session de sauvegarde.

banque de boîtes aux lettres

Processus consistant à créer une copie des données sur un support de stockage. Les activités sont définies dans une spécification de sauvegarde ou une session interactive. L'ensemble des clients configurés dans une spécification de sauvegarde est sauvegardé lors d'une session de sauvegarde unique, par le biais du même type de sauvegarde (complète ou incrémentale). Le résultat d'une session de sauvegarde est un ensemble de supports sur lesquels des données ont été écrites ; celui-ci est également appelé jeu de sauvegarde ou de supports.
Voir aussi spécification de sauvegarde, sauvegarde incrémentale et sauvegarde complète.

banque de clés

Ensemble complet d'objets d'intégration associés à une sauvegarde.

banque de dossiers publics

(terme propre à Oracle) Regroupement logique de fichiers sauvegardés qui sont créés à l'aide de la commande de sauvegarde RMAN. Un jeu de sauvegarde est un ensemble complet de fichiers associés à une sauvegarde. Pour améliorer les performances, les fichiers peuvent être multiplexés. Un jeu de sauvegarde contient soit des fichiers de données soit des journaux d'archive, mais non les deux à la fois.

banque d'informations

Liste d'objets à sauvegarder, accompagnée d'un ensemble de périphériques ou de lecteurs à utiliser, d'options de sauvegarde pour tous les objets spécifiés, ainsi que du jour et de l'heure où les sauvegardes doivent être effectuées. Les objets peuvent être des disques/volumes entiers ou une partie de ceux-ci ; il peut

s'agir par exemple de fichiers, de répertoires, voire même du registre Windows. L'utilisateur peut définir des listes de sélection de fichiers, telles que les listes d'inclusion ou d'exclusion.

basculement

(terme propre à ZDB) Système connecté aux volumes cibles d'un ou plusieurs systèmes d'application. Le système de sauvegarde est généralement connecté à un(e) périphérique de sauvegarde pour procéder à la sauvegarde des données dans la réplique. *Voir aussi* système d'application, volume cible et réplique.

basculement

Voir sauvegarde incrémentale, sauvegarde différentielle, sauvegarde de transactions, sauvegarde complète et sauvegarde delta.

Base de données centralisée de gestion des supports (CMMDB)

Sauvegarde de Data Protector vers le dispositif HP IAP (Integrated Archiving Platform). Elle s'appuie sur la capacité d'IAP à éliminer les redondances des données stockées au niveau des blocs (segments) en créant une adresse de contenu unique pour chaque segment de données. Seuls les segments modifiés sont transmis sur le réseau et ajoutés à la banque.

base de données cible

Data Protector propose plusieurs affichages pour les spécifications de sauvegarde :
Par type - en fonction du type de données disponibles pour les sauvegardes ou les modèles. Affichage par défaut.
Par groupe - en fonction du groupe auquel les spécifications/modèles de sauvegarde appartiennent.
Par nom - en fonction du nom des spécifications/modèles de sauvegarde.
Par gestionnaire - si vous utilisez le MoM, vous pouvez également définir l'affichage de sauvegarde en fonction du Gestionnaire de cellule auquel appartiennent les spécifications/modèles de sauvegarde.

Base de données de registres COM+

(terme propre à EMC Symmetrix) Business Continuance - Procédé permettant aux utilisateurs d'accéder et de gérer des copies instantanées des périphériques standard EMC Symmetrix.
Voir aussi BCV.

base de données du catalogue de récupération

(terme propre à HP StorageWorks Disk Array XP) La fonction Business Copy (BC) XP permet à l'utilisateur de conserver des copies internes des LDEV HP StorageWorks Disk Array XP afin de sauvegarder ou de dupliquer des données par exemple. Les copies (volumes secondaires ou S-VOL) peuvent être séparées des volumes principaux (P-VOL) et connectées à un système différent, à des fins aussi diverses que la sauvegarde ou le développement. Pour la sauvegarde, les P-VOL doivent être

connectés au système d'application et l'un des jeux de miroirs S-VOL doit être connecté au système de sauvegarde.
Voir aussi HP StorageWorks Disk Array XP LDEV, CA, unité de commande principale, système d'application et système de sauvegarde.

base de données du gestionnaire de supports amovibles

(terme propre à HP StorageWorks EVA) Business Copy EVA est une solution logicielle de réplication locale qui vous permet de créer des copies à un instant donné (répliques) des volumes sources en utilisant les fonctions de snapshot et de clonage du microprogramme EVA.
Voir aussi réplique, volume source, snapshot, et CA+BC EVA.

base de données ZDB

(terme propre à EMC Symmetrix) Solution d'environnement de stockage protégé dans le cadre de laquelle des périphériques EMC Symmetrix ont été spécialement configurés en tant que miroirs ou volumes CB pour protéger les données stockées sur des périphériques EMC Symmetrix standard.
Voir aussi BCV.

bases de données système

(terme propre à HP StorageWorks Virtual Array) Business Copy VA vous permet de conserver des copies internes des LUN HP StorageWorks Virtual Array pour la sauvegarde ou la duplication de données dans une même baie de virtualisation. Les copies (LUN enfants ou Business Copy) peuvent être utilisées à des fins aussi diverses que la sauvegarde, l'analyse de données ou le développement. Lorsqu'ils sont utilisés à des fins de sauvegarde, les LUN d'origine (parents) sont connectés au système d'applications. Les LUN Business Copy (enfants) sont, quant à eux, connectés au système de sauvegarde.
Voir aussi LUN HP StorageWorks Virtual Array système d'application et système de sauvegarde.

BC

*(terme propre à EMC Symmetrix)*Business Continuance Volumes ou périphériques BCV - il s'agit de SLD dédiés, préconfigurés dans l'ICDA sur lequel l'opération Business Continuance est exécutée. Des adresses SCSI distinctes, lesquelles diffèrent des adresses utilisées par les SLD dont elles sont le miroir, sont attribuées aux périphériques BCV. Ces derniers sont utilisés comme miroirs séparables des SLD EMC Symmetrix principaux devant être protégés.
Voir aussi BC et Processus BC.

BC

Les opérateurs booléens pour la fonction de recherche sur le texte entier du système d'aide en ligne sont AND, OR, NOT et NEAR (ET, OU, NON et PROCHE). Utilisés lors d'une recherche, ils vous permettent de définir précisément votre requête en établissant une relation entre les termes de la recherche. Si vous ne spécifiez aucun opérateur dans une

recherche comportant plusieurs termes, l'opérateur AND est utilisé par défaut. Par exemple, la requête récupération après sinistre manuelle est équivalente à manuelle AND sinistre AND récupération.

BC EVA

Volume/disque/partition contenant les fichiers nécessaires à la première étape du processus d'amorçage. La terminologie utilisée par Microsoft définit le volume/disque/partition d'amorçage comme le volume/disque/partition contenant les fichiers du système d'exploitation.

BC VA

(terme propre à SAP R/3) Outil de sauvegarde SAP R/3 permettant à l'utilisateur d'archiver les fichiers journaux de rétablissement. BRARCHIVE permet également d'enregistrer l'ensemble des journaux et profils du processus d'archivage. *Voir aussi* BRBACKUP et BRRESTORE.

BCV

(terme propre à SAP R/3) Outil de sauvegarde SAP R/3 permettant d'effectuer une sauvegarde en ligne ou hors ligne du fichier de contrôle, de fichiers de données distincts ou de l'ensemble des espaces de tables et, le cas échéant, des fichiers journaux de rétablissement en ligne.
Voir aussi BRARCHIVE et BRRESTORE.

bibliothèque

(terme propre à SAP R/3) Outil de sauvegarde SAP R/3 pouvant être utilisé pour restaurer les types de fichiers suivants :

- fichiers de données de base de données, fichiers de contrôle et fichiers journaux de rétablissement en ligne sauvegardés avec BRBACKUP
- fichiers journaux de rétablissement archivés avec BRARCHIVE
- fichiers "non-base de données" sauvegardés avec BRBACKUP

Vous pouvez spécifier des fichiers, des espaces de table, des sauvegardes complètes, des numéros de séquence de fichiers journaux de rétablissement ou l'ID de session de la sauvegarde. *Voir aussi* BRBACKUP et BRARCHIVE.

bibliothèque de bandes magnéto-optiques

Le Backup Session Manager Data Protector (Gestionnaire de session de sauvegarde) contrôle la session de sauvegarde. Ce processus est toujours exécuté sur le système du Gestionnaire de cellule.

bibliothèque de bandes virtuelle (VTL, pour Virtual Tape Library)

(terme propre à HP StorageWorks Disk Array XP) La fonction Continuous Access (CA) XP permet à l'utilisateur de créer et de conserver des copies distantes de LDEV HP StorageWorks Disk Array XP pour la duplication ou la sauvegarde de données, ou la récupération après sinistre. Les opérations CA impliquent

les baies de disques principales et distantes (secondaires). Les premières concernent les volumes principaux CA (P-VOL), contenant les données d'origine, qui sont connectés au système d'application. Les secondes contiennent les volumes secondaires AC (S-VOL) qui sont connectés au système de sauvegarde.
Voir aussi BC *(terme propre à HP StorageWorks Disk Array XP)*, unité de commande principale et HP StorageWorks Disk Array XP LDEV.

bibliothèque de base de données

(terme propre à HP StorageWorks EVA) L'utilisation combinée de Continuous Access (CA) EVA et de Business Copy (BC) EVA vous permet de créer et de conserver des copies (répliques) des volumes sources sur une baie EVA distante, puis d'utiliser ces copies comme source pour une réplication locale sur cette baie distante.
Voir aussi BC EVA, réplique et volume source.

bibliothèque du Gestionnaire RAID

(terme spécifique à StorageTek) Cartridge Access Port - port d'accès intégré au panneau porte d'une bibliothèque permettant d'insérer ou d'éjecter les supports.

bibliothèque StorageTek ACS

Permet de définir la durée pendant laquelle les informations concernant les données sauvegardées (noms et versions de fichiers) sont conservées dans la base de données IDB.
Voir aussi protection des données.

boîte aux lettres

Catalog Database, Base de données du catalogue - Il s'agit d'une partie de la base de données IDB contenant des informations sur les sauvegardes, les copies d'objet, les restaurations, les sessions de gestion de supports, ainsi que sur les données sauvegardées. En fonction du niveau de journalisation sélectionné, la CDB contient également les noms et versions de fichiers. Cette partie de la base de données se trouve toujours dans la cellule locale.
Voir aussi MMDB.

BRARCHIVE

(terme propre à UNIX) Context Dependent File, fichier contextuel - Il s'agit d'un fichier constitué de plusieurs fichiers regroupés sous le même chemin d'accès. Le système sélectionne habituellement l'un des fichiers à l'aide du contexte du processus. Ce mécanisme permet à des exécutables dépendant des machines, à des fichiers de données système et à des fichiers de périphériques de fonctionner correctement depuis l'ensemble des hôtes d'un cluster, tout en utilisant le même chemin d'accès.

BRBACKUP

Ensemble de systèmes contrôlés par un Gestionnaire de cellule. Une cellule représente habituellement les systèmes d'un site ou

d'une entité organisationnelle qui sont connectés à un même réseau local. Un contrôle centralisé permet d'administrer les tâches et les stratégies de sauvegarde et de restauration.

BRRESTORE

Système principal de la cellule dans lequel est installé le logiciel Data Protector central et d'où sont gérées toutes les activités de sauvegarde et de restauration. L'interface graphique utilisée pour les opérations de gestion peut se trouver sur un système différent. Chaque cellule dispose d'un Gestionnaire de cellule.

BSM

Data Protector permet de configurer une gestion centralisée des licences pour l'ensemble de l'environnement de l'entreprise, constitué de plusieurs cellules. Toutes les licences Data Protector sont installées et conservées dans le système du Gestionnaire de cellule d'entreprise. En fonction de vos besoins, vous pouvez ensuite affecter des licences à des cellules spécifiques.
Voir aussi MoM.

CA

Voir CMMDB.

CA+BC EVA

(Terme propre à Windows) Fonction du système de fichiers Windows, qui consigne un enregistrement de chaque modification survenant au niveau des fichiers et répertoires d'un volume NTFS local.

canal

(terme propre à Windows) Module pouvant être interrogé pour déterminer quels objets d'un système de fichiers ont été créés, modifiés ou supprimés.

CAP

(terme propre à Oracle) Allocation de ressources du Gestionnaire de récupération Oracle. Chaque canal alloué lance un nouveau processus Oracle qui effectue des opérations de sauvegarde, de restauration et de récupération. Le type de canal affecté détermine le type de support utilisé :

- type 'disque'
- type 'sbt_tape'

Si le canal spécifié est de type 'sbt_tape' et qu'Oracle est intégré à Data Protector, le processus du serveur essaie de lire les sauvegardes ou d'écrire les fichiers de données sur Data Protector.

caractère générique

(terme propre à IAP) Processus consistant à diviser les données en blocs (segments), qui reçoivent chacun une adresse de contenu unique. Cette adresse sert ensuite à déterminer si un segment en particulier est déjà sauvegardé sur le dispositif IAP. Si des données dupliquées sont identifiées (deux adresses sont identiques, à savoir que l'adresse est la même que celle d'un autre segment de données déjà stocké dans IAP), elles ne

sont pas sauvegardées. Ainsi, les données redondantes sont éliminées et le stockage est optimal.
Voir aussi sauvegarde sur IAP.

Catalogue de récupération

(terme propre à Microsoft Exchange Server et Lotus Domino Server) L'enregistrement circulaire est un mode de base de données Microsoft Exchange Server et Lotus Notes/Domino Server, dans lequel le contenu des fichiers journaux de transactions est périodiquement réécrit une fois que les données correspondantes ont été transmises à la base de données. L'enregistrement circulaire réduit les besoins en espace disque.

CDB

Sauvegarde de tous les systèmes de fichiers montés sur un client. Les systèmes de fichiers montés sur le client une fois la spécification de sauvegarde créée ne sont pas détectés automatiquement.

CDF, fichier

Sauvegarde de tous les systèmes de fichiers montés sur un client. Lorsque la sauvegarde commence, Data Protector découvre les disques se trouvant sur les clients. La sauvegarde du client avec découverte de disque permet de simplifier la configuration de la sauvegarde et d'améliorer la couverture de sauvegarde des systèmes sur lesquels des disques sont fréquemment montés/démontés.

cellule

ou système client Tout système configuré avec des fonctions Data Protector et dans une cellule.

chaîne de périphériques

Application prenant en charge d'API cluster (Application Programming Interface). Chaque application compatible cluster déclare ses propres ressources critiques (volumes de disques (sous Microsoft Cluster Server), groupes de volumes (sous MC/ServiceGuard), services d'application, noms et adresses IP, etc.).

chaîne de restauration

(terme propre à Microsoft Exchange Server) Cluster Continuous Replication (CCR ou réplication continue en cluster) est une solution de haute disponibilité qui fait appel à des options de gestion des clusters et de basculement pour créer et conserver une copie exacte (copie CCR) d'un groupe de stockage. Un groupe de stockage est répliqué sur un serveur distinct. CCR supprime tous les points de défaillance de vos serveurs de back-end Exchange. Vous pouvez procéder à des sauvegardes à l'aide de VSS sur le noeud Exchange Server passif qui contient une copie CCR, de telle sorte à réduire la charge sur le noeud actif.
Les copies CCR servent à des fins de récupération après sinistre, puisqu'il est possible de basculer sur la copie CCR en quelques secondes. Un groupe de stockage répliqué est

représenté comme une nouvelle instance du module d'écriture Exchange nommé Service de réplication Exchange et peut être sauvegardé (à l'aide de VSS) comme n'importe quel groupe de stockage.
Voir aussi Service de réplication Exchange et Local Continuous Replication.

chaîne de sauvegarde

(terme propre à Informix Server) Script CMD Windows créé dans INFORMIXDIR lorsqu'une base de données Informix Serveur est configurée. Le script CMD est un ensemble de commandes système chargé d'exporter les variables d'environnement pour Informix Server.

changeur automatique

Centralized Media Management Database, base de données centralisée de gestion des supports - La CMMDB Data Protector résulte de la fusion des bases de données de gestion des supports à partir de plusieurs cellules dans l'environnement MoM. Elle permet à l'utilisateur de partager des supports et périphériques haut de gamme avec plusieurs cellules dans un environnement MoM. Une cellule peut contrôler les systèmes robotiques desservant les périphériques connectés à des systèmes se trouvant dans d'autres cellules. La CMMDB doit résider sur le Gestionnaire MoM. Une connexion réseau fiable entre la cellule MoM et les autres cellules Data Protector est vivement recommandée.
Voir aussi MoM.

chargeur automatique

(terme propre à Windows) La base de données de registres COM+ et le registre Windows stockent les attributs d'applications, de classes et de matériels COM+. Elles garantissent ainsi la cohérence entre ces attributs et assurent un fonctionnement courant pour gérer ces derniers.

chargeurs

Ensemble de commandes de type DOS et UNIX qui peuvent être utilisées dans les scripts shell pour effectuer des tâches de configuration, de sauvegarde restauration, et de gestiondans Data Protector.

clé de session

(terme propre à HP StorageWorks EVA) Interface utilisateur permettant de configurer, d'administrer et de surveiller votre système de stockage HP StorageWorks EVA. Elle est utilisée pour effectuer diverses tâches de gestion du stockage, par exemple, la création de familles de disques virtuels, la gestion du matériel de stockage et la création de snapclones et de snapshots de disques virtuels. Le logiciel Command View EVA s'exécute sur le système de gestion du stockage HP. Il est accessible via un navigateur Web.
Voir aussi Agent SMI-S HP StorageWorks EVA et fournisseur HP StorageWorks SMI-S EVA.

client — *(terme propre à VLS)* Interface utilisateur graphique sur le Web servant à configurer, à gérer et à surveiller le VLS sur un réseau local.
Voir aussi VLS (Virtual Library System - Système de bibliothèques virtuelles).

client de gestion VMware — *Voir* simultanéité de l'Agent de disque.

client dynamique — *(terme propre à Oracle et SAP R/3)* Fichier de données Oracle contenant des entrées spécifiant la structure physique de la base de données. Il fournit des informations sur la cohérence de la base de données utilisées pour la récupération.

Cluster Continuous Replication — *(terme propre à HP StorageWorks EVA)* Paire formée par des volumes sources sur un EVA local et leurs répliques sur un EVA distant.
Voir aussi volume source, réplique et CA+BC EVA

CMMDB — Processus (service) CRS (Cell Request Server ou serveur des requêtes de cellule) qui s'exécute sur le Gestionnaire de cellule de Data Protector, et lance et contrôle les sessions de sauvegarde et de restauration. Le processus démarre dès que Data Protector est installé sur le Gestionnaire de cellule. Sur les systèmes Windows, le CRS s'exécute sous le compte de l'utilisateur spécifié lors de l'installation. Sur les systèmes UNIX, il s'exécute sous le compte `root`.

Command View (CV) EVA — Le Gestionnaire de session de copie et de consolidation (Copy and Consolidation Session Manager) Data Protector contrôle les sessions de copie et de consolidation d'objets et s'exécute sur le système du Gestionnaire de cellule.

Command View VLS — *(terme propre à Oracle et SAP R/3)* Fichier physique créé par Oracle et contenant des structures de données telles que les tables et index. Un fichier de données ne peut appartenir qu'à une seule base de données Oracle.

commandes de pré- et post-exécution — Permet de définir le délai de protection des données sauvegardées sur un support, c'est-à-dire la durée pendant laquelle Data Protector ne peut les écraser. Une fois ce délai expiré, Data Protector peut réutiliser le support lors d'une prochaine session de sauvegarde.
Voir aussi protection de catalogue.

compte utilisateur (compte utilisateur Data Protector) — Séquence de données transférées via le canal de communication.

consolidation d'objet	Sous Windows Vista et Windows Server 2008, il s'agit du répertoire contenant les fichiers de programme Data Protector. Sur les autres systèmes Windows, c'est le répertoire contenant les fichiers de données et de programme Data Protector. Le chemin par défaut est `%ProgramFiles%\OmniBack`, mais vous pouvez le modifier dans l'assistant d'installation de Data Protector au moment de l'installation. *Voir aussi* donnes_programme_Data_Protector.
conteneur	Sous Windows Vista et Windows Server 2008, il s'agit du répertoire contenant les fichiers de données Data Protector. Le chemin par défaut est `%ProgramData%\OmniBack`, mais vous pouvez le modifier dans l'assistant d'installation de Data Protector au moment de l'installation. *Voir aussi* répertoire_Data_Protector.
contrôleur de domaine	Ensemble de routines Data Protector permettant le transfert de données entre Data Protector et le serveur d'une intégration de base de données en ligne (serveur Oracle par exemple).
copie d'objet	Plusieurs bases de données sont sauvegardées simultanément si le nombre de périphériques disponibles permet d'effectuer des sauvegardes en parallèle.
copie d'objet	*(terme propre à HP StorageWorks EVA)* Regroupement logique de disques virtuels EVA. Ce groupe peut contenir jusqu'à huit jeux de copies à condition qu'ils aient des caractéristiques communes et partagent un journal CA EVA commun. *Voir aussi* jeu de copies.
copie intelligente	Ordinateur sur lequel est stockée une base de données volumineuse, une base de données SAP R/3 ou Microsoft SQL, par exemple. Une base de données stockée sur un serveur est accessible aux clients.
copie miroir	*(terme propre à Informix Server)* Objet base de données physique Informix Server. Il peut s'agir d'un blobspace, d'un dbspace ou d'un fichier journal logique.
création de snapshot	Le répertoire de catalogue des détails (DC) contient des fichiers binaires DC où sont stockées les informations relatives aux versions de fichier. Il constitue la partie DCBF de la base de données IDB, dont il occupe environ 80 %. Le répertoire DC par défaut est intitulé `dcbf` et se trouve sur le Gestionnaire de cellule, dans le répertoire `donnes_programme_Data_Protector\db40` (Windows Server 2008), `répertoire_Data_Protector\db40` (autres systèmes Windows) ou `/var/opt/omni/server/db40` (systèmes UNIX). Vous pouvez cependant en créer

davantage et utiliser un emplacement de votre choix. Chaque cellule peut gérer jusqu'à 10 répertoires DC. Par défaut, la taille maximale d'un répertoire DC est de 16 Go.

création de split mirror

La partie DCBF (Detail Catalog Binary Files) de la base de données IDB stocke des informations sur les versions et les attributs des fichiers. Cette partie occupe 80 % de la base IDB. Un fichier binaire DC est créé par support Data Protector utilisé pour la sauvegarde. Sa taille maximale est limitée par les paramètres de système de fichiers.

CRS

Sauvegarde contenant toutes les modifications apportées à la base de données depuis la dernière sauvegarde, quel qu'en soit le type.
Voir aussi types de sauvegarde.

Cryptage AES 256 bits

Unité physique contenant soit un lecteur, soit une unité plus complexe (une bibliothèque par exemple).

cryptage sur lecteur

Série de périphériques autonomes configurés pour une utilisation séquentielle. Lorsqu'un support contenu dans un périphérique est saturé, la sauvegarde se poursuit automatiquement sur le support du périphérique suivant dans la chaîne de périphériques.

CSM

(terme propre à EMC Symmetrix) Unité logique représentant plusieurs périphériques EMC Symmetrix. Un même périphérique ne peut appartenir à plus d'un groupe de périphériques. Tous les périphériques d'un groupe doivent se trouver sur la même unité EMC Symmetrix. Les groupes de périphériques vous permettent d'identifier et d'utiliser un sous-ensemble de périphériques EMC Symmetrix disponibles.

Dbobject

On dit qu'un périphérique fonctionne en mode continu s'il peut fournir un volume de données suffisant au support pour que celui-ci avance en continu. Dans le cas contraire, l'avancement de la bande doit être interrompu, le périphérique attend d'avoir reçu d'autres données, fait légèrement reculer la bande, puis reprend l'écriture des données, et ainsi de suite. En d'autres termes, si le taux auquel les données sont écrites sur la bande est inférieur ou égal à celui auquel elles sont fournies au périphérique par le système informatique, le périphérique fonctionne en mode continu. Ce procédé améliore considérablement les performances du périphérique et la gestion de l'espace de stockage.

DCBF

Système sur lequel s'exécute le protocole DHCP (Dynamic Host Configuration Protocol), permettant l'affectation dynamique des adresses IP et la configuration réseau pour les clients DHCP.

découverte des disques

Procédé de sauvegarde incrémentale consistant à ne sauvegarder que les modifications réalisées depuis la dernière sauvegarde complète. Pour réaliser ce type de sauvegarde, spécifiez le type de sauvegarde Incr1.
Voir aussi sauvegarde incrémentale.

demande de montage

(terme propre à Microsoft SQL Server) Sauvegarde de base de données au cours de laquelle ne sont sauvegardées que les modifications intervenues après la dernière sauvegarde complète de la base.
Voir aussi types de sauvegarde.

dépôt de fichier

Sauvegarde de base de données au cours de laquelle seules les modifications intervenues après la dernière sauvegarde complète de la base sont sauvegardées.

disque virtuel

Solution de sauvegarde SAN au sein de laquelle la transmission directe des données entre le disque et la bande (ou un autre périphérique de stockage secondaire) est facilitée par la commande SCSI Extended Copy (Xcopy). La sauvegarde directe permet de réduire le nombre d'E/S sur les systèmes dans un environnement SAN. La commande SCSI Extended Copy (XCopy) facilite la transmission directe des données entre le disque et la bande (ou un autre périphérique de stockage secondaire). Cette commande est fournie par un élément de l'infrastructure comprenant les ponts, les commutateurs, les bibliothèques de bandes et les sous-systèmes de disques.
Voir aussi moteur XCopy.

disques partagés

(terme propre à Windows) Les jonctions de répertoires utilisent le concept de point d'analyse de Windows. Une jonction de répertoire NTFS 5 permet à l'utilisateur de rediriger une requête de répertoire/fichier vers un autre emplacement.

DMZ

Processus permettant de restaurer le disque du système principal d'un client dans un état proche de celui dans lequel il se trouvait après une sauvegarde complète.

données sauvegardées publiques/privées

Composant devant être installé sur un client pour que ce dernier puisse être sauvegardé et restauré. L'Agent de disque contrôle la lecture et l'écriture de données sur un disque. Pendant une session de sauvegarde, l'Agent de disque lit les données stockées sur un disque et les envoie à l'Agent de support qui les déplace ensuite vers le périphérique. Pendant une session de restauration, l'Agent de disque reçoit des données de l'Agent de support et les écrit sur le disque.

données_ programme_ Data_Protector	Nombre d'Agents de disque autorisés à envoyer des données simultanément à un Agent de support.
DR OS	Détection des disques au cours de la sauvegarde d'un client avec découverte des disques. Lors de cette sauvegarde, Data Protector découvre (détecte) les disques présents sur le client (même s'ils ne l'étaient pas lors de la configuration de la sauvegarde) et les sauvegarde. Ce type de sauvegarde est très utile dans les environnements dynamiques où les configurations changent rapidement. Une fois les disques développés, chacun d'entre eux hérite de toutes les options de son objet client principal. Même des commandes de pré- ou post-exécution sont spécifiées une fois, elles sont lancées de nombreuses fois, une fois par objet.
droits d'accès	*(terme propre à Veritas Volume Manager)* Unité de base de stockage des données dans un système VxVM. Un groupe de disques peut être constitué d'un ou de plusieurs volumes physiques. Le système peut contenir plusieurs groupes de disques.
droits utilisateur	Sauvegarde ultra-rapide au cours de laquelle Data Protector sauvegarde les fichiers en tant qu'images bitmap. Ce type de sauvegarde (rawdisk) ne suit pas la structure des fichiers et des répertoires stockés sur le disque ; elle stocke la structure de l'image disque au niveau des octets. Vous pouvez effectuer une sauvegarde d'image disque de certaines sections du disque ou de sa totalité.
échangeur	Concept permettant de gérer l'utilisation de l'espace disque pour l'ensemble des utilisateurs ou pour certains d'entre eux sur un système informatique. Plusieurs plates-formes de système d'exploitation utilisent ce concept.
emplacement	Le processus de sauvegarde des données en plusieurs étapes permet d'améliorer les performances des sauvegardes et des restaurations, de réduire les coûts de stockage des données sauvegardées et d'améliorer la disponibilité et l'accessibilité des données pour restauration. Les étapes de sauvegarde consistent à sauvegarder d'abord les données sur un type de support (par exemple un disque) puis ultérieurement les copier sur un type de support différent (par exemple sur bande).
emplacement(s) de supports	Format de support, disponible avec la bibliothèque de fichiers, qui prend en charge une variante optimisée de la sauvegarde synthétique : la sauvegarde complète virtuelle. L'utilisation de ce format est un prérequis à la sauvegarde complète virtuelle.

Voir aussi sauvegarde complète virtuelle.

enregistrement circulaire

Service reliant les partages de fichiers dans un seul espace de noms. Ces partages peuvent résider sur le même ordinateur ou sur des ordinateurs différents. Le DFS permet à un client d'accéder aux ressources de manière transparente.

environnement de sauvegarde d'entreprise

La zone démilitarisée (DMZ) est un réseau inséré en tant que "zone neutre" entre le réseau privé d'une société (intranet) et le réseau public extérieur (Internet). Elle empêche les utilisateurs externes d'accéder directement aux serveurs de la société sur l'intranet de celle-ci.

espace de table

Dans le modèle client-serveur DNS, il s'agit du serveur contenant les informations relatives à une partie de la base de données DNS et rendant les noms des ordinateurs accessibles aux programmes de résolution client en faisant une demande de résolution de noms via Internet.

établissement (rétablissement) incrémental

Serveur d'un réseau responsable de la sécurité de l'utilisateur et de la vérification des mots de passe dans un groupe d'autres serveurs.

état de paire

Données requises pour l'installation et la configuration temporaires du système d'exploitation pour récupération après sinistre (DR OS).

état des supports

Un système d'exploitation de récupération après sinistre (DR OS) est un environnement de système d'exploitation permettant d'exécuter la récupération après sinistre. Il fournit à Data Protector un environnement d'exécution de base (accès au disque, au réseau, à la bande et au système de fichiers). Le système d'exploitation doit être installé et configuré pour que la récupération après sinistre Data Protector puisse être effectuée. Le système d'exploitation de récupération après sinistre héberge non seulement le processus de récupération après sinistre Data Protector, mais fait également partie du système restauré car il remplace ses propres données de configuration par les données de configuration d'origine.

Etat système

Unité physique recevant des données provenant d'un système informatique et capable de les écrire sur un support magnétique (généralement un lecteur de bande). Un lecteur peut également lire les données du support et les envoyer au système informatique.

étiquette de supports	Le cryptage sur lecteur Data Protector utilise la fonctionnalité de cryptage du lecteur. Au cours de la sauvegarde, le lecteur crypte les données et les métadonnées qui sont écrites sur le support.
exportation de supports	Numéro permettant d'identifier la position mécanique d'un lecteur au sein d'un périphérique de bibliothèque. Le contrôle robotique utilise ce numéro pour accéder à un lecteur.
facteurs d'état des supports	*Voir* sauvegarde client avec découverte des disques.
Fibre Channel	*Voir* Agent Symmetrix (SYMA).
fichier d'amorçage d'urgence	*(terme propre à Informix Server)* Le fichier de configuration Informix Server `ixbar.`*`id_serveur`* qui se trouve dans le répertoire *`INFORMIXDIR`*`/etc` (sous Windows) ou *`INFORMIXDIR`*`\etc` (sous UNIX). *`INFORMIXDIR`* est le répertoire de base d'Informix Server et *`ID_serveur`* la valeur du paramètre de configuration `SERVERNUM`. Chaque ligne du fichier d'amorçage d'urgence correspond à un objet sauvegarde.
fichier de contrôle	Une sauvegarde incrémentale classique inclut les fichiers modifiés depuis une sauvegarde précédente, mais présente certaines limites en matière de détection des modifications. Une sauvegarde incrémentale avancée détecte et sauvegarde de manière fiable les fichiers renommés et déplacés, ainsi que ceux dont les attributs ont été modifiés.
fichier de données	Plusieurs cellules peuvent être regroupées et gérées depuis une cellule centrale. L'environnement de sauvegarde d'entreprise comprend tous les clients répartis entre plusieurs cellules Data Protector, lesquelles sont gérées et administrées à partir d'une cellule centrale utilisant le concept Manager-of-Managers. *Voir aussi* MoM.
Fichier de récupération de l'IDB	Référentiel central de l'ensemble des notifications ayant trait à Data Protector. Par défaut, toutes les notifications sont envoyées au journal d'événements. Le journal d'événements n'est accessible qu'aux utilisateurs Data Protector appartenant au groupe `Admin` et à ceux qui disposent des droits d'utilisateur portant sur les `rapports et notifications`. Vous pouvez afficher ou supprimer l'ensemble des événements du journal.
Fichier des jours chômés	*(terme propre à Windows)* Fichiers dans lesquels Windows consigne tous les événements, tels que le démarrage ou l'arrêt des services et les connexions et déconnexions des utilisateurs.

Data Protector peut sauvegarder les journaux d'événements Windows dans le cadre de la sauvegarde de la configuration Windows.

fichier d'options globales

(terme propre à Microsoft Exchange Server) Service de Microsoft Exchange Server représentant les groupes de stockage répliqués au moyen de la technologie LCR (Local Continuous Replication) ou CCR (Cluster Continuous Replication).
Voir aussi Cluster Continuous Replication et Local Continuous Replication.

fichier DRS

Egalement appelé échangeur SCSI.
Voir aussi bibliothèque.

fichier épars

Processus consistant à supprimer de l'IDB (base de données interne) toutes les données relatives aux sessions de sauvegarde (comme les systèmes, objets et noms des fichiers) qui résident sur les supports. Les informations relatives aux supports et à leur relation par rapport à un pool sont également supprimées de la base de données IDB. Toutefois, les données enregistrées sur les supports restent inchangées.
Voir aussi importation de supports.

fichier sqlhosts

(terme propre à Microsoft Exchange Server) Technologie de base de données servant de système de stockage pour les échanges d'informations dans Microsoft Exchange Server.

fichier sst.conf

Transfert des données de cluster les plus importantes, également appelées groupe (Windows) ou package (Unix), d'un nœud de cluster à un autre. Un basculement peut se produire en raison de défaillances logicielles ou matérielles, ou d'opérations de maintenance au niveau du nœud primaire.

fichier st.conf

(terme propre à HP StorageWorks EVA) Opération qui renverse les rôles entre source et destination dans les configurations CA + BC EVA.
Voir aussi CA + BC EVA.

fichier TSANDS.CFG

Voir passerelle Fibre Channel.

fichiers de récupération

Norme ANSI pour l'interconnexion informatique à grande vitesse. Utilisant des câbles à fibre optique ou en cuivre, cette technologie permet la transmission bidirectionnelle ultra-rapide de fichiers de données volumineux, et peut être déployée entre des sites distants de plusieurs kilomètres. La technologie Fibre Channel relie les noeuds au moyen de trois

topologies physiques différentes : point à point, en boucle et par commutation.

fichiers journaux de transaction

Une passerelle ou multiplexeur Fibre Channel permet de réaliser une migration des périphériques SCSI parallèles existants, tels que les baies de disques RAID, les disques SSD et les bibliothèques de bandes vers un environnement Fibre Channel. Une interface Fibre Channel se trouve à une extrémité de la passerelle. Des ports SCSI parallèles se trouvent à l'autre extrémité. La passerelle ou multiplexeur permet de déplacer les paquets SCSI entre les périphériques Fibre Channel et SCSI parallèles.

fichiers journaux logiques

Fichier contenant les données d'une sauvegarde vers un périphérique de bibliothèque de fichiers.

flux de données

Périphérique résidant sur un disque et constitué de plusieurs emplacements utilisés pour le stockage de fichiers.

fnames.dat

Périphérique résidant sur un disque qui fonctionne comme une bibliothèque avec plusieurs supports et contient donc plusieurs fichiers appelés dépôts de fichier.

format de support de fichiers distribués

Service Windows dupliquant les stratégies de groupe et les scripts d'ouverture de session de la banque du contrôleur de domaine. Ce service duplique également les partages de système de fichiers distribués (DFS) entre des systèmes et permet à tout serveur d'effectuer une opération de réplication.

formatage

(terme propre à Windows) Processus consistant à parcourir un système de fichiers pour déterminer quels objets ont été créés, modifiés ou supprimés.

fournisseur de copie miroir

Un même fichier peut être sauvegardé plusieurs fois lors des sauvegardes complètes et incrémentales (si des modifications ont été apportées au fichier). Si le niveau de journalisation sélectionné pour la sauvegarde est TOUT, Data Protector conserve dans la base de données IDB une entrée pour le nom de fichier lui-même et une pour chaque version (date/heure) du fichier.

fournisseur HP StorageWorks SMI-S EVA

Organisation des fichiers sur un disque dur. Un système de fichiers est enregistré pour que les attributs et le contenu des fichiers soient stockés sur le support de sauvegarde.

fusion

(terme propre à HP StorageWorks Disk Array XP) HP StorageWorks Disk Array XP peut comporter jusqu'à trois copies miroir d'un volume principal, chacune d'entre elles pouvant également posséder deux copies supplémentaires. Les trois copies miroir sont appelées miroirs de premier niveau.

Voir aussi volume principal et numéro de MU.

génération de sauvegarde	*(terme propre à Oracle)* La zone de récupération flash est un groupe de disques de gestion de stockage automatique, de système de fichiers ou de répertoires gérés Oracle 10g/11g qui sert de zone de stockage centralisé pour des fichiers liés à la sauvegarde et la restauration (fichiers de récupération). *Voir aussi* fichiers de récupération.
Gestionnaire de cellule	*Voir* droits utilisateur.
gestion centralisée des licences	Les fichiers `fnames.dat` de la base de données IDB contiennent des informations sur les noms des fichiers sauvegardés. Ces fichiers occupent généralement 20 % environ de la base de données IDB si des noms de fichiers sont stockés.
Gestion de stockage automatique	Processus consistant à effacer toutes les données contenues sur un support et à préparer ce dernier pour l'utiliser avec Data Protector. Les informations relatives au support (ID du support, description et emplacement) sont enregistrées dans la base IDB ainsi que sur les supports concernés (en en-tête de ces derniers). Les supports Data Protector comportant des données protégées ne sont pas formatés tant que la protection n'a pas expiré ou que la protection du support n'est pas retirée ou le support recyclé.
Gestion de stockage hiérarchique (HSM, pour Hierarchical Storage Management)	Source auxiliaire de supports utilisée par les pools n'ayant plus aucun support disponible. Les pools de supports doivent être configurés pour l'utilisation de pools libres.
Gestionnaire de récupération (RMAN)	Sauvegarde au cours de laquelle tous les objets sélectionnés sont sauvegardés, qu'ils aient été ou non modifiés récemment. *Voir aussi* types de sauvegarde.
Gestionnaire RAID XP	Sauvegarde de toutes les données d'une base de données, non limitée aux seules données modifiées après la dernière sauvegarde (complète ou incrémentale) de la base de données. Une sauvegarde de base de données complète ne dépend d'aucune autre sauvegarde.
groupe	Sauvegarde de tout le contenu d'une boîte aux lettres.
groupe de disques	Session de sauvegarde ZDB sur bande ou ZDB sur disque + bande au cours de laquelle tous les objets sélectionnés sont

copiés sur la bande, même si aucune modification n'a eu lieu depuis la dernière sauvegarde.
Voir aussi sauvegarde ZDB incrémentale.

groupe de périphériques

Fichier permettant à l'utilisateur de personnaliser Data Protector. Ce fichier fournit des informations sur les options globales, lesquelles concernent différents aspects de Data Protector, généralement les délais d'attente et les limites, et affectent la cellule Data Protector entière. Le fichier est situé sur le Gestionnaire de cellule, dans le répertoire *donnes_programme_Data_Protector*`\Config\Server\Options` (Windows Server 2008), *répertoire_Data_Protector*`\Config\Server\Options` (autres systèmes Windows) ou `/etc/opt/omni/server/options` (systèmes HP-UX ou Solaris).

groupe de réplication de données

(terme propre à Microsoft Cluster Server) Ensemble de ressources (par exemple, volumes de disque, services d'applications, noms et adresses IP) nécessaires à l'exécution d'applications compatibles cluster spécifiques.

groupe de stockage

Interface utilisateur graphique fournie par Data Protector pour faciliter l'accès à l'ensemble des tâches de configuration, d'administration et d'utilisation. En plus de son interface utilisateur graphique d'origine sous Windows, Data Protector fournit également une interface Java d'apparence et de fonctionnalités similaires pour bon nombre d'autres plates-formes.

groupe de volumes

(terme propre à Microsoft Exchange Server) Récupération de base de données Microsoft Exchange Server qui est effectuée après une restauration par le moteur de base de données, à l'aide de fichiers journaux de transactions.

groupe d'utilisateurs

Jeu de données de cluster comportant un horodatage, destiné à fournir des informations sur le statut opérationnel d'un noeud de cluster spécifique. Cet ensemble de données est distribué à tous les nœuds de cluster.

HP ITO

Méthode visant à optimiser l'utilisation de l'espace disque pour le stockage des données et consistant à faire migrer les données les moins souvent utilisées vers des disques optiques moins coûteux. Lorsque cela est nécessaire, les données migrent de nouveau sur le disque dur. Cette méthode permet de trouver un équilibre entre le besoin d'extraire rapidement les données du disque dur et l'utilisation de disques optiques moins coûteux.

HP ITO

Fichier contenant des informations sur les jours chômés. Vous pouvez définir des jours chômés différents en modifiant

le fichier Jours chômés sur le Gestionnaire de cellule, dans le répertoire *donnes_programme_Data_Protector*\Config\Server\holidays (Windows Server 2008), *répertoire_Data_Protector*\Config\Server\holidays (autres systèmes Windows ou /etc/opt/omni/server/Holidays (systèmes UNIX).

HP OM — *Voir* sauvegarde de client avec découverte de disques.

HP Operation Manager SMART Plug-In (SPI) — Client Data Protector actif utilisé pour la récupération après sinistre avec restitution de disque, sur lequel est installé un Agent de disque Data Protector.

HP StorageWorks Disk Array XP LDEV — *Voir* OM.

HP VPO — *Voir* OM.

ICDA — Solution prête à l'emploi et entièrement intégrée constituant un complément du logiciel HP Operations Manager et permettant d'étendre le domaine géré. Grâce à l'intégration Data Protector, mise en oeuvre sous la forme d'un module HP Operations Manager SMART Plug-In, un utilisateur peut mettre en place la surveillance d'un nombre arbitraire de Gestionnaires de cellule Data Protector en tant qu'extension du logiciel HP Operations Manager (OM).

ID de connexion — *Voir* OM

ID de sauvegarde — Partition logique d'un disque physique dans une baie de disques HP StorageWorks Disk Array XP. Les LDEV sont des entités qui peuvent être dupliquées dans les configurations Continuous Access XP (CA) et Business Copy XP (BC) ou bien utilisées en tant qu'entités autonomes.
Voir aussi BC, CA *(terme propre à HP StorageWorks Disk Array XP)*, et réplique.

ID de session — Logiciel de Data Protector qui exécute toutes les tâches nécessaires à l'intégration de HP StorageWorks Enterprise Virtual Array. Avec l'Agent SMI-S EVA, le contrôle sur la baie est assuré par le fournisseur HP StorageWorks SMI-S EVA qui dirige la communication entre les demandes entrantes et CV EVA.
Voir aussi Command View (CV) EVA et fournisseur HP StorageWorks SMI-S EVA.

ID de support — Interface permettant de contrôler HP StorageWorks Enterprise Virtual Array. Le fournisseur SMI-S EVA s'exécute en tant

que service distinct sur le système de gestion du stockage HP et agit comme passerelle entre les requêtes entrantes et Command View EVA. Avec l'intégration de Data Protector HP StorageWorks EVA, le fournisseur SMI-S EVA accepte les requêtes standardisées de l'Agent SMI-S EVA, communique avec Command View EVA pour l'appel d'informations ou de méthodes et renvoie des réponses standardisées.
Voir aussi Agent SMI-S HP StorageWorks EVA et Command View (CV) EVA.

ID d'objet

Partition logique d'un disque physique dans une baie de disques HP StorageWorks Virtual Array. Les LUN sont des entités qui peuvent être répliquées dans la configuration Business Copy VA de HP StorageWorks ou qui peuvent être utilisées comme des entités autonomes.
Voir aussi BC VA et réplique.

IDB (Base de données interne)

Voir OM.

image DR

(terme propre à EMC Symmetrix) ICDA (Integrated Cached Disk Arrays) d'EMC est un périphérique à baie de disques combinant un ensemble de disques physiques, un certain nombre de canaux FWD SCSI, une mémoire cache interne et un logiciel de contrôle et de diagnostic communément appelé "microcode".

importation de supports

La base de données interne de Data Protector, située sur le Gestionnaire de cellule, permet d'identifier les données sauvegardées, le type de support utilisé, la façon dont les sessions de sauvegarde et de restauration doivent se dérouler , ainsi que les périphériques et bibliothèques configurés.

index de lecteur

Fichier de l'IDB (obrindex.dat) contenant des informations sur les sauvegardes IDB, les périphériques et les supports utilisés pour la sauvegarde. Ces données peuvent simplifier considérablement la récupération de la base de données IDB. Il est recommandé de déplacer le fichier, ainsi que les journaux de transactions de la base de données interne, sur un disque physique distinct des autres répertoires de la base, ainsi que de faire une copie du fichier.

Inet

Processus consistant à relire dans l'IDB (base de données interne) l'ensemble des données relatives aux sessions de sauvegarde qui se trouvent sur le support. Ceci permet ensuite à l'utilisateur d'accéder rapidement et facilement aux données stockées sur les supports.
Voir aussi exportation de supports.

Informations d'audit	Procédé consistant à ne sauvegarder que les fichiers auxquels des modifications ont été apportées depuis la dernière sauvegarde. Plusieurs niveaux de sauvegarde incrémentale sont disponibles, ce qui permet de contrôler en détail la longueur de la chaîne de restauration. *Voir aussi* types de sauvegarde.
informations de connexion à la base de données catalogue de récupération	*(terme propre à Microsoft Exchange Server)* Sauvegarde des données Microsoft Exchange Server qui ont été modifiées depuis la dernière sauvegarde complète ou incrémentale. Avec la sauvegarde incrémentale, seuls les fichiers de journal des transactions sont sauvegardés. *Voir aussi* types de sauvegarde.
informations de connexion à la base de données cible Oracle	Une sauvegarde incrémentale de boîte aux lettres consiste à sauvegarder toutes les modifications apportées à la boîte aux lettres depuis la dernière sauvegarde, quel qu'en soit le type.
initialisation	Une sauvegarde incrémentale1 de boîte aux lettres consiste à sauvegarder toutes les modifications apportées à la boîte aux lettres depuis la dernière sauvegarde complète.
instance Oracle	*(terme propre à EMC Symmetrix)* Opération de contrôle BCV ou SRDF. Dans les opérations de contrôle BCV, un établissement incrémental entraîne la synchronisation incrémentale du périphérique BCV et son fonctionnement en tant que support en miroir EMC Symmetrix. Des paires doivent avoir été préalablement définies entre les périphériques EMC Symmetrix. Dans les opérations de contrôle SRDF, un établissement incrémental entraîne la synchronisation incrémentale du périphérique (R2) cible et son fonctionnement en tant que support en miroir EMC Symmetrix. Des paires doivent avoir été préalablement définies entre les périphériques EMC Symmetrix.
instanciation unique	*(terme propre à EMC Symmetrix)* Opération de contrôle BCV ou SRDF. Dans les opérations de contrôle BCV, une restauration incrémentale réaffecte un périphérique BCV comme miroir disponible suivant du périphérique standard de la paire. Cependant, les périphériques standard sont mis à jour uniquement avec les données écrites sur le périphérique BCV au cours de la séparation des paires d'origine ; les données écrites sur le périphérique standard au cours de la séparation sont écrasées par les données du miroir BCV. Dans les opérations de contrôle SRDF, une restauration incrémentale réaffecte un périphérique (R2) cible comme miroir disponible suivant du périphérique (R1) source de la paire. Cependant, les périphériques (R1) sources sont mis à jour uniquement avec les données écrites sur le périphérique (R2) cible au cours de

la séparation des paires d'origine ; les données écrites sur le périphérique (R1) source au cours de la séparation sont écrasées par les données du miroir (R2) cible.

interface de ligne de commande (CLI)

Session de sauvegarde de système de fichiers ZDB (avec temps d'indisponibilité nul) sur bande ou sur disque + bande qui ne copie sur le support que les modifications effectuées depuis la dernière sauvegarde protégée (complète ou incrémentale). *Voir aussi* sauvegarde ZDB complète.

interface de périphérique virtuel

Processus s'exécutant sur chaque système UNIX ou service s'exécutant sur chaque système Windows dans la cellule Data Protector. Il est responsable de la communication entre les systèmes de la cellule et du lancement des processus requis pour la sauvegarde et la restauration. Le service Inet est lancé dès que Data Protector est installé sur un système. Le processus Inet est démarré par le démon inetd.

Interface utilisateur graphique (GUI)

(terme propre à Microsoft Exchange Server) Service de Microsoft Exchange Server chargé de la gestion du stockage. La banque d'informations de Microsoft Exchange Server gère deux types de banques : les boîtes aux lettres et les dossiers publics. Une banque de boîtes aux lettres est constituée de boîtes aux lettres appartenant à des utilisateurs individuels. Une banque d'informations publiques contient des dossiers et des messages publics partagés entre plusieurs utilisateurs. *Voir aussi* service Gestionnaire de clés et service de réplication de sites.

interface XBSA

(terme propre à Informix Server) Ce terme désigne la solution Informix Dynamic Server.

Internet Information Services (IIS)

Voir formatage.

ISQL

Système informatique contenant un référentiel des packages logiciels Data Protector pour une architecture spécifique. Le Serveur d'installation permet l'installation à distance des clients Data Protector. Dans les environnements mixtes, deux serveurs d'installation au moins sont nécessaires : un pour les systèmes UNIX et un pour les systèmes Windows.

ITO

(terme propre à la sauvegarde ZDB) Processus qui utilise une réplique, générée par une session ZDB sur disque ou ZDB sur disque + bande, pour restaurer le contenu des volumes sources dans l'état dans lequel ils étaient au moment de la création de la réplique. Cela évite d'avoir à exécuter une restauration à partir d'une bande.. Suivant l'application/la

base de données concernée, cela peut suffire. Dans d'autres cas, des étapes supplémentaires peuvent être requises en vue d'une récupération complète, l'application de journaux de transaction par exemple.
Voir aussi réplique, sauvegarde avec temps d'indisponibilité nul (ZDB), sauvegarde ZDB sur disque et sauvegarde ZDB sur disque+bande.

Jeu ASR — Objet sauvegarde d'une intégration de Data Protector, telle que Oracle ou SAP DB.

jeu de copies — *(terme propre à Windows)* Microsoft Internet Information Services est un serveur d'applications et de fichiers réseau qui prend en charge de nombreux protocoles. La fonction principale d'IIS consiste à transmettre les informations des pages HTML (Hypertext Markup Language) à l'aide du protocole HTTP (Hypertext Transport Protocol).

jeu de copies miroir — L'adresse IP (Internet Protocol) correspond à l'adresse numérique d'un système et permet de l'identifier de manière unique sur le réseau. L'adresse IP est constituée de quatre groupes de chiffres séparés par des points.

jeu de répliques — *(terme propre à Sybase)* Utilitaire Sybase utilisé pour exécuter des tâches d'administration système sur Sybase SQL Server.

jeu de sauvegarde — *Voir* OM.

jeu de sauvegarde — Le client de l'interface Java est un composant de l'interface utilisateur graphique Java qui contient uniquement les fonctionnalités liées à l'interface utilisateur et qui doit être relié au serveur de l'interface Java pour fonctionner.

jeu de supports — Le serveur de l'interface Java est un composant de l'interface utilisateur graphique Java qui est installé sur le système Gestionnaire de cellule Data Protector. Le serveur de l'interface Java reçoit des requêtes du client de l'interface Java, les traite et renvoie les réponses au client de l'interface Java. Les données sont échangées via le protocole HTTP (Hypertext Transfer Protocol) sur le port 5556.

jonction de répertoire — *Voir* bibliothèque.

journal de rétablissement — Périphérique constitué de plusieurs emplacements utilisés pour le stockage de bandes magnéto-optiques ou de fichiers. Lorsqu'il est utilisé pour le stockage de fichiers, le périphérique de bibliothèque de stockage est appelé "périphérique de bibliothèque de stockage de fichiers".

journal de rétablissement archivé

Outil évitant d'avoir à fournir manuellement une phrase passe pour décrypter la clé privée. Vous devez l'installer et le configurer sur le Serveur d'installation si vous exécutez une installation à distance via un shell sécurisé.

journal de rétablissement en ligne

(terme propre à Microsoft Exchange Server) Service Microsoft Exchange Server qui fournit une fonction de cryptage pour une meilleure sécurité.
Voir aussi banque d'informations et service de réplication de sites.

journal de rétablissement hors ligne

Le serveur gestionnaire de clé (KMS - Key Management Server) est un service centralisé qui s'exécute sur le Gestionnaire de cellule et assure la gestion des clés pour la fonctionnalité de cryptage Data Protector. Ce service démarre dès que Data Protector est installé sur le Gestionnaire de cellule.

Journal des modifications

Toutes les clés de cryptage sont stockées de manière centralisée dans la banque de clés sur le Gestionnaire de cellule et sont gérées par le serveur gestionnaire de clés (KMS).

journal d'événements (Journal d'événements Data Protector)

(terme propre à EMC Symmetrix) Un objet sauvegarde logique (LBO, pour Logical Backup Object) est un objet de stockage/récupération de données dans l'environnement EMC Symmetrix. Il est stocké/récupéré par EMC Symmetrix comme une entité unique et ne peut être restauré que dans son intégralité.

Journaux d'audit

Egalement appelée "changeur automatique", "bibliothèque de bandes magnéto-optiques", "chargeur automatique" ou "échangeur". Une bibliothèque contient des supports stockés dans des emplacements de référentiel. Chaque emplacement contient un support (par exemple, DDS/DAT). Les supports sont déplacés entre les emplacements et les lecteurs par un mécanisme robotique permettant un accès aléatoire aux supports. Une bibliothèque peut contenir plusieurs lecteurs.

journaux de transactions

ou opération sans surveillance Sauvegarde ou restauration ayant lieu en dehors des heures de fonctionnement normales, ce qui signifie qu'aucun opérateur n'est présent pour utiliser l'application de sauvegarde ou les demandes de montage de service, par exemple.

journaux d'événements

(terme propre à Oracle) Fichier de configuration Oracle décrivant un ou plusieurs listeners TNS (Transparent Network Substrate) sur un serveur.

keychain

Par défaut, Data Protector équilibre automatiquement l'utilisation des périphériques sélectionnés pour la sauvegarde,

de manière à ce qu'ils soient exploités de façon égale. Ce procédé permet d'optimiser l'utilisation des périphériques en équilibrant le nombre d'objets écrits sur chacun. Cette opération s'effectuant automatiquement pendant la sauvegarde, l'utilisateur n'a pas besoin de gérer la sauvegarde des données ; il lui suffit de spécifier les périphériques à utiliser. Si vous ne souhaitez pas utiliser le partage de charge, vous pouvez sélectionner le périphérique à utiliser avec chaque objet dans le spécification de sauvegarde. Data Protector accèdera aux périphériques dans l'ordre spécifié.

KMS

La récupération à distance peut être exécutée si tous les hôtes d'Agents de support spécifiés dans le fichier DRS sont accessibles. Si l'un d'entre eux échoue, le processus de récupération après sinistre bascule du mode distant au mode local. Dans ce cas, une recherche est exécutée sur les périphériques connectés en local au système cible. Si la recherche ne renvoie qu'un seul périphérique, celui-ci sera automatiquement utilisé. Dans le cas contraire, Data Protector vous invitera à sélectionner le périphérique à utiliser pour la restauration.

LBO

(terme propre à Microsoft Exchange Server) Local Continuous Replication (LCR ou réplication continue locale) est une solution sur serveur unique qui crée et conserve une copie exacte (copie LCR) d'un groupe de stockage. Une copie LCR réside sur le même serveur que le groupe de stockage d'origine. Suite à sa création, une copie LCR est maintenue à jour par le biais de la technologie de propagation des modifications (réexécution des journaux). La fonction de réplication de LCR garantit que les journaux qui n'ont pas été répliqués ne sont pas supprimés. En conséquence de ce fonctionnement, l'exécution de sauvegardes dans un mode qui supprime les journaux risque de ne pas libérer d'espace si la réplication est suffisamment loin derrière en matière de copie des journaux.
Les copies LCR servent à des fins de récupération après sinistre, puisqu'il est possible de basculer sur la copie LCR en quelques secondes. Si une copie LCR servant à la sauvegarde est située sur un disque différent de celui des données d'origine, la charge des E/S sur une base de données de production s'avère alors minimale.
Un groupe de stockage répliqué est représenté comme une nouvelle instance du module d'écriture Exchange nommé Service de réplication Exchange et peut être sauvegardé (à l'aide de VSS) comme n'importe quel groupe de stockage.
Voir aussi Cluster Continuous Replication et Service de réplication Exchange.

lecteur

Vous pouvez configurer plusieurs fois un même périphérique physique avec des caractéristiques différentes en utilisant des noms de périphérique différents. Le nom de verrouillage est une chaîne spécifiée par l'utilisateur servant à verrouiller toute configuration de périphérique de ce type afin d'empêcher un conflit si plusieurs de ces périphériques (noms de périphériques) sont utilisés simultanément. Utilisez un nom de verrouillage identique pour toutes les définitions de périphérique s'appuyant sur le même périphérique physique.

liste de préallocation

(terme propre à Informix Server UNIX) Script fourni par ON-Bar et que l'utilisateur peut utiliser pour lancer la sauvegarde des fichiers journaux logiques lorsque Informix Server émet une alarme de saturation de journal. Le paramètre de configuration `ALARMPROGRAM` Informix Server sélectionné par défaut est *`REP_INFORMIX`*`/etc/log_full.sh`, où *`REP_INFORMIX`* est le répertoire de base d'Informix Server. Si vous ne souhaitez pas que les journaux logiques soient sauvegardés en continu, attribuez la valeur *`INFORMIXDIR`*`/etc/no_log.sh` au paramètre de configuration `ALARMPROGRAM`.

LISTENER.ORA

Le niveau de journalisation détermine la quantité de détails sur les fichiers et répertoires enregistrés dans l'IDB (base de données interne) pendant la sauvegarde, la copie d'objets ou la consolidation d'objet. Vous pouvez toujours restaurer vos données, sans tenir compte du niveau de journalisation utilisé pendant la sauvegarde. Data Protector propose quatre niveaux de journalisation : Journaliser tout, Journaliser répertoires, Journaliser fichiers, Pas de journalisation. Les différents paramètres de niveau de journalisation influencent la croissance de la base de données IDB, la vitesse de sauvegarde et la facilité d'exploration des données à restaurer.

Local Continuous Replication

Concerne la sauvegarde de base de données en ligne. Les fichiers journaux logiques sont des fichiers dans lesquels les données modifiées sont stockées avant d'être transférées au disque. En cas de panne, les fichiers journaux logiques permettent de repositionner toutes les transactions qui ont été transférées et d'annuler toutes celles qui ne l'ont pas encore été.

LUN HP StorageWorks Virtual Array

(terme propre à Microsoft SQL Server) Nom sous lequel un utilisateur se connecte à Microsoft SQL Server. Pour qu'un ID de connexion soit reconnu, une entrée doit avoir été créée pour l'utilisateur associé dans la table système syslogin de Microsoft SQL Server.

LVM

(terme propre à Oracle et SAP R/3) Le format des informations de connexion est le suivant : `nom_utilisateur/mot de passe@service`, où :

- `nom_utilisateur` est le nom sous lequel un utilisateur est reconnu par le serveur Oracle et par les autres utilisateurs. Chaque nom d'utilisateur est associé à un mot de passe ; l'utilisateur doit les entrer tous les deux pour pouvoir se connecter à une base de données cible Oracle. Il doit également disposer de droits SYSDBA ou SYSOPER Oracle.
- `mot de passe` doit correspondre à celui figurant dans le fichier de mots de passe Oracle (`orapwd`) ; ce fichier permet d'authentifier les utilisateurs chargés de l'administration de la base de données.
- `service`est le nom servant à identifier un processus du serveur SQL*Net pour la base de données cible.

make_net_recovery

(terme propre à Oracle) Le format des informations de connexion à la base de données du catalogue de récupération (Oracle) est le suivant :`nom_utilisateur/mot_de_passe@service`, où la description du nom d'utilisateur, du mot de passe et du nom du service est la même que celle qui figure dans les informations de connexion SQL*Net V2 à la base de données cible Oracle. Dans ce cas, le `service` correspond au nom du service de la base de données catalogue de récupération et non à la base de données cible Oracle.
Notez que l'utilisateur Oracle spécifié doit être le propriétaire du catalogue de récupération Oracle.

make_tape_ recovery

(terme propre à Lotus Domino Server) Interface destinée à l'échange de données de sauvegarde et de récupération entre Lotus Domino Server et une solution de sauvegarde comme Data Protector.

Manager-of-Managers(MoM)

Un LVM (Logical Volume Manager), ou gestionnaire de volume logique, est un sous-système permettant de structurer l'espace disque physique et de le mettre en correspondance avec les volumes logiques sur les systèmes UNIX. Un système LVM est constitué de plusieurs groupes de volumes, comportant chacun plusieurs volumes.

MAPI

Voir Wake ONLAN.

MCU

(terme propre à Microsoft Exchange Server) Emplacement où sont livrés les messages électroniques. Cet emplacement est défini par l'administrateur pour chaque utilisateur. Si un ensemble de dossiers personnels est désigné comme emplacement de distribution du courrier électronique, les

messages sont acheminés de la boîte aux lettres vers cet emplacement.

Microsoft Exchange Server

(terme propre à Microsoft Exchange Server) Partie de la banque d'informations conservant les informations se trouvant dans les boîtes aux lettres des utilisateurs. Une banque de boîtes aux lettres est constituée d'un fichier binaire RTF `.edb` et d'un fichier de contenu Internet natif continu `.stm`.

Microsoft Management Console (MMC)

(terme propre à HP StorageWorks Disk Array XP) Baie de disques HP StorageWorks XP contenant les volumes principaux pour les configurations CA et BC et agissant comme périphérique maître.
Voir aussi BC (terme propre à HP StorageWorks Disk Array XP), CA *(terme spécifique à HP StorageWorks Disk Array XP)*, et HP StorageWorks Disk Array XP LDEV.

Microsoft SQL Server

Voir MoM.

Microsoft Volume Shadow Copy Service (VSS)

`make_net_recovery` est une commande Ignite-UX qui permet de créer des archives de récupération via le réseau sur le serveur Ignite-UX ou tout autre système spécifié. Le système cible peut être récupéré via les sous-réseaux après démarrage à l'aide d'une bande amorçable créée par la commande Ignite-UX `make_boot_tape` ou lorsque le système démarre directement à partir du serveur Ignite-UX. Vous pouvez automatiser le démarrage direct à partir du serveur Ignite-UX au moyen de la commande Ignite-UX `bootsys` ou le spécifier en mode interactif sur la console d'amorçage.

miroir de premier niveau

`make_tape_recovery` est une commande Ignite-UX qui permet de créer une bande (d'installation) de récupération amorçable adaptée au système et de mettre en oeuvre la récupération après sinistre sans surveillance en connectant le périphérique de sauvegarde directement au système cible et en démarrant le système cible à partir de la bande de récupération amorçable. Le périphérique de sauvegarde doit être connecté au client en local durant la création des archives et la récupération du client.

miroir d'objet

(terme propre à Microsoft Exchange server) L'interface MAPI (Messaging Application Programming Interface) est l'interface de programmation qui permet aux applications et aux clients de messagerie communiquer avec les systèmes de messagerie et d'information.

miroir *(terme propre à EMC Symmetrix et HP StorageWorks Disk Array XP)*	*Voir* Unité de commande principale (MCU, pour Main Control Unit).
mise au coffre des supports	Processus contrôlant la lecture et l'écriture de données sur un périphérique qui lui-même lit ou écrit des données sur un support (généralement une bande). Pendant une session de sauvegarde, un Agent de support reçoit des données de l'Agent de disque et les envoie au périphérique qui les écrit ensuite sur le support. Pendant une session de restauration, un Agent de support localise les données stockées sur le support de sauvegarde et les envoie à l'Agent de disque qui les écrit ensuite sur le disque. Un Agent de support gère également le contrôle robotique d'une bibliothèque.
mise en miroir d'objet	Procédé permettant de déterminer l'ordre d'utilisation des supports pour la sauvegarde. Dans le cas d'une stratégie d'allocation stricte, Data Protector demande un support spécifique. Dans le cas d'une stratégie souple, Data Protector demande tout support approprié. Dans le cas d'une stratégie de priorité aux supports formatés, Data Protector préfère utiliser les supports inconnus, même si des supports non protégés sont disponibles dans la bibliothèque.
MMD	Qualité des supports telle qu'elle est reflétée par les facteurs d'état des supports. Plus l'âge et l'utilisation faite des supports sont importants, plus les risques d'erreurs de lecture et d'écriture sont élevés sur les supports à bande. Un support doit être remplacé lorsque son état est MEDIOCRE.
MMDB	Limites d'âge et de réécriture définies par l'utilisateur pour déterminer l'état d'un support.
mode compatible VSS	Identificateur unique attribué à un support par Data Protector.
mode resynchronisation	Identificateur défini par l'utilisateur et servant à décrire un support.
module d'écriture	Emplacement physique d'un support défini par l'utilisateur, par exemple, "bâtiment 4" ou "stockage hors-site".
Module fournisseur d'informations sur les modifications	Session servant à exécuter une action sur un support, telle que l'initialisation, l'analyse du contenu, la vérification des données stockées sur le support, ou la copie de ce dernier.

MoM	Ensemble de supports du même type (DDS par exemple) utilisé et suivi comme un groupe. Les supports sont formatés et affectés à un pool de supports.
moteur de stockage extensible (ESE, pour Extensible Storage Engine)	Une session de sauvegarde a pour résultat le stockage de données sur un groupe de supports appelé "jeu de supports". Selon la stratégie d'utilisation des supports, plusieurs sessions peuvent se partager les mêmes supports.
moteur XCopy	Type physique d'un support, comme DDS ou DLT.
MSM	La stratégie d'utilisation des supports permet de contrôler la manière dont les nouvelles sauvegardes sont ajoutées aux supports déjà utilisés. Ses options sont les suivantes : `Ajout possible`, `Sans possibilité d'ajout` et `Ajout possible aux incrémentales uniquement`.
niveau de journalisation	La fusion correspond à un mode de résolution des conflits de fichiers au cours d'une restauration. Si le fichier à restaurer se trouve déjà à l'emplacement de destination, c'est celui dont la date de modification est la plus récente qui est conservé. Les fichiers qui ne sont pas présents sur le disque sont toujours restaurés. *Voir aussi* réécriture.
nom de verrouillage	Système de messagerie "client-serveur" et de groupes de travail fournissant une connexion transparente à de nombreux systèmes de communication différents. Il offre aux utilisateurs un système de messagerie électronique, une solution de planification de groupe et individuelle, des formulaires en ligne et des outils d'automatisation du flux de travail. Il fournit également au développeur une plate-forme sur laquelle il peut élaborer des applications personnalisées de partage d'informations et de service de messagerie.
Numéro de MU	*(terme propre à Windows)* Modèle d'administration pour environnements Windows. Cette console met à votre disposition une interface utilisateur d'administration simple, cohérente et intégrée permettant de gérer de nombreuses applications à partir d'une seule et même interface, à condition toutefois que les applications soient compatibles avec le modèle MMC.
obdrindex.dat	Système de gestion de base de données conçu pour répondre aux besoins du traitement distribué "client-serveur".
objet	Service logiciel offrant une interface de communication unifiée destinée à coordonner la sauvegarde et la restauration d'une application VSS, quelles que soient les fonctions de

cette dernière. Ce service collabore avec l'application de sauvegarde, les modules d'écriture, fournisseurs de copies miroir et le noyau du système d'exploitation pour mettre en oeuvre la gestion des copies miroir des volumes et des jeux de copies miroir.
Voir aussi copie miroir, fournisseur de copie miroir, réplique et module d'écriture.

objet de sauvegarde — *Voir* volume cible.

objet d'intégration — *Voir* rotation de jeux de répliques.

OM — Le processus (service) MMD (Media Management Daemon), démon de gestion des supports, s'exécute sur le Gestionnaire de cellule Data Protector et contrôle les opérations des périphériques et la gestion des supports. Le processus démarre dès que Data Protector est installé sur le Gestionnaire de cellule.

On-Bar — La base de données de gestion des supports (MMDB) fait partie de la base de données IDB, laquelle contient les informations concernant les supports, les pools de supports, les périphériques, les bibliothèques, les lecteurs de bibliothèques et les emplacements configurés dans la cellule, ainsi que les supports Data Protector utilisés pour la sauvegarde. Dans un environnement de sauvegarde d'entreprise, cette partie de la base de données peut être commune à toutes les cellules.
Voir aussi CMMDB, CDB.

ONCONFIG — Plusieurs cellules peuvent être regroupées et gérées depuis une cellule centrale. Le système de gestion de la cellule centrale est le Manager-of-Managers (MoM). Les cellules sont appelées clients MoM. Vous pouvez ainsi configurer et gérer plusieurs cellules à partir d'un point central.

OpC — Message apparaissant à l'écran et invitant l'utilisateur à insérer un support spécifique dans un périphérique. Lorsque vous avez répondu à la demande de montage en fournissant le support requis et en confirmant, la session se poursuit.

OpenSSH — Point d'accès à un disque ou à un volume logique dans une structure de répertoires, par exemple `/opt` ou `d:`. Sous UNIX, les points de montage sont accessibles au moyen de la commande `bdf` ou `df`.

Opérateurs booléens — Le Gestionnaire de session de supports (MSM, pour Media Session Manager) de Data Protector s'exécute sur le Gestionnaire de cellule et régit les sessions de supports, telles que la copie de supports.

opération hors contrôle	*(terme propre à HP StorageWorks Disk Array XP)* Numéro d'unité miroir. Nombre entier (0, 1 ou 2) servant à indiquer un miroir de premier niveau. *Voir aussi* miroir de premier niveau.
opération sans surveillance	Licence permettant à l'utilisateur d'exécuter un nombre illimité d'Agents de support sur un même système. Cette licence, liée à l'adresse IP du Gestionnaire de cellule, n'est plus disponible.
Oracle Data Guard	*Voir* fichier de récupération de l'IDB.
ORACLE_SID	Périphérique pouvant émuler un lecteur de CD-ROM. Chargé à l'aide d'un disque amorçable, il peut être utilisé en tant que périphérique de sauvegarde ou d'amorçage dans le cadre de la récupération après sinistre.
P1S file	*Voir* objet sauvegarde.
package	Processus consistant à fusionner une chaîne de restauration d'un objet sauvegarde, constituée d'une sauvegarde complète et d'au moins une sauvegarde incrémentale, en une nouvelle version consolidée de cet objet. Ce processus fait partie de la procédure de sauvegarde synthétique. Le résultat est une sauvegarde complète synthétique de l'objet sauvegarde spécifié.
Paquet magique	Processus consistant à fusionner une chaîne de restauration d'un objet sauvegarde, constituée d'une sauvegarde complète et d'au moins une sauvegarde incrémentale, en une nouvelle version consolidée de cet objet.
parallélisme	Copie d'une version spécifique d'un objet créée au cours d'une session de copie ou de sauvegarde avec la fonction de mise en miroir d'objets.
parallélisme de bases de données	Un processus qui crée une copie supplémentaire des données sauvegardées sur un jeu de supports. Pendant une session de copie d'objet, les objets sauvegardés sélectionnés sont copiés à partir de la source vers le support cible.
parcours de l'arborescence de fichiers	Processus de copie de versions d'objet sélectionnées sur un jeu de supports spécifique. Vous pouvez sélectionner pour la copie des versions d'objet d'une ou de plusieurs sessions de sauvegarde.
partage de charge	*(terme propre à Windows)* Les ID d'objet (OID) permettent d'accéder aux fichiers NTFS 5, quel que soit l'emplacement de ces derniers au sein du système. Data Protector considère les OID comme des flux de fichiers.

passage

Copie d'un objet sauvegarde créée via une mise en miroir de cet objet. Les miroirs d'objet sont souvent appelés copies d'objet.

passerelle FC

Processus consistant à écrire les mêmes données sur plusieurs jeux de supports au cours d'une session de sauvegarde. Data Protector vous permet de mettre en miroir tous les objets sauvegarde ou certains seulement sur un ou plusieurs jeux de supports.

passerelle Fibre Channel

Sauvegarde au cours de laquelle la base de données d'une application ne peut pas être utilisée par l'application.

- Pour les méthodes de sauvegarde simples (non ZDB), la base de données est généralement mise en veille, afin de permettre une utilisation par le système de sauvegarde et non par l'application, pendant toute la période de sauvegarde (plusieurs minutes ou heures). Par exemple, pour les sauvegardes sur bande, jusqu'à ce que le flux de données vers la bande soit terminé.
- Pour les méthodes ZDB, la base de données est également mise en veille, mais uniquement pendant le processus de duplication des données (plusieurs secondes). Le fonctionnement normal de la base de données peut alors être rétabli pour le reste du processus de sauvegarde.

Voir aussi sauvegarde avec temps d'indisponibilité nul (ZDB) et sauvegarde en ligne.

périphérique

Ce type de récupération est exécuté si le Gestionnaire de cellule est inaccessible, en raison de problèmes réseau, par exemple. Seuls les périphériques autonomes et les périphériques de bibliothèque SCSI peuvent être utilisés pour une récupération hors ligne. La récupération du Gestionnaire de cellule s'effectue toujours hors ligne.

périphérique cible (R2)

Voir journal de rétablissement archivé.

périphérique compatible OBDR

(terme propre à Informix Server) Système de sauvegarde et de restauration pour Informix Server. ON-Bar vous permet de créer une copie des données Informix Server et de les restaurer ultérieurement. Le système de sauvegarde et de restauration ON-Bar nécessite l'intervention des composants suivants :

- la commande `onbar`
- Data Protector en tant que solution de sauvegarde
- l'interface XBSA

- les tables de catalogue ON-Bar qui servent à sauvegarder les dbobjects et à effectuer le suivi des instances de dbobjects dans plusieurs sauvegardes.

périphérique de bibliothèque de fichiers

(terme propre à Informix Server) Variable d'environnement spécifiant le nom du fichier de configuration ONCONFIG actif. En cas d'absence de la variable d'environnement ONCONFIG, Informix Server utilise les valeurs de configuration du fichier `onconfig` dans le répertoire *`INFORMIXDIR`*`\etc` (sous Windows) ou *`INFORMIXDIR`*`/etc/` (sous UNIX).

périphérique de bibliothèque de stockage

Sauvegarde exécutée alors qu'une application de base de données reste disponible et utilisable. La base de données passe dans un mode de sauvegarde particulier et y reste tant que l'application de sauvegarde a besoin d'accéder aux objets de données d'origine. Pendant ce laps de temps, la base de donnée est entièrement opérationnelle ; toutefois ses performances peuvent être légèrement réduites et la taille des fichiers journaux peut augmenter très rapidement.

- Pour les méthodes de sauvegarde simples (non ZDB), le mode de sauvegarde est requis pendant toute la durée de la sauvegarde (plusieurs minutes ou heures). Par exemple, pour les sauvegardes sur bande, jusqu'à ce que le flux de données vers la bande soit terminé.
- Pour les méthodes ZDB, le mode de sauvegarde est requis uniquement pendant le processus de duplication des données (plusieurs secondes). Le fonctionnement normal de la base de données peut alors être rétabli pour le reste du processus de sauvegarde.

Dans certains cas, les journaux de transactions doivent également être sauvegardés pour permettre la restauration d'une base de données cohérente.
Voir aussi sauvegarde avec temps d'indisponibilité nul (ZDB) et sauvegarde hors ligne.

périphérique de bibliothèque de stockage de fichiers

(terme propre à Oracle) Journaux de rétablissement qui n'ont pas été archivés, mais qui sont à la disposition de l'instance à des fins d'enregistrement de la base de données ou qui sont pleins et attendent d'être archivés ou réutilisés.
Voir aussi journal de rétablissement archivé.

périphérique de fichier autonome

Voir OM.

périphérique de sauvegarde

Ensemble d'outils de connexion réseau permettant d'accéder à des machines distantes en toute sécurité grâce à une variété de méthodes d'authentification et de cryptage. Vous devez

l'installer et le configurer sur le Serveur d'installation et le client si vous exécutez une installation à distance via un shell sécurisé.

périphérique en mode continu

(terme propre à Oracle) Oracle Data Guard est la principale solution de récupération après sinistre d'Oracle. Oracle Data Guard peut gérer jusqu'à neuf bases de données en attente (auxiliaires), chacune constituant une copie en temps réel de la base de données de production (principale), pour protéger contre les altérations, les corruptions de données, les erreurs humaines et les sinistres. En cas de problème de la base de données de production, le basculement sur l'une des bases de données en attente est possible, celle-ci devenant alors la nouvelle base de données principale. En outre, le temps d'indisponibilité prévu pour la maintenance peut être réduit, car il est possible de faire rapidement basculer le traitement de production de la base de données principale actuelle sur une base de données en attente, et inversement ensuite.

périphérique physique

(terme propre à Oracle) Chaque installation d'une base de données Oracle sur un ou plusieurs systèmes. Plusieurs instances de base de données peuvent s'exécuter sur un même système informatique.

périphérique source (R1)

(terme propre à Oracle) Nom unique pour une instance de serveur Oracle. Pour passer d'un serveur Oracle à un autre, spécifiez le `ORACLE_SID` voulu. `ORACLE_SID` est inséré dans les parties CONNECT DATA du descripteur de connexion dans un fichier `TNSNAMES.ORA` et dans la définition du listener TNS dans le fichier `LISTENER.ORA`.

planificateur

Configuration système sauvegardée par Data Protector avant qu'un sinistre ne frappe le système.

point d'analyse

Option définissant un mode de résolution des conflits de fichiers au cours d'une restauration. Tous les fichiers sauvegardés sont restaurés, même s'ils sont plus anciens que les fichiers existants. *Voir aussi* fusion.

point de montage

HP Operations Manager pour Unix offre des fonctions puissantes pour gérer les opérations d'un grand nombre de systèmes et d'applications à l'intérieur d'un réseau. Data Protector fournit une intégration avec ce produit de gestion. Cette intégration est mise en œuvre sous la forme d'un module SMART Plug-In pour les serveurs de gestion OM sous HP-UX, Solaris et Linux. Les versions antérieures d'OM se nommaient IT/Operation, Operations Center et Vantage Point Operations. *Voir aussi* fusion.

point de montage de volume

La propriété d'une sauvegarde détermine qui est autorisé à restaurer des fichiers à partir de la sauvegarde. Le propriétaire de la session est la personne qui démarre la sauvegarde interactive. Si un utilisateur démarre une spécification de sauvegarde existante sans la modifier, la session n'est pas considérée comme interactive. Dans ce cas, si le propriétaire de la sauvegarde a été défini dans la spécification de la sauvegarde, celui-ci reste le propriétaire de la session. Dans le cas contraire, le propriétaire de la session est l'utilisateur qui a démarré la sauvegarde concernée. Pour les sauvegardes planifiées, le propriétaire par défaut de la session pour le Gestionnaire de cellule Unix est root.sys@*`Gestionnaire de cellule`*. Pour le Gestionnaire de cellule Windows, il s'agira de l'utilisateur indiqué pendant l'installation du Gestionnaire de cellule. Il est possible de modifier la propriété de manière à ce qu'un utilisateur spécifique devienne le propriétaire de la session.

pool de supports

Le fichier P1S contient des informations sur le formatage et le partitionnement de tous les disques installés sur un système lors d'une récupération après sinistre automatisée évoluée (EADR). Il est créé lors d'une sauvegarde complète et enregistré sur un support de sauvegarde et sur le Gestionnaire de cellule dans le répertoire*`répertoire_Data_Protector`*`\Config\Server\dr\p1s` d'un Gestionnaire de cellule Windows ou le répertoire `/etc/opt/omni/server/dr/p1s` d'un Gestionnaire de cellule UNIX, sous le nom `recovery.p1s`.

pool libre

(terme propre à MC/ServiceGuard et Veritas Cluster) Ensemble de ressources (par exemple, groupes de volumes, services d'applications, noms et adresses IP) nécessaires à l'exécution d'une application compatible cluster spécifique.

pool smart copy

(terme propre à HP StorageWorks Disk Array XP) Une paire de disques miroir peut avoir différentes valeurs d'état selon l'action effectuée. Les trois valeurs d'état les plus importantes sont les suivantes :

- COPY - La paire mise en miroir est en cours de resynchronisation. Les données sont transférées d'un disque à l'autre. Les disques ne contiennent pas les mêmes données.
- PAIR - La paire mise en miroir est complètement synchronisée et les données stockées sur les deux disques (le volume principal et le volume miroir) sont identiques.
- SUSPENDED - Le lien entre les disques miroir est suspendu. Cela signifie qu'il est possible d'accéder aux disques et de les mettre à jour indépendamment. Toutefois, la relation

de miroir est maintenue et la paire de disques peut être resynchronisée sans pour autant effectuer un transfert complet du contenu du disque.

post-exec

Procédé consistant à restaurer simultanément (c'est-à-dire en parallèle) des données sauvegardées vers plusieurs disques, en exécutant pour cela plusieurs Agents de disque qui reçoivent des données d'un Agent de support. Pour que la restauration parallèle fonctionne, les données sélectionnées doivent se trouver sur des disques ou volumes logiques différents, et lors de la sauvegarde, les données provenant des différents objets doivent avoir été envoyées au même périphérique avec deux Agents de disque ou plus. Pendant une restauration parallèle, les données concernant les différents objets à restaurer sont lues simultanément sur les supports, améliorant ainsi les performances du système.

pré-exécution

Concept consistant à lire plusieurs flux de données depuis une base de données en ligne.

Processus BC

Unité physique contenant soit un lecteur, soit une unité plus complexe (une bibliothèque, par exemple).

profil utilisateur

Option de sauvegarde permettant d'exécuter une commande ou un script après la sauvegarde d'un objet ou une fois la session de sauvegarde terminée. Les commandes post-exécution ne sont pas fournies avec Data Protector. L'utilisateur doit les créer lui-même. Elles peuvent être rédigées sous la forme de programmes exécutables ou de fichiers séquentiels sous Windows, ou bien de scripts shell sous UNIX.
Voir aussi pré-exécution.

propriétaire de la sauvegarde

Les commandes pré- et post-exécution servent à réaliser des actions supplémentaires avant et après une sauvegarde ou une restauration. Elles ne sont pas fournies avec Data Protector. L'utilisateur doit les créer lui-même. Ils peuvent être écrits sous forme d'exécutables ou de fichiers de commandes sous Windows, ou de scripts shell sous UNIX.

propriété

Dans un pool de supports, sous-ensemble de supports définissant l'ordre dans lequel les supports sont utilisés pour la sauvegarde.

protection

Option de sauvegarde permettant d'exécuter une commande ou un script avant la sauvegarde d'un objet ou le lancement de la session de sauvegarde. Les commandes pré-exécution ne sont pas fournies avec Data Protector. L'utilisateur doit les créer lui-même. Elles peuvent être rédigées sous la forme

de programmes exécutables ou de fichiers séquentiels sous Windows, ou bien de scripts shell sous UNIX.
Voir aussi post-exécution.

protection de catalogue

(terme propre à HP StorageWorks Disk Array XP) Il s'agit de LDEV HP StorageWorks Disk Array XP standard agissant comme volume principal pour les configurations CA et BC. Le P-VOL est situé dans le MCU.
Voir aussi volume secondaire (S-VOL) et unité de commande principale (MCU).

protection des données

Voir protection des données, ainsi que protection de catalogue.

pulsation

(terme propre à Microsoft Exchange Server) Partie de la banque d'informations conservant les informations se trouvant dans les dossiers publics. Une banque de dossiers publics est constituée d'un fichier binaire RTF `.edb` et d'un fichier de contenu Internet natif continu `.stm`.

quota de disque

Lors de la configuration d'une sauvegarde, l'utilisateur peut indiquer si les données sauvegardées seront :

- publiques, c'est-à-dire visibles (et accessibles pour la restauration) par tous les utilisateurs de Data Protector
- privées, c'est-à-dire visibles (et accessibles pour la restauration) uniquement par la propriétaire de la sauvegarde et les administrateurs

quotas de disque utilisateur

Redundant Array of Inexpensive Disks, baie de disques durs redondants bon marché.

RAID

(terme propre à HP StorageWorks Disk Array XP) Bibliothèque utilisée en interne par Data Protector sur les systèmes Solaris pour permettre l'accès aux données de configuration, d'état et de performances de HP StorageWorks Disk Array XP, ainsi qu'aux fonctions clé de HP StorageWorks Disk Array XP, au moyen d'appels de fonction convertis en une séquence de commandes SCSI de bas niveau.

Rapport d'audit

(terme propre à HP StorageWorks Disk Array XP) L'application Gestionnaire RAID XP met à disposition de l'utilisateur une liste complète de commandes permettant d'établir des rapports et de contrôler le statut des applications CA et BC. Ces commandes communiquent avec l'unité de commande de disque HP StorageWorks Disk Array XP par le biais d'une instance du Gestionnaire RAID. Cette instance convertit les commandes en une séquence de commandes SCSI de bas niveau.

RCU	*Voir* sauvegarde d'image disque.
RDF1/RDF2	*Voir* Unité de télécommande (RCU, pour Remote Control Unit).
RDS	Système de gestion de base de données relationnelle.
RecoveryInfo (Infos de récupération)	*(terme propre à EMC Symmetrix)* Type de groupe de périphériques SRDF. Seuls les périphériques RDF peuvent être attribués à un groupe RDF. Le type de groupe RDF1 contient des périphériques sources (R1) et le type de groupe RDF2 des périphériques cibles (R2).
récupération après sinistre	Le processus RDS (Raima Database Server) s'exécute sur le Gestionnaire de cellule Data Protector et gère la base de données IDB. Le processus démarre dès que Data Protector est installé sur le Gestionnaire de cellule.
récupération hors ligne	*(terme propre à Oracle)* Ensemble de tables et de vues Oracle permettant au Gestionnaire de récupération de stocker des informations sur les bases de données Oracle. Grâce à ces informations, le Gestionnaire de récupération peut gérer la sauvegarde, la restauration et la récupération des bases de données Oracle. Le catalogue de récupération contient des informations sur : • le schéma physique de la base de données cible Oracle, • les jeux de sauvegarde de fichiers de données et de journaux d'archive • les copies de fichiers de données, • les journaux de rétablissement archivés • les scripts stockés
récupération locale et distante	*(terme propre à Oracle)* Base de données Oracle contenant un schéma de catalogue de récupération. Ne stockez pas le catalogue de récupération dans votre base de données cible.
récupération matérielle	*(terme propre à Oracle)* Les fichiers de récupération sont des fichiers propres à Oracle 10g/11g qui résident dans la zone de récupération flash : fichier de contrôle actuel, journaux de rétablissement en ligne, journaux de rétablissement archivés, journaux de flashback, sauvegardes automatiques de fichier de contrôle, copies de fichier de données et éléments de sauvegarde. *Voir aussi* zone de récupération flash.
recyclage	Lors de la sauvegarde de fichiers de configuration Windows, Data Protector collecte les informations sur la configuration système actuelle (volume, configuration disque et réseau).

Ces informations sont nécessaires pour la récupération après sinistre.

réécriture — *(terme spécifique à Oracle)* Interface de ligne de commande Oracle contrôlant un processus du serveur Oracle pour la sauvegarde, la restauration ou la récupération de la base de données à laquelle il est connecté. RMAN stocke les informations sur les sauvegardes dans le catalogue de récupération ou dans le fichier de contrôle. Ces informations peuvent être utilisées lors de sessions de restauration ultérieures.

Registre Windows — Processus consistant à supprimer la protection de toutes les données sauvegardées se trouvant sur le support, autorisant ainsi Data Protector à les écraser au cours de l'une des sauvegardes ultérieures. Les données provenant de la même session, mais se trouvant sur d'autres supports, ne sont plus protégées non plus. Le recyclage ne modifie pas les données qui se trouvent sur le support.

Répertoire de catalogue des détails (DC) — *(terme propre à Oracle)* Chaque base de données Oracle dispose d'un ensemble de plusieurs fichiers journaux de rétablissement. Cet ensemble est appelé "journal de rétablissement de la base de données". Oracle y consigne toutes les modifications apportées aux données.

répertoire_Data_Protector — *(terme propre à HP StorageWorks Disk Array XP)* Unité agissant comme esclave d'une MCU dans une configuration CA. Dans les configurations bidirectionnelles, la RCU peut également agir comme une MCU.

réplique — *(terme propre à Windows)* Service Windows pour la gestion de supports amovibles (tels que des bandes et des disques) et de périphériques de stockage (bibliothèques). Le stockage sur périphériques amovibles permet aux applications d'accéder aux mêmes ressources et de les partager.

restauration incrémentale — *(terme propre à Windows)* Attribut contrôlé par le système et pouvant être associé à tout répertoire ou fichier. La valeur d'un attribut d'analyse peut comporter des données définies par l'utilisateur. Le format des données est reconnu par l'application sur laquelle elles étaient stockées et par un filtre de système de fichiers installé dans le but de permettre l'interprétation des données et le traitement des fichiers. Chaque fois que le système de fichiers rencontre un fichier comportant un point d'analyse, il essaie de trouver le filtre de système de fichiers associé au format de données.

restauration instantanée — *(terme propre à ZDB)* Image, à un instant donné, des données stockées sur les volumes sources qui contiennent

des objets sauvegarde propres à l'utilisateur. En fonction du matériel/logiciel avec lequel elle est créée, l'image peut être un doublon exact indépendant (clone) des blocs de stockage au niveau du disque physique (split mirror, par exemple) ou bien une copie virtuelle (par exemple, un snapshot). Du point de vue d'un système d'exploitation de base, le disque physique contenant les objets sauvegarde est répliqué dans son intégralité. Toutefois, si un gestionnaire de volume est utilisé sur UNIX, le groupe entier de volumes ou de disques contenant un objet sauvegarde (volume logique) est dupliqué. Si des partitions sont utilisées sous Windows, c'est l'ensemble du volume physique contenant la partition sélectionnée qui est répliqué.
Voir aussi snapshot, création de snapshot, split mirror et création de split mirror.

restauration parallèle

(terme propre à la sauvegarde ZDB) Groupe de répliques créées à l'aide de la même spécification de sauvegarde.
Voir aussi réplique et rotation de jeu de répliques.

restauration split mirror

(terme propre à ZDB) Utilisation d'un jeu de répliques pour la création régulière de sauvegardes : chaque fois qu'une même spécification de sauvegarde requérant l'utilisation d'un jeu de répliques est exécutée, une nouvelle réplique est créée et ajoutée au jeu, jusqu'à obtention du nombre maximal de répliques pour le jeu. La réplique la plus ancienne du jeu est alors remplacée et le nombre maximal de répliques du jeu conservé.
Voir aussi réplique et jeu de répliques.

RMAN *(terme propre à Oracle)*

Toutes les sauvegardes nécessaires à la restauration d'un objet sauvegarde à un point donné dans le temps. Une chaîne de restauration consiste en une sauvegarde complète de l'objet et un certain nombre de sauvegardes incrémentales liées.

rotation de jeu de répliques

Procédé consistant à copier les données d'un support de sauvegarde vers un système client.

rotation des miroirs *(terme propre à HP StorageWorks Disk Array XP)*

(terme propre au fournisseur VSS HP StorageWorks Disk Array XP) L'un des deux modes de fonctionnement du fournisseur matériel VSS XP. Quand le fournisseur XP est en mode de resynchronisation, le volume source (P-VOL) et sa réplique (S-VOL) sont en relation de miroir suspendu après une sauvegarde. Le nombre maximum de répliques (S-VOL par P-VOL) faisant l'objet d'une rotation est de trois, à condition que la plage de MU soit de 0-2 ou de 0, 1, 2. La restauration d'une sauvegarde dans ce type de configuration est seulement possible par le biais d'une resynchronisation d'un S-VOL avec son P-VOL.

Voir aussi mode compatible VSS, volume source, volume principal (P-VOL), réplique, volume secondaire (S-VOL), numéro de MU et jeu de répliques.

RSM

Voir gestionnaire de récupération.

RSM

Le Restore Session Manager Data Protector (Gestionnaire de session de restauration) contrôle la session de restauration. Ce processus est toujours exécuté sur le système du Gestionnaire de cellule.

sauvegarde avec temps d'indisponibilité nul (ZDB, pour zero downtime backup)

(terme propre à Windows) Le RSM (Removable Storage Manager), ou Gestionnaire de supports amovibles, comprend un service de gestion des supports facilitant la communication entre les applications, les changeurs robotiques et les bibliothèques de supports. Il permet à plusieurs applications de partager des bibliothèques de supports robotiques locales et des lecteurs de disques ou de bandes, et de gérer les supports amovibles.

sauvegarde complète

Fonction permettant d'identifier les supports contenus dans un périphérique. Cette fonction synchronise la MMDB avec les supports qui se trouvent aux positions sélectionnées (emplacements d'une bibliothèque, par exemple).

sauvegarde complète de boîte aux lettres

Fonction permettant d'identifier les supports contenus dans un périphérique. Cette fonction synchronise la MMDB avec les supports se trouvant aux emplacements sélectionnés (les logements d'une bibliothèque, par exemple). Elle est utile pour analyser et vérifier le support effectivement présent dans le périphérique lorsque quelqu'un a manipulé le support manuellement sans utiliser Data Protector pour l'éjecter ou l'insérer, par exemple.

sauvegarde complète synthétique

Fonction permettant de contrôler le moment et la fréquence des sauvegardes automatiques. En définissant un calendrier, l'utilisateur peut automatiser le lancement des sauvegardes.

sauvegarde complète virtuelle

(terme propre à HP StorageWorks Disk Array XP) LDEV XP agissant comme miroir CA ou BC secondaire d'un autre LDEV (P-VOL). Dans le cas d'un CA, les S-VOL peuvent être utilisés comme périphériques de secours dans une configuration MetroCluster. Des adresses SCSI distinctes, différentes des adresses utilisées par les P-VOL, sont attribuées aux S-VOL. *Voir aussi* volume principal (P-VOL) and unité de commande principale (MCU)

sauvegarde de client

Voir session de sauvegarde,session de gestion des supports et session de restauration.

sauvegarde de client avec découverte de disques	Identificateur d'une session de sauvegarde, de restauration, de copie d'objets, de consolidation d'objet ou de gestion de supports, qui est constitué de la date d'exécution de la session et d'un numéro unique.
sauvegarde de disque en plusieurs étapes	Cette variable d'environnement pour les scripts de pré-exécution et de post-exécution constitue une identification unique de session dans Data Protector, y compris pour les sessions de test. La clé de session n'est pas enregistrée dans la base de données ; elle permet de spécifier les options relatives aux commandes `omnimnt`, `omnistat`, et `omniabort`.
sauvegarde de la base de données complète	*(terme propre à Microsoft VSS)* Volume représentant un doublon du volume d'origine à un moment donné. La sauvegarde de données s'effectue alors depuis la copie miroir, et non depuis le volume d'origine. Le volume d'origine change à mesure que le processus de sauvegarde se poursuit ; la copie miroir, en revanche, demeure identique. *Voir aussi* Microsoft Volume Shadow Copy Service et réplique.
sauvegarde de la CONFIGURATION Windows	*(terme propre à Microsoft VSS)* Entité qui effectue le travail de création et de représentation des copies miroir de volumes. Les fournisseurs possèdent les données des copies miroir et exposent les copies miroir. Les fournisseurs peuvent être de type logiciel (par exemple les fournisseurs système) ou matériel (disques locaux, baies de disques). *Voir aussi* copie miroir.
sauvegarde de snapshot *(terme propre à HP StorageWorks VA et HP StorageWorks EVA)*	*(terme propre à Microsoft VSS)* Ensemble de copies miroir créées au même moment. *Voir aussi* copie miroir et jeu de répliques.
sauvegarde de transaction	Disque Windows situé sur un autre système et mis à la disposition d'autres utilisateurs sur le réseau. Les systèmes dotés de disques partagés peuvent être sauvegardés, même en l'absence d'un Agent de disque Data Protector.
sauvegarde de transactions	Les fichiers SIBF (Serverless Integrations Binary Files), ou fichiers binaires d'intégrations sans serveur, représentent la partie de la base de données IDB stockant les métadonnées brutes NDMP. Ces données sont nécessaires à la restauration des objets NDMP.
sauvegarde delta	*(terme propre à IAP)* Processus de reconnaissance de la redondance des données, au niveau objet et au niveau

segment. Il calcule un hachage puissant pour chaque segment de données et s'en sert comme adresse de contenu unique pour déterminer si des tentatives de stockage de doublons sont effectuées.
Voir aussi sauvegarde sur IAP

sauvegarde d'hôte

(terme propre à Microsoft Exchange Server) Service Microsoft Exchange Server 2000/2003 qui offre une compatibilité avec Microsoft Exchange Server 5.5 par l'émulation du service d'annuaire Exchange Server 5.5.
Voir aussi banque d'informations et service gestionnaire de clés.

sauvegarde différentielle

Position mécanique d'un élément dans une bibliothèque. Chaque emplacement peut contenir un support, comme une bande DLT. Data Protector attribue un numéro à chaque emplacement. Pour être lu, un support est déplacé par un mécanisme robotique de son emplacement dans le lecteur.

sauvegarde différentielle

Voir sauvegarde split miror (split mirror backup).

sauvegarde différentielle de base de données

(terme propre à VLS) Copie des données sauvegardées créée entre la bande virtuelle et la bibliothèque de bandes physiques. Le processus smart copy (copie intelligente) permet à Data Protector d'établir une distinction entre les supports source et cible, et ainsi de gérer les supports.
Voir aussi VLS (Virtual Library System - système de bibliothèques virtuelles).

sauvegarde d'image disque (rawdisk)

(terme propre à VLS) Pool définissant quels emplacement de la bibliothèque de destination sont disponibles au titre de cibles Smart Copy pour une bibliothèque virtuelle source spécifiée.
Voir aussi Système de bibliothèque virtuelle (VLS) et copie intelligente.

sauvegarde directe

Session Messages Binary Files - Les fichiers binaires de messages de session (SMBF), un élément de la base de données interne, contiennent les messages générés lors des sessions de sauvegarde, de restauration, de copie d'objets, de consolidation d'objet et de gestion des supports. Chaque session génère un fichier binaire. Les fichiers sont regroupés par année et mois.

sauvegarde du journal des transactions

(terme propre à HP StorageWorks VA et HP StorageWorks EVA) Il s'agit d'un type de réplique générée à l'aide de techniques de création de snapshot. Plusieurs types de snapshot sont disponibles, présentant des caractéristiques différentes en fonction des baies/techniques utilisées. Ces répliques sont

dynamiques et peuvent être des copies virtuelles basées sur le contenu des volumes source ou des doublons exacts indépendants (clones), en fonction du type de snapshot et du temps écoulé depuis la création.
Voir aussi réplique et création de snapshot.

sauvegarde en ligne
Voir sauvegarde ZDB sur bande, sauvegarde ZDB sur disque et sauvegarde ZDB sur disque+bande.

sauvegarde hors ligne
(terme propre à HP StorageWorks VA et HP StorageWorks EVA) Il s'agit d'une technique de création de réplique permettant de générer des copies de volumes sources via la technologie de virtualisation du stockage. Les répliques sont considérées comme créées à un instant donné bien précis, sans pré-configuration, et sont immédiatement disponibles. Cependant, les processus de copie en arrière-plan se poursuivent après la création.
Voir aussi snapshot.

sauvegarde incrémentale
(terme propre à EMC Symmetrix) Périphérique EMC Symmetrix prenant part aux opérations SRDF avec un périphérique cible (R2). Toutes les données écrites sur ce périphérique sont mises en miroir sur un périphérique cible (R2) situé sur une unité EMC Symmetrix distante. Tout périphérique R1 doit être attribué à un type de groupe RDF1.
Voir aussi target (R2) device.

sauvegarde incrémentale
(terme propre à la sauvegarde ZDB) Volume de stockage contenant les données à répliquer.

sauvegarde incrémentale avancée
Fichier contenant des données avec des parties de bloc vides. Exemples : matrice dont une partie ou la plupart des données contient des zéros, fichiers provenant d'applications de visualisation d'images, bases de données rapides. Si l'option de traitement des fichiers épars n'est pas activée pendant la restauration, il se peut que la restauration soit impossible.

sauvegarde incrémentale de la boîte aux lettres
(terme propre à EMC Symmetrix et HP StorageWorks Disk Array XP) Réplique générée à l'aide de techniques Split Mirror. Cette réplique fournit un doublon exact indépendant ou un clone du contenu des volumes source.
Voir aussi réplique et création de split mirror.

sauvegarde incrémentale1 de la boîte aux lettres
Voir sauvegarde ZDB sur bande.

sauvegarde rawdisk
Voir sauvegarde ZDB sur bande, sauvegarde ZDB sur disque et sauvegarde ZDB sur disque+bande.

sauvegarde sans bande*(terme propre à la sauvegarde ZDB)*

(terme propre à EMC Symmetrix et HP StorageWorks Disk Array XP) Technique de création de réplique qui synchronise un groupe préconfiguré de volumes cibles (un miroir) avec un groupe de volumes sources jusqu'à ce qu'une réplique du contenu des volumes sources soit requise. La synchronisation est ensuite interrompue (le miroir est divisé) et une réplique split mirror des volumes source au moment de la division reste dans les volumes cible.
Voir aussi split mirror.

sauvegarde split mirror *(terme propre à HP StorageWorks Disk Array XP)*

(terme propre à EMC Symmetrix et HP StorageWorks Disk Array XP) Processus par lequel les données sauvegardées lors d'une session ZDB sur bande ou ZDB sur disque + bande sont restaurées à partir de supports à bandes vers une réplique Split Mirror, qui est ensuite synchronisée avec les volumes sources. Les objets sauvegarde individuels ou les sessions complètes peuvent être restauré(e)s à l'aide de cette méthode.
Voir aussi sauvegarde ZDB sur bande, sauvegarde ZDB sur disque+bande et réplique.

sauvegarde split mirror*(terme propre à EMC Symmetrix)*

(terme propre à Informix Server) Fichier d'informations de connectivité Informix Server (sous UNIX) ou registre (sous Windows) contenant les noms de tous les serveurs de base de données, ainsi que tous les alias auxquels les clients d'un ordinateur hôte peuvent se connecter.

sauvegarde sur IAP

Le fichier de données de récupération système (DRS) Data Protector contient les informations système requises pour l'installation et la configuration du système d'exploitation en cas de sinistre. Il s'agit d'un fichier ASCII généré lorsque la sauvegarde de la CONFIGURATION est effectuée sur un client Windows, puis stockée sur le Gestionnaire de cellule.

sauvegarde synthétique

(terme propre à EMC Symmetrix) L'utilitaire SRDF (Symmetrix Remote Data Facility), ou utilitaire de gestion des données distantes Symmetrix, est un processus de continuité des activités permettant de dupliquer efficacement et en temps réel les données des SLD entre plusieurs environnements de traitement séparés. Ces environnements peuvent se trouver au sein d'un même ordinateur ou être séparés par de grandes distances.

sauvegarde système sur bande

(terme propre à HP StorageWorks Disk Array XP) Module logiciel Data Protector exécutant toutes les tâches nécessaires à une intégration de sauvegarde Split Mirror. Il communique avec le système de stockage HP StorageWorks Disk Array XP à l'aide de l'utilitaire du Gestionnaire RAID XP (pour les systèmes HP-UX et Windows) ou de la bibliothèque du Gestionnaire RAID (pour les systèmes Solaris).

sauvegarde ZDB	Le fichier `/usr/kernel/drv/sst.conf` doit être présent sur chaque client Solaris Data Protector auquel un périphérique de bibliothèque multi-lecteurs est connecté. Il doit contenir une entrée pour l'adresse SCSI du mécanisme robotique de chaque périphérique de bibliothèque connecté au client.
sauvegarde ZDB complète	Le fichier `/kernel/drv/st.conf` doit être présent sur chaque client Solaris Data Protector auquel un périphérique de sauvegarde est connecté. Il doit contenir des informations sur le périphérique et une adresse SCSI pour chaque lecteur de sauvegarde connecté au client. Une seule entrée SCSI est requise pour un périphérique à lecteur unique, tandis qu'il en faut plusieurs pour un périphérique de bibliothèque multi-lecteurs.
sauvegarde ZDB incrémentale	Périphériques possédant plusieurs emplacements destinés au stockage des supports et disposant généralement d'un seul lecteur. Un chargeur sélectionne les supports dans une pile de manière séquentielle. Une bibliothèque, en revanche, peut sélectionner les supports de manière aléatoire depuis son référentiel.
sauvegarde ZDB sur bande	Un périphérique de fichier est un fichier dans un répertoire désigné vers lequel vous sauvegardez des données.
sauvegarde ZDB sur disque	*(terme propre à Microsoft Exchange Server)* Regroupement de banques de boîtes aux lettres et de dossiers publics se partageant un ensemble de fichiers journaux de transactions. Exchange Server gère chaque groupe de stockage au moyen d'un processus de serveur distinct.
sauvegarde ZDB sur disque+bande	*(terme propre à StorageTek)* Système de bibliothèque (également connu sous le nom de "Silo") constitué d'une unité de gestion de bibliothèque (LMU) et d'un à vingt-quatre modules de stockage en bibliothèque (LSM) connectés à l'unité.
Script CMD pour Informix Server	*(terme propre à la sauvegarde ZDB)*Un volume de stockage représente un objet qui peut être transféré sur un système d'exploitation ou toute autre entité (un mécanisme de virtualisation, par exemple) et sur lequel peuvent résider des systèmes de gestion de volume, des systèmes de fichiers ou d'autres objets. Les systèmes de gestion de volumes et les systèmes de fichiers sont basés sur ce type de stockage. Habituellement, ils peuvent être créés ou existent déjà dans un système de stockage tel qu'une baie de disques.
script shell log_full	*Voir* basculement.

segmentation

(terme propre à Sybase) Interface destinée à l'échange de données de sauvegarde et de récupération entre un serveur SQL Sybase et une solution de sauvegarde comme Data Protector.

Serveur d'installation

(terme propre à StorageTek) Automated Cartridge System Library Server (ACSLS), serveur de bibliothèque à système de cartouche automatisé - logiciel chargé de la gestion du système de cartouche automatisé (ACS).

serveur de bases de données

(terme propre à Sybase) Le serveur d'une architecture "client-serveur" Sybase. Le serveur Sybase SQL gère plusieurs bases de données et utilisateurs, assure le suivi des positions physiques des données sur les disques, établit le mappage entre la description logique des données et leur stockage physique et maintient les caches de données et de procédures en mémoire.

serveur de lecteurs multiples

(terme propre à EMC Symmetrix) Module logiciel Data Protector qui prépare l'environnement EMC Symmetrix aux opérations de sauvegarde et de restauration.

serveur de l'interface Java

Méthode qui produit une sauvegarde complète synthétique, équivalente à une sauvegarde complète classique en termes de données, sans perturber les serveurs de production ou le réseau. Une sauvegarde complète synthétique est créée à partir d'une sauvegarde complète précédente et d'un certain nombre de sauvegardes incrémentales.

Serveur DHCP

Résultat d'une opération de consolidation d'objet, au cours de laquelle une chaîne de restauration d'un objet sauvegarde est fusionnée en une nouvelle version complète synthétique de cet objet. En termes de vitesse de restauration, une telle sauvegarde est équivalente à une sauvegarde complète classique.

serveur DNS

(terme propre à Oracle) Interface Oracle chargée d'exécuter les actions nécessaires au chargement, à l'étiquetage et au déchargement des périphériques de sauvegarde appropriés lorsqu'Oracle émet des demandes de sauvegarde ou de restauration.

serveur Informix

(terme propre à Sybase) Les quatre bases de données système d'un serveur Sybase SQL nouvellement installé sont les suivantes :

- base de données principale (master)
- base de données temporaire (tempdb)
- base de données de procédures système (sybsystemprocs)
- base de données modèle (model).

serveur virtuel	*(terme propre à Windows)* Les données d'état système comprennent le registre, la base de données d'enregistrement de classe COM+, les fichiers de démarrage système et la base de données de services de certificats (à condition que le serveur soit du type "certificate server"). Si le serveur correspond à un contrôleur de domaine, les données d'état du système contiennent également les services Active Directory et le répertoire SYSVOL. Si le serveur exécute le service de cluster, les données d'état système comprennent également les points de contrôle du registre de ressource et le journal de récupération de ressource quorum, qui contient les informations les plus récentes concernant la base de données de clusters.
serveur WINS	Volume, disque ou partition contenant les fichiers du système d'exploitation. La terminologie utilisée par Microsoft définit ces éléments comme ceux contenant les fichiers nécessaires pour assurer les premières étapes du processus d'amorçage.
service de réplication de fichiers (FRS, pour File Replication Service)	*(terme propre à Windows)* Répertoire partagé contenant la copie des fichiers publics du domaine sur le serveur. Ces fichiers sont reproduits sur tous les contrôleurs du domaine.
Service de réplication Exchange	Partie de la structure d'une base de données. Chaque base de données est divisée de manière logique en un ou plusieurs espaces de table. Chaque espace de table contient des fichiers de données ou des volumes bruts qui lui sont exclusivement associés.
service Gestionnaire de clés	*Voir* sauvegarde ZDB sur disque.
service Réplication de site	*(terme propre à Oracle)* Terme utilisé dans le contexte du Gestionnaire de récupération (RMAN). La base de données cible est celle qui est sauvegardée ou restaurée.
session	*(terme propre à EMC Symmetrix)* Périphérique EMC Symmetrix prenant part aux opérations SRDF avec un périphérique source (R1). Il réside sur l'unité EMC Symmetrix distante. Il est apparié à un périphérique source (R1) dans l'unité EMC Symmetrix locale et reçoit toutes les données écrites sur le périphérique dont il est le miroir. Pendant les opérations d'E/S courantes, les applications utilisateur ne peuvent accéder à ce périphérique cible. Tout périphérique R2 doit être affecté à un type de groupe RDF2. *Voir aussi* périphérique source (R1).

session de consolidation d'objet	*(terme propre à la récupération après sinistre)* Système après la survenue d'un sinistre. Le système cible est généralement non amorçable et l'objet de la récupération après sinistre consiste justement à redonner à ce système sa configuration initiale. La différence entre un système endommagé et un système cible réside dans le fait que, pour le système cible, le matériel défaillant a été remplacé.
session de copie d'objet	*(terme propre à la sauvegarde ZDB)* Volume de stockage sur lequel les données sont dupliquées.
session de gestion de supports	*(terme propre à Windows)* Les services Terminal Server de Windows fournissent un environnement multi-sessions permettant aux clients d'accéder à des sessions Windows virtuelles ainsi qu'à des applications Windows exécutées sur le serveur.
session de restauration	*(terme propre à Microsoft SQL Server)* Entité exécutable appartenant à un seul processus. Elle comprend un compteur de programme, une pile en mode utilisateur, une pile en mode kernel et un ensemble de valeurs de registre. Plusieurs threads peuvent être exécutés en même temps dans un même processus.
session de sauvegarde	*(terme propre à EMC Symmetrix)* Processus Business Continuance permettant de créer une copie instantanée d'un ou plusieurs périphériques logiques Symmetrix (SLD). Cette copie est créée sur des SLD préconfigurés spécialement et appelés BCV ; elle est accessible via une adresse de périphérique distincte.
SGBDR	Tape Library Unit ou unité de bibliothèque de bandes.
SIBF	*(terme propre à Oracle et SAP R/3)* Fichier de configuration réseau contenant des descripteurs de connexion mappés à des noms de services. La maintenance du fichier peut s'effectuer au niveau central ou au niveau local, afin d'être accessible à tous les clients ou à chacun d'entre eux individuellement.
simultanéité	Mécanisme destiné à s'assurer qu'un ensemble d'actions est considéré comme une seule unité de travail. Les bases de données utilisent les transactions pour effectuer un suivi des modifications.
SMB	Les sauvegardes de transaction nécessitent généralement moins de ressources que les sauvegardes de base de données ; elles peuvent donc être effectuées plus souvent que les sauvegardes de base de données. En effectuant des sauvegardes de transaction, l'utilisateur peut récupérer la base de données telle

qu'elle était à un moment précis précédant la survenue d'un problème.

SMBF — *(terme propre à Sybase et SQL)* Sauvegarde du journal de transactions contenant un enregistrement des modifications effectuées depuis la dernière sauvegarde complète ou la dernière sauvegarde de transactions.

snapshot — Les sauvegardes de journal de transactions nécessitent généralement moins de ressources que les sauvegardes de base de données ; elles peuvent donc être effectuées plus souvent que les sauvegardes de base de données. En effectuant des sauvegardes des journaux de transactions, l'utilisateur peut récupérer la base de données telle qu'elle était à un moment précis.

snapshot transportable — Fichiers qui enregistrent les transactions relatives aux modifications de la base de données, et assurent la tolérance aux pannes en cas de sinistre de la base de données.

spécification de sauvegarde — *(terme propre à Data Protector)* Assurent le suivi des modifications de la base de données IDB. Il est recommandé d'activer l'archivage des journaux de transactions pour éviter de perdre les fichiers journaux créés après la dernière sauvegarde de la base de données IDB et nécessaires à sa récupération.

split mirror — *(terme propre à Sybase)* Table système où sont enregistrées automatiquement toutes les modifications apportées à la base de données.

SRDF — *(terme propre à Microsoft VSS)* Copie miroir créée sur le système d'application et pouvant être présentée au système de sauvegarde où est effectuée une sauvegarde.
Voir aussi Microsoft Volume Shadow Copy Service (VSS).

stratégie d'allocation de supports — *(terme propre à Novell NetWare)*Fichier permettant à l'utilisateur de spécifier les noms des conteneurs à partir desquels les sauvegardes doivent commencer. Il s'agit d'un fichier texte situé dans le répertoire `SYS:SYSTEM\TSA` du serveur où est chargé `TSANDS.NLM`.

stratégie d'utilisation des supports — Le serveur d'interface utilisateur graphique Java (le service `UIProxy`) s'exécute sur le Gestionnaire de cellule Data Protector. Il est chargé de la communication entre le client de l'interface Java et le Gestionnaire de cellule. De plus, il effectue des opérations logiques et envoie uniquement les informations importantes au client. Le processus démarre dès que Data Protector est installé sur le Gestionnaire de cellule.

Sybase SQL Server *Voir* opération hors contrôle.

système cible Vous ne pouvez utiliser Data Protector que si vous disposez d'un compte utilisateur Data Protector, lequel limite l'accès non autorisé à Data Protector et aux données sauvegardées. Les administrateurs Data Protector créent ce compte en spécifiant un nom d'utilisateur, les systèmes à partir desquels l'utilisateur peut se connecter et le groupe d'utilisateurs Data Protector auquel il sera affecté. Ces éléments sont vérifiés chaque fois que l'utilisateur démarre l'interface utilisateur de Data Protector ou effectue certaines tâches.

système d'application (contrôle des comptes utilisateur) Composant de sécurité des systèmes Windows Vista et Windows Server 2008 qui limite les logiciels d'application aux privilèges utilisateur standard jusqu'à ce qu'un administrateur autorise une augmentation du niveau de privilèges.

Système de bibliothèques virtuelles (VLS, pour Virtual Library System) La prise en charge de la gestion de quota NTFS permet d'optimiser le suivi et le contrôle de l'utilisation de l'espace disque sur les volumes de stockage partagés. Data Protector sauvegarde simultanément les quotas de disque utilisateur sur l'ensemble du système et pour tous les utilisateurs configurés.

système de fichiers Chaque utilisateur de Data Protector est membre d'un groupe d'utilisateurs et chaque utilisateur faisant partie d'un groupe d'utilisateurs reçoit les mêmes droits. Le nombre de groupes d'utilisateurs et leurs droits utilisateur peuvent être définis librement. Dans Data Protector, on distingue trois groupes d'utilisateurs par défaut : administrateur, Opérateur et Utilisateur.

système de fichiers distribués (DFS) *(terme propre à Windows)* nformations de configuration définies pour chaque utilisateur. Ces informations comprennent la configuration du bureau, les couleurs d'écran sélectionnées, les connexions réseau, etc. Lorsqu'un utilisateur se connecte, le système charge son profil et l'environnement Windows le prend en compte.

système de sauvegarde Les droits utilisateur ou droits d'accès correspondent aux autorisations nécessaires pour exécuter certaines tâches dans Data Protector. telles que la configuration d'une sauvegarde, le démarrage d'une session de sauvegarde ou le lancement d'une session de restauration. Les utilisateurs disposent des droits d'accès du groupe d'utilisateurs auquel ils appartiennent.

système d'hébergement ou système hôte	Procédé consistant à stocker des supports dans un emplacement sécurisé et distant. Les supports sont retournés au "centre de données" lorsqu'une restauration de données est nécessaire ou lorsqu'ils sont prêts à être réutilisés pour d'autres sauvegardes. La façon dont la mise au coffre est réalisée dépend de la stratégie de sauvegarde adoptée par votre entreprise et de sa politique de protection et de fiabilité de données.
système d'origine	Fonction permettant à l'utilisateur de contrôler si les données Data Protector stockées sur un support spécifique sont lisibles. En outre, si l'option CRC (contrôle de redondance cyclique) était activée lors de la sauvegarde, vous pouvez contrôler la cohérence de chaque bloc.
SysVol	*(terme propre à HP StorageWorks EVA)* Micrologiciel gérant tous les aspects du fonctionnement du système de stockage, dont les communications avec Command View EVA via les contrôleurs HSV. *Voir aussi* Command View (CV) EVA.
table des journaux de transactions	*(terme propre à Microsoft SQL Server)* Interface de programmation de Microsoft SQL Server permettant de sauvegarder et de restaurer rapidement des bases de données volumineuses.
Terminal Services	*(terme propre à HP StorageWorks EVA)* Unité de stockage attribuée à partir d'un pool de disques HP StorageWorks Enterprise Virtual Array. Les disques virtuels sont les entités dupliquées à l'aide de la fonctionnalité Snapshot de HP StorageWorks Enterprise Virtual Array. *Voir aussi* volume source et volume cible.
thread	Type de sauvegarde synthétique efficace au cours de laquelle les données sont consolidées à l'aide de pointeurs au lieu d'être copiées. Elle est réalisée si toutes les sauvegardes (la sauvegarde complète, les sauvegardes incrémentales et la sauvegarde complète virtuelle résultante) sont écrites dans une seule bibliothèque de fichiers qui utilise le format de support de fichiers distribués.
TimeFinder	Périphérique de stockage de données sur disque hébergeant une ou plusieurs bibliothèques de bandes virtuelles (VTL).
TLU	Machine virtuelle dans un environnement de clusters définie sur un domaine par un nom et une adresse IP réseau. Son adresse est mise en cache par le service de cluster et mappée au nœud cluster qui exécute les ressources du serveur virtuel. De cette façon, toutes les demandes concernant un serveur virtuel donné sont mises en cache par un noeud de cluster spécifique.

TNSNAMES.ORA

(terme propre à VLS) Technologie d'archivage qui sauvegarde les données sur des lecteurs de disques de la même façon que si elles étaient stockées sur bande. Les systèmes de bandes virtuelles permettent d'accélérer les processus de sauvegarde et de restauration et de réduire les coûts de fonctionnement.
Voir aussi système de bibliothèques virtuelles (VLS) et bibliothèque de bandes virtuelle.

transaction

(terme propre à VLS) Emulation de bibliothèque de bandes fournissant les mêmes fonctionnalités qu'un stockage sur bandes traditionnel.
Voir aussi Système de bibliothèques virtuelles (VLS).

type de support

(terme propre à l'intégration VMware) Client utilisé par Data Protector pour communiquer avec VMware Virtual Infrastructure. Il peut s'agir d'un système VirtualCenter Server (environnement VirtualCenter) ou d'un système ESX Server (environnement ESX Server autonome).

types de sauvegarde

(terme propre à ADIC et STK) Un volser (VOLume SERial number - numéro de série de volume) est une étiquette située sur le support qui permet d'identifier la bande physique dans les très grandes bibliothèques. Il s'agit d'une appellation spécifique aux périphériques ADIC/GRAU et StorageTek.

UIProxy

Unité de stockage des données dans un système LVM. Un groupe de volumes peut être constitué d'un ou plusieurs volumes physiques. Le système peut contenir plusieurs groupes de volumes.

unité de commande principale (MCU, pour Main Control Unit)

(terme propre à Windows) Répertoire vide sur un volume pouvant être utilisé pour le montage d'un autre volume. Le point de montage de volume sert de passerelle vers le volume cible. Une fois le volume monté, les utilisateurs et les applications peuvent consulter les données stockées sur celui-ci par le chemin d'accès au système de fichiers complet (fusionné), comme si les deux volumes ne faisaient qu'un.

unité de télécommande (RCU)

Voir Microsoft Volume Shadow Copy Service.

User Account Control (UAC)

Voir OM.

volser

Le gestionnaire de volume Veritas est un système permettant de gérer l'espace disque sur les plates-formes Solaris. Un système VxVM est constitué de groupes arbitraires d'un ou plusieurs volumes physiques organisés en groupes de disques logiques.

volume cible	Fonction de mise en marche à distance pour les systèmes s'exécutant en mode d'économie d'énergie à partir d'un autre système se trouvant sur le même réseau local.
volume de stockage	Fonction Data Protector permettant à l'utilisateur d'afficher des rapports sur l'état de la sauvegarde, de la consolidation et de la copie d'objet, ainsi que sur la configuration Data Protector à l'aide de l'interface Web.
volume principal (P-VOL)	Caractère pouvant être utilisé pour représenter un ou plusieurs caractères. Par exemple, l'astérisque (*) représente généralement un ou plusieurs caractères et le point d'interrogation (?) un seul caractère. Les caractères génériques sont souvent utilisés avec les systèmes d'exploitation pour spécifier plusieurs fichiers par nom.
volume secondaire (S-VOL)	Data Protector permet de sauvegarder la CONFIGURATION Windows, y compris le registre Windows, les profils utilisateur, les journaux d'événements et les données des serveurs WINS et DHCP (s'ils sont configurés) en une seule étape.
Volume Shadow Copy Service	Base de données centralisée utilisée par Windows pour stocker les informations relatives à la configuration du système d'exploitation et des applications installées.
volume source	Système sur lequel s'exécute le logiciel Windows Internet Name Service chargé de la résolution des noms des ordinateurs du réseau Windows en adresses IP. Data Protector peut sauvegarder les données du serveur WINS dans le cadre de la configuration Windows.
volume/disque/ partition d'amorçage	*(terme propre à Microsoft VSS)* Processus initiant la modification des données sur le volume d'origine. Les modules d'écriture sont généralement des applications ou des services système écrivant des informations permanentes sur un volume. Ils participent également au processus de synchronisation des copies miroir en assurant la cohérence des données.
volume/disque/ partition système	*(terme propre à Informix Server)* L'utilitaire ON-Bar et Data Protector communiquent par le biais de l'interface de programmation XBSA (X/Open Backup Services Application).
VPO	*(terme propre à la sauvegarde directe)* Commande SCSI-3 permettant de copier des données d'un périphérique de stockage doté d'une adresse SCSI source vers un périphérique de stockage doté d'une adresse SCSI cible, autorisant ainsi une sauvegarde directe. Les données transitent du périphérique source (en bloc ou en continu, c'est-à-dire sur disque ou sur bande) vers le périphérique cible (en bloc ou en continu)

via XCopy. Ainsi, le serveur de contrôle n'a plus besoin de transférer les données du périphérique de stockage vers la mémoire ni de les écrire sur le périphérique cible.
Voir aussi sauvegarde directe.

VSS

Voir sauvegarde avec temps d'indisponibilité nul (zero downtime backup).

VxFS

(terme propre à la sauvegarde ZDB) Partie de la base de données IDB stockant des informations relatives à ZDB telles que les volumes source, les répliques et des informations relatives à la sécurité. La base de données ZDB est utilisée pour la sauvegarde avec temps d'indisponibilité nul, la restauration instantanée et la restauration split mirror.
Voir aussi sauvegarde avec temps d'indisponibilité nul (ZDB, pour zero downtime backup).

VxVM (Veritas Volume Manager)

(terme propre à la sauvegarde ZDB) Type de sauvegarde avec temps d'indisponibilité nul caractérisé par le fait que la réplique créée est conservée sur la baie de disques en tant que sauvegarde des volumes source à un instant donné. Il est possible de conserver plusieurs répliques, générées avec la même spécification de sauvegarde à des instants différents, dans un jeu de répliques. Une réplique effectuée à partir d'une sauvegarde ZDB sur disque peut être restaurée via le processus de restauration instantanée.
Voir aussi sauvegarde avec temps d'indisponibilité nul (ZDB, pour zero downtime backup), sauvegarde ZDB sur bande, sauvegarde ZDB sur disque+bande, restauration instantanée et rotation de jeu de répliques.

Wake ONLAN

(terme propre à la sauvegarde ZDB) Type de sauvegarde avec temps d'indisponibilité nul au cours de laquelle la réplique créée est conservée sur la baie de disques en tant que sauvegarde des volumes sources à un instant précis, de la même façon que lors d'une session ZDB sur disque. Toutefois, les données de la réplique sont également transférées sur un support de sauvegarde, comme lors du processus ZDB sur bande. Si cette méthode de sauvegarde est utilisée, les données sauvegardées dans la même session peuvent être restaurées via le processus de restauration instantanée, la restauration Data Protector standard à partir d'une bande ou sur des baies Split Mirror, via la restauration Split Mirror.
Voir aussi sauvegarde avec temps d'indisponibilité nul (ZDB, pour zero downtime backup), sauvegarde ZDB sur disque, sauvegarde ZDB sur bande, restauration instantanée, réplique et rotation de jeu de répliques.

Web reporting

(terme propre à la sauvegarde ZDB) Type de sauvegarde avec temps d'indisponibilité nul caractérisé par le fait que la réplique créée est copiée en continu sur un support de sauvegarde, généralement une bande. La restauration instantanée étant impossible avec ce type de sauvegarde, la réplique ne doit pas être conservée sur la baie de disques après la sauvegarde. Les données sauvegardées peuvent être restaurées à l'aide de la restauration Data Protector standard à partir d'une bande. Sur les baies split mirror, la restauration split mirror peut également être utilisée.
Voir aussi sauvegarde avec temps d'indisponibilité nul (ZDB, pour zero downtime backup), sauvegarde ZDB sur disque, restauration instantanée, sauvegarde ZDB sur disque+bande et réplique.

zone de récupération flash

Mode de sauvegarde utilisant des techniques de réplication de données, fournies par une baie de disques, pour réduire l'impact des opérations de sauvegarde sur un système d'application. Une réplique des données à sauvegarder est tout d'abord créée. Toutes les opérations de sauvegarde suivantes sont effectuées au niveau des données répliquées plutôt que les données d'origine, le système d'application pouvant retourner en mode de fonctionnement normal.
Voir aussi sauvegarde ZDB sur disque, sauvegarde ZDB sur bande, sauvegarde ZDB sur disque+bande et récupération instantanée.

Index

A

A.05.10, A.05.50 ou A.06.00
  migration de licences, 365
activation de la vérification d'accès
  pour un client, 218
  pour une cellule, 220
adresse IP, TCP/IP, 392
adresses SCSI
  Voir interface SCSI
adresses SCSI non utilisées
  Voir interface SCSI
Agent de disque
  configuration, sur HP OpenVMS, 136
agent de disque
  concepts, 30
Agent de support
  installation pour l'utilisation d'une bibliothèque ADIC/GRAU, 120
agent de support
  concepts, 30
  configuration sous Novell NetWare, 130
  configuration, sur HP OpenVMS, 137
  installation pour une bibliothèque StorageTek ACS, 125
  types, 30
Agent de support NDMP, concepts, 30
Agent général de support
  vérification de l'installation, sous Novell NetWare, 436
aide
  obtention, 27
ajout
  ajout de pilote de robot SCSI au noyau, sous HP-UX, 410
  droits d'accès, sous Linux, 105
Ajout de clients à la cellule
  interface utilisateur graphique de Data Protector, 78
  interface graphique Java de Data Protector, 78
ajout de composants logiciels
  à des systèmes Solaris, 244
  à des systèmes Windows, 242
  présentation, 242
  sur des systèmes HP-UX, 243
Application Recovery Manager
  mise à niveau, 286
attribution des licences
  déplacement des licences, 329
  détermination des licences installées, 329
  détermination des mots de passe requis, 320
  Edition serveur unique, 363
  extensions de lecteur, 352
  Extensions fonctionnelles, 307
  extensions fonctionnelles, 354
  formulaires d'attribution de licences, 369
  gestion centralisée des licences, configuration, 330
  Gestionnaire de cellule, 308
  licences basées sur la capacité, 309
  licences basées sur la capacité, exemples, 314
  licences basées sur les entités, 308
  licences de lecteur, 307
  migration de Data Protector, 365
  migration de licence, 364
  mise à niveau à partir de Data Protector A.05.10, A.05.50 et A.06.00, 250
  mise à niveau à partir de SSE, 285
  mots de passe d'urgence, 322
  mots de passe permanents, 321

mots de passe permanents, obtention et installation, 322, 328
mots de passe temporaires, 321
obtention et installation de mots de passe permanents, 322, 328
Packs Starter, 307
présentation, 319
présentation des attributions de licences des produits, 320
présentation des produits, 350
productions de rapports sur les licences, 318
structure du produit, 307, 349
types de mots de passe, 321
utilisation des licences, après mise à niveau, 250, 285
utilitaire AutoPass, 322
vérification des mots de passe, 328
vérification et signalement des licences manquantes, 307
auto-migration VLS
configuration requise, 179
installation, 179

B

Bibliothèque ACS StorageTek
connexion de lecteurs, 119
bibliothèque ACS StorageTek
installation de l'agent de support, 118
préparation des clients, 124
bibliothèque ADIC
Voir bibliothèque ADIC/GRAU
bibliothèque ADIC/GRAU
connexion de lecteurs, 119
installation de l'agent de support, 118
installation d'agents des supports des données sur les clients, 120
préparation des clients, 119
bibliothèque GRAU
Voir bibliothèque ADIC/GRAU
bibliothèque HP StorageWorks 330fx, définition des ID SCSI, 422
bibliothèque HP StorageWorks DLT 28/48 logements, connexion, 430
bibliothèque StorageTek
Voir bibliothèque ACS StorageTek
bibliothèque StorageTek ACS
installation d'agents des supports des données sur les clients, 125

C

caractères multi-octets, 277
cellule
activation de la sécurité, 220
concepts, 29
exportation de clients, 211
exportation d'un client Microsoft Cluster Server, 213
importation de clients, 205
importation de clusters, 208
importation d'un Serveur d'installation, 207
licences, 307
mise à niveau, présentation, 248
sécurisation de clients, 218
vérification des connexions DNS, 334
cellule
licences, 308
chargeur automatique HP Surestore 12000e, connexion, 428
CLI
Voir interface de ligne de commande
client
activation de la vérification d'accès, 218
ajout de droits d'accès root, sous Linux, 105
changement de composants logiciels, 242
compatible cluster, importation dans une cellule, 208
concepts, 29
concepts de sécurité, 214
configuration après installation, sur Solaris, 99
configuration de TCP/IP, sous Windows, 391
configuration du noyau, sous Linux, 107

configuration pour l'utilisation des périphériques de sauvegarde, sous Solaris, 417
configuration pour Veritas Volume Manager, sur Microsoft Cluster Server, 441
création de fichiers de périphérique, sous HP-UX, 412
création de fichiers de périphérique, sous Solaris, 420
désinstallation à distance, 231
exportation d'une cellule, 211
importation dans une cellule, 205
installation des intégrations compatibles cluster, présentation, 148
installation des intégrations, présentation, 145
installation distante, présentation, 78
installation en local sur HP OpenVMS, 132
installation en local, sous Novell NetWare, 126
installation, présentation, 70
Microsoft Cluster Server, exportation d'une cellule, 213
mise à niveau à partir de Data Protector A.05.10, A.05.50 et A.06.00, 263
mise à niveau à partir de Data Protector A.05.10, A.05.50 et A.06.00, sous MC/ServiceGuard, 264
mise à niveau, sur Microsoft Cluster Server, 305
préparation à l'utilisation d'une bibliothèque ADIC/GRAU, 119
préparation pour l'utilisation d'une bibliothèque StorageTek ACS, 124
refus d'accès par des hôtes, 222
résolution des problèmes, 336, 339, 340, 345, 347
sécurisation, 218
suppression de la vérification d'accès, 222
vérification de la configuration TCP/IP, sous Windows, 395
vérification de l'installation, 342
client ACS, 118
client AIX
connexion de périphériques de sauvegarde, 111
installation, 110
client cartes LAN multiples, importation, 207
client DAS, 118
client de l'interface Java, 228, 231
client d'intégration, 145
Voir aussi intégrations
client d'intégration ZDB, 146
Voir aussi intégrations
client ESX Server
installation, 109
client HP OpenVMS
configuration de l'agent de disque, 136
configuration de l'Agent de support, 137
désinstallation, 232
importation, 207
client HP-UX
connexion de périphériques de sauvegarde, 96
installation, 94
résolution des problèmes, 339

client Linux
configuration du noyau, 107
connexion de périphériques de sauvegarde, 108
installation, 103
résolution des problèmes d'installation à distance, 105
Client Microsoft Terminal Services, 53
client MPE/iX, installation, 139
client NDMP, importation, 207
client Novell NetWare
configuration de l'Agent de support, 130
fichier HPDEVBRA.NLM, 440
fichier HPUMA.NLM, 440
installation, 126
minimisation du trafic réseau, 130
vérification de l'installation de l'Agent général de support, 436
client SCO
connexion de périphériques de sauvegarde, 117
installation, 116
client Siemens Sinix
connexion de périphériques de sauvegarde, 112
installation, 112
client Solaris
configuration, après installation, 99
connexion de périphériques de sauvegarde, 102
installation, 97
résolution des problèmes, 339
client sous Windows
connexion de périphériques de sauvegarde, 92
désinstallation, 231
installation, 87
résolution des problèmes, 336, 340, 345
Client Terminal Services, 53
client Tru64
connexion de périphériques de sauvegarde, 115
installation, 114
client, connexion de périphériques de sauvegarde
clients AIX, 111
clients HP-UX, 96
clients Linux, 108
clients SCO, 117
clients Siemens Sinix, 112
clients Solaris, 102
clients sous Windows, 92
clients Tru64, 115
lecteurs de bibliothèque ADIC/GRAU, 119
client, installation
agent de support pour bibliothèque ADIC/GRAU, 120
agent de support pour bibliothèque StorageTek ACS, 125
auto-migration VLS, 179
Edition serveur unique, 184
IAP, 178
intégration DB2, 153
intégration de HP StorageWorks EVA, 171
intégration HP StorageWorks Disk Array XP, 159
intégration HP StorageWorks VA, 165
intégration Informix, 150
intégration Lotus, 154
intégration Microsoft Exchange, 149
intégration Microsoft SharePoint Portal Server, 150
intégration Microsoft SQL, 149
intégration Microsoft Volume Shadow Copy, 153
intégration NDMP, 153
intégration NNM, 153
intégration Oracle, 152
intégration SAP DB, 151
intégration SAP R/3, 151
intégration Sybase, 150
Intégration VMware, 152
sur des systèmes de clusters IBM HACMP, 203
sur des systèmes HP-UX, 94
sur des systèmes Novell NetWare Cluster Services, 201

sur des systèmes Siemens Sinix, 112
sur des systèmes Tru64, 114
sur des systèmes Veritas Cluster, 200
sur les systèmes AIX, 110
sur les systèmes ESX Server, 109
sur les systèmes Linux, 103
sur les systèmes MC/ServiceGuard, 187
sur les systèmes Microsoft Cluster Server, 197
sur les systèmes Novell NetWare, 126
sur les systèmes SCO, 116
sur les systèmes Solaris, 97
sur les systèmes UNIX, 142
sur les systèmes Windows, 87
sur systèmes HP OpenVMS, 132
sur systèmes MPE/iX, 139
cluster
changement de composants logiciels, 242
désinstallation, 231
importation dans une cellule, 208
installation des clients, 197, 200, 201
installation des intégrations, 148
installation du Gestionnaire de cellule, 188
Microsoft Cluster Server, exportation d'une cellule, 213
cluster IBM HACMP
installation des clients, 203
commande, 251, 318, 398
commande infs, 412
commande ioscan, 409, 412, 414
commande omnicheck, 229, 334
commande omnisetup.sh
installation, 143, 182
mise à niveau, 251, 254
commande omnisv, 251
commandes
infs, 412
ioscan, 409, 412, 414
modifications apportées à l'interface en ligne de commande, après mise à niveau, 445
netstat, 398
omnicc, 318
omnicheck, 229, 334
omnikeymigrate, 250
omnisetup.sh, 143, 182, 251
omnisetup.sh , 254
omnisv, 251
composants d'installation
Agent de disque, 30
Agent de support, 30
Agent de support général, 30
Agent de support NDMP, 30
interface utilisateur, 29
Serveur d'installation, 29
composants logiciels
ajout, sous HP-UX, 243
ajout, sous Solaris, 244
ajout, sous Windows, 242
changement, présentation, 242
changement, sur des clients cluster, 242
codes composants, 143
dépendances, sous HP-UX, 243
dépendances, sous Solaris, 244
présentation, 73
suppression, sous UNIX, 243
suppression, sous Windows, 242

concepts
agent de disque, 30
agent de support, 30
Agent de support NDMP, 30
cellule, 29
client, 29
conversion de nom de fichier de l'IDB, 277
environnement de sauvegarde, 29
exportation, 211
Gestionnaire de cellule, 29
importation, 205
installation distante, 32
interface graphique utilisateur (GUI), 37, 38
interface utilisateur, 29
Serveur d'installation, 29
concepts d'environnement de sauvegarde, 29
configuration
Agent de disque, sur HP OpenVMS, 136
Agent de support sous Novell NetWare, 130
Agent de support, sur HP OpenVMS, 137
clients avec Veritas Volume Manager, sur Microsoft Cluster Server, 441
clients Solaris, après l'installation, 99
clients Solaris, avant l'utilisation des périphériques de sauvegarde, 417
fichier sst.conf, 419
fichier st.conf, 99, 417
Gestionnaire de cellule avec Veritas Volume Manager, sur MSCS, 441
noyau, sur des clients Linux, 107
robot SCSI, sous HP-UX, 407
TCP/IP, sous Windows, 391
configuration requise
auto-migration VLS, 179
IAP, 178
installation de Gestionnaire de cellule, sous UNIX, 44
installation de Gestionnaire de cellule, sous Windows, 52
installation de Serveur d'installation, sous UNIX, 62
installation de Serveur d'installation, sous Windows, 65
mise à niveau à partir de Data Protector A.05.10, A.05.50 et A.06.00, 251
connexion de périphériques de sauvegarde
bibliothèque HP StorageWorks DLT 28/48 logements, 430
chargeur automatique HP Surestore 12000e, 428
clients AIX, 111
clients HP-UX, 96
clients Linux, 108
clients SCO, 117
clients Siemens Sinix, 112
clients Solaris, 102
clients sous Windows, 92
clients Tru64, 115
lecteur de bande DAT 24 HP StorageWorks, 426
lecteur de bande Seagate Viper 200 LTO, 434
lecteurs de bibliothèque ADIC/GRAU, 119
présentation, 423
contrôleur SCSI
Voir interface SCSI
conventions
typographie, 26
conversion de nom de fichier de l'IDB
concepts, 277
conversion des noms de fichier
Voir conversion de nom de fichier de l'IDB
correctifs
commande omnicheck, 229
vérification, 228

création
fichiers de périphérique, sous HP-UX, 412
fichiers de périphérique, sous Solaris, 420
fichiers de périphérique, sous Windows, 406
fichiers de trace de l'exécution, installation, 347
croissance de la base de données
Voir IDB
CRS
Voir service Cell Request Server (CRS)
cryptage
auto-migration des clés de cryptage, 250

D

DCBF
Voir fichiers binaires de catalogue des détails
débogage de l'installation, 348
définition
ID SCSI, pour une bibliothèque HP StorageWorks 330fx, 422
paramètres du contrôleur SCSI, sous Windows, 414
variables d'environnement, sous Gestionnaire de cellule UNIX, 51
démarrage
GUI, UNIX, 37
démon swagent, 340
dépannage de l'interface utilisateur localisée, 183
déplacement des licences, 329
désactivation des pilotes de robots SCSI, sous Windows, 404
désinstallation
clients cluster, 231
clients, à distance, 231
clients, de HP OpenVMS, 232
configuration requise, 230
Gestionnaire de cellule, de MC/ServiceGuard, 234
Gestionnaire de cellule, sous HP-UX, 234
Gestionnaire de cellule, sous Linux, 239
Gestionnaire de cellule, sous Windows, 232, 237
particularités de l'intégration Oracle, 244
présentation, 230
Serveur d'installation, de MC/ServiceGuard, 234
Serveur d'installation, sous HP-UX, 234
Serveur d'installation, sous Linux, 240
Serveur d'installation, sous UNIX, 238
Serveur d'installation, sous Windows, 232
utilitaire AutoPass, sous HP-UX, 234
utilitaire AutoPass, sous Solaris, 238
utilitaire AutoPass, sous Windows, 233
utilitaire pkgrm, 237
utilitaire rpm, 239
détermination
adresse SCSI non utilisées, sous HP-UX, 414
adresses SCSI non utilisées, sous Solaris, 416
adresses SCSI non utilisées, sous Windows, 421
licences installées, 329
mots de passe requis pour l'attribution de licences, 320
DNS
commande omnicheck, 334
vérification des connexions dans une cellule, 334

document
conventions, 26
documentation connexe, 19
documentation
commentaires, 28
site Web de HP, 19
documentation connexe, 19
droits d'accès
ajout au compte root, sous Linux, 105
DVD-ROM
liste des DVD-ROM d'installation, 34

E

Edition serveur unique
installation, 184
limites, 184
mise à niveau de plusieurs installations, 285
mise à niveau vers Data Protector A.06.10, 284, 285
présentation des produits, licences, 350
types de licence, 363
exportation
client Microsoft Cluster Server, 213
clients, 212
Extensions fonctionnelles, licences, 307

F

fichier allow_hosts, 220, 222
fichier cell_info, 245
fichier de périphérique
création, sous HP-UX, 412
création, sous Solaris, 420
création, sous Windows, 406
fichier deny_hosts, 222
fichier global, 261
fichier HPDEVBRA.NLM, 440
fichier HPUMA.NLM, 440
fichier inet.log, 220, 223, 302
fichier installation_servers, 65
fichier nsswitch.conf, 402
fichier omni_info, 245
fichier omnirc, 262
fichier services, 398
fichier sst.conf, 419
fichier st.conf, 99, 417
fichiers
allow_hosts, 220
HPDEVBRA.NLM, 440
allow_hosts, 221, 222
deny_hosts, 222
HPUMA.NLM, 440
services, 398
fichiers binaires de catalogue des détails
modification manuelle de la taille maximale par défaut, 262
fichiers de configuration
cell_info, 245
fichier st.conf, 99
fichiers configurés automatiquement, sous Gestionnaire de cellule UNIX, 49
global, 261
inet.conf, 402
installation_servers, 65
modification, installation de clients Solaris, 99
modifications, après mise à niveau, 442
nsswitch.conf, 402
omni_info, 245
omnirc, 262
problèmes de mise à niveau, 343
sst.conf, 419
st.conf, 417
vérification des changements de configuration après mise à niveau à partir de Data Protector A.05.10, A.05.50 et A.06.00, 261
fichiers de trace de l'exécution
création, 348
option debug, 347
fichiers de trace.
Voir fichiers de trace de l'exécution
fichiers journaux
description, 347
emplacement, 346
inet.log, 220, 223, 302
vérification de l'installation, 345

formulaires d'attribution de licences, 369

G

Génération de rapports Web, installation, 185
Gestionnaire de cellule, 51
  changement de composants logiciels, 242
  choix du système, 35
  concepts, 29
  concepts de sécurité, 214
  configuration des variables d'environnement, sous UNIX, 51
  configuration pour Veritas Volume Manager, sur Microsoft Cluster Server, 441
  configuration requise pour l'installation, sous UNIX, 44
  configuration requise pour l'installation, sous Windows, 52
  désinstallation, de MC/Service-Guard, 234
  désinstallation, de Solaris, 237
  désinstallation, sous HP-UX, 234
  désinstallation, sous Linux, 239
  désinstallation, sous Windows, 232
  fichiers configurés automatiquement, sous UNIX, 49
  fonctions, 35
  installation, sous HP-UX, 46
  installation, sous HP-UX, à l'aide d'outils natifs, 373
  installation, sous Linux, à l'aide d'outils natifs, 377
  installation, sous Solaris, à l'aide d'outils natifs, 375
  installation, sous Windows, 52
  installation, sur MC/ServiceGuard, 186
  installation, sur Microsoft Cluster Server, 188
  installation, sur Solaris, 46
  mise à niveau à partir de Data Protector A.05.10 et A.05.50, sous HP-UX, 254
  mise à niveau à partir de Data Protector A.05.10, A.05.50 et A.06.00, sous HP-UX, 251
  mise à niveau à partir de Windows NT vers une nouvelle version de Windows, 288
  mise à niveau de l'Edition serveur unique, 285
  mise à niveau manuelle, sous UNIX, 345
  mise à niveau, sur MC/Service-Guard, 298
  mise à niveau, sur Microsoft Cluster Server, 302
  modification du nom, 397
  préparation d'un serveur NIS, 401
  résolution des problèmes, 336, 338, 343, 345, 347
  résolution des problèmes d'installation, sous UNIX, 52
  séquence d'installation, 42
  serveur gestionnaire de clés (KMS), 51
  service Cell Request Server (CRS), 51, 59
  service du serveur gestionnaire de clés (KMS), 60
  service Media Management Daemon (MMD), 51, 60
  service Raima Database Server (RDS), 51, 60
  service UIProxy, 60
  structure des répertoires, sous UNIX, 48
  vérification des changements de configuration, 261
Gestionnaire de cellule
  résolution des problèmes, 52

Gestionnaire de cellule HP-UX
configuration des variables d'environnement, 51
configuration requise pour l'installation, 44
désinstallation, 234
fichiers configurés automatiquement, 49
installation, 46
installation, utilisation d'outils natifs, 373
migration de PA-RISC vers IA-64, 289
mise à niveau à partir de Data Protector A.05.10 et A.05.50, 254
mise à niveau à partir de Data Protector A.05.10, A.05.50 et A.06.00, 251
résolution des problèmes, 52, 343, 345
résolution des problèmes d'installation, 52
structure des répertoires, 48
Gestionnaire de cellule Linux
configuration des variables d'environnement, 51
configuration requise pour l'installation, 44
désinstallation, 239
fichiers configurés automatiquement, 50
installation, 46
installation, utilisation d'outils natifs, 377
résolution des problèmes, 52
résolution des problèmes d'installation, 52
structure des répertoires, 48
Gestionnaire de cellule Solaris
configuration des variables d'environnement, 51
configuration requise pour l'installation, 44
désinstallation, 237
fichiers configurés automatiquement, 50
installation, 46
installation, utilisation d'outils natifs, 375
résolution des problèmes, 338, 343, 345
résolution des problèmes d'installation, 52
structure des répertoires, 48
Gestionnaire de cellule Windows
configuration requise pour l'installation, 52
désinstallation, 232
installation, 52
migration de 32 bits vers 64 bits, 294
résolution des problèmes, 336, 343
résolution des problèmes d'installation, 61

H

HP
support technique, 27

I

IAP
configuration requise, 178
IDB
croissance, 36
résolution des problèmes de mise à niveau, 343

importation
clients, 205
clients cartes LAN multiples, 207
clients HP OpenVMS, 207
clients NDMP, 207
clusters, 208
périphérique VLS, 207
Serveur d'installation, 207
serveur IAP, 207
inet.conf
fichier, 402
installation
à distance, concepts, 32
Agent de support pour ACS bibliothèque StorageTek, 118
Agent de support pour bibliothèque ADIC/GRAU, 118
agent de support pour bibliothèque ADIC/GRAU, 120
agent de support pour bibliothèque StorageTek ACS, 125
clients compatibles cluster, 187, 197, 200, 201, 203
clients d'auto-migration VLS, 179
clients en local, 87, 132, 139, 142
clients IAP, 178
codes des composants logiciels, 143
composants
Voir composants d'installation
composants logiciels, 73
création de fichiers de trace de l'exécution, 348
débogage, 348
dépannage, sous Windows, 336
Edition serveur unique, 184
étapes générales, 31
fichiers journaux, 345
Gestionnaire de cellule compatible cluster, 186, 188
installation des clients, présentation, 70
installation distante, présentation, 78
intégration DB2, 153
intégration de HP StorageWorks EVA, 171
intégration HP StorageWorks Disk Array XP, 159
intégration HP StorageWorks VA, 165
intégration Informix, 150
intégration Lotus, 154
intégration Microsoft Exchange, 149
intégration Microsoft SharePoint Portal Server, 150
intégration Microsoft SQL, 149
intégration Microsoft Volume Shadow Copy, 153
intégration NDMP, 153
intégration NNM, 153
intégration Oracle, 152
intégration SAP DB, 151
intégration SAP R/3, 151
intégration Sybase, 150
Intégration VMware, 152
intégrations, 145
intégrations compatibles cluster, 148
intégrations, présentation, 145
interface utilisateur localisée, 180
mots de passe permanents, 322, 328
omnisetup.sh, 239
présentation, 29
Rapports Web, 185
résolution des problèmes de clients, sous UNIX, 339
résolution des problèmes liés au Gestionnaire de cellule, sous Solaris, 338
résolution des problèmes liés aux clients, sous Windows, 340
utilitaire AutoPass, sous UNIX, 47
utilitaire AutoPass, sous Windows, 58
utilitaire pkgadd, 238
vérification des clients, 342
installation de Gestionnaire de cellule
installation, sous HP-UX, à l'aide d'outils natifs, 373
installation de Serveur d'installation
système sous HP-UX, à l'aide d'outils natifs, 379

installation des clients
sur des systèmes de clusters IBM HACMP, 203
sur des systèmes HP-UX, 94
sur des systèmes Novell NetWare Cluster Services, 201
sur des systèmes Siemens Sinix, 112
sur des systèmes Tru64, 114
sur des systèmes Veritas Cluster, 200
sur les systèmes AIX, 110
sur les systèmes ESX Server, 109
sur les systèmes Linux, 103
sur les systèmes MC/ServiceGuard, 187
sur les systèmes Microsoft Cluster Server, 197
sur les systèmes Novell NetWare, 126
sur les systèmes SCO, 116
sur les systèmes Solaris, 97
sur les systèmes UNIX, 142
sur les systèmes Windows, 87
sur système HP OpenVMS, 132
sur systèmes MPE/iX, 139
installation distante
clients, 78
intégrations, 148
résolution des problèmes, sous Linux, 105
installation du Gestionnaire de cellule
configuration requise, sous UNIX, 44
configuration requise, sous Windows, 52
sur des systèmes HP-UX, 46
sur les systèmes Linux, 46
sur les systèmes MC/ServiceGuard, 186
sur les systèmes Microsoft Cluster Server, 188
sur les systèmes Solaris, 46
sur les systèmes Windows, 52
système sous Linux, à l'aide d'outils natifs, 377
système sous Solaris, à l'aide d'outils natifs, 375
installation du Serveur d'installation
configuration requise, sous UNIX, 62
configuration requise, sous Windows, 65
présentation, 61
sur les systèmes UNIX, 62
sur les systèmes Windows, 65
système sous Linux, à l'aide d'outils natifs, 384
système sous Solaris, à l'aide d'outils natifs, 380
installation en local, clients, 87, 132, 139, 142
Integrated Archive Platform (IAP)
installation, 178
intégration DB2, installation, 153
intégration de HP StorageWorks EVA
installation, 171
intégration EVA
mise à niveau à partir de Data Protector A.05.10 et A.05.50, 273
intégration HP StorageWorks Disk Array XP
installation, 159
intégration HP StorageWorks VA
installation, 165
Intégration Informix
mise à niveau à partir de Data Protector A.05.10 et A.05.50, sous UNIX, 268
intégration Informix
mise à niveau à partir de Data Protector A.05.10 et A.05.50, sous Windows, 269
intégration Informix, installation, 150
intégration Lotus, installation, 154
intégration Microsoft Exchange
installation, 149
installation sur systèmes avec HP StorageWorks Disk Array XP, 164
installation sur systèmes avec HP StorageWorks EVA, 177
installation sur systèmes avec HP StorageWorks VA, 171

intégration Microsoft SharePoint Portal Server
installation, 150
intégration Microsoft SQL
installation, 149
installation sur les systèmes avec baie de disques EMC Symmetrix, 159
installation sur systèmes avec HP StorageWorks Disk Array XP, 165
installation sur systèmes avec HP StorageWorks EVA, 177
installation sur systèmes avec HP StorageWorks VA, 171
intégration Microsoft Volume Shadow Copy, installing, 153
intégration NDMP, installation, 153
intégration NNM, installation, 153
intégration Oracle
installation, 152
installation sur les systèmes avec baie de disques EMC Symmetrix, 155
installation sur systèmes avec HP StorageWorks Disk Array XP, 160
installation sur systèmes avec HP StorageWorks EVA, 172
installation sur systèmes avec HP StorageWorks VA, 166
mise à niveau à partir de Data Protector A.05.10 et A.05.50, 265
particularités de la désinstallation, 244
intégration SAP DB, installation, 151
intégration SAP R/3
installation, 151
installation sur les systèmes avec baie de disques EMC Symmetrix, 156
installation sur systèmes avec HP StorageWorks Disk Array XP, 161
installation sur systèmes avec HP StorageWorks EVA, 174
installation sur systèmes avec HP StorageWorks VA, 168
mise à niveau à partir de Data Protector A.05.10 et A.05.50, 267
Intégration Sybase
mise à niveau à partir de Data Protector A.05.10 et A.05.50, sous UNIX, 270
intégration Sybase
mise à niveau à partir de Data Protector A.05.10 et A.05.50, sous Windows, 272
intégration Sybase, installation, 150
Intégration VMware
installation, 152
intégrations
EVA, 273
installation compatibles cluster, 148
installation distante, 148
installation en local, 148
mise à niveau de SAP R/3, sous Windows, 267
mise à niveau de Sybase, sous UNIX, 270
mise à niveau de Sybase, sous Windows, 272
mise à niveau d'Informix, sous UNIX, 268
mise à niveau d'Informix, sous Windows, 269
mise à niveau d'Oracle, sous Windows, 265
mise à niveau EVA, 273
Oracle, sous UNIX, 265
présentation, 146
SAP R/3, sous UNIX, 267

intégrations, installation
intégration DB2, 153
intégration de HP StorageWorks EVA, 171
intégration HP StorageWorks Disk Array XP, 159
intégration HP StorageWorks VA, 165
intégration Informix, 150
intégration Lotus, 154
intégration Microsoft Exchange, 149
intégration Microsoft SharePoint Portal Server, 150
intégration Microsoft SQL, 149
intégration Microsoft Volume Shadow Copy, 153
intégration NDMP, 153
intégration NNM, 153
intégration Oracle, 152
intégration SAP DB, 151
intégration SAP R/3, 151
intégration Sybase, 150
Intégration VMware, 152
interface de ligne de commande (CLI), 29, 37
interface graphique
Voir interface graphique utilisateur
Interface graphique Java de Data Protector
modification du numéro de port par défaut, 400
interface graphique Java de Data Protector
ajout de clients à la cellule, 79
interface graphique Java de Data Protector , 104
interface graphique utilisateur (GUI)
concepts, 37, 38
démarrage, UNIX , 37
vues, 38
interface SCSI
ajout de pilote de robot au noyau, sous HP-UX, 410
configuration de robot SCSI, sous HP-UX, 407
configuration des paramètres du contrôleur, sous Windows, 414
définition ID, pour une bibliothèque HP StorageWorks 330fx, 422
désactivation des pilotes de robots, sous Windows, 404
détermination des adresses non utilisées, sous HP-UX, 414
détermination des adresses non utilisées, sous Solaris, 416
détermination des adresses non utilisées, sous Windows, 421
utilisation de lecteurs de bandes, sous Windows, 402
interface utilisateur
Voir interface de ligne de commande (CLI), interface graphique utilisateur (GUI)
choix du système, 37
concepts, 29
dépannage de l'installation de l'interface utilisateur localisée, 183
installation de l'interface utilisateur localisée, 180
interface utilisateur graphique (GUI)
interface graphique Java de Data Protector, 37
interface graphique Java de Data Protector , 74
interface utilisateur localisée, 180
Voir aussi Interface utilisateur
internationalisation, IDB, 277

J

journalisation excessive, 223

K

KMS
Voir service du serveur gestionnaire de clés (KMS)

L

lecteur de bande DAT 24 HP StorageWorks, connexion, 426
lecteur de bande Seagate Viper 200 LTO, connexion, 434
lecteurs de bandes
  Voir interface SCSI
lecteurs de bandes SCSI.
  Voir interface SCSI
licence d'utilisation., 319
licences, 319
licences A.05.10, A.05.50 ou A.06.00, 365
licences de lecteur, 307
licences d'utilisation, 319
licences liées, 308
limites
  Edition serveur unique, 184
  mise à niveau, 248
  mise à niveau de Manager-of-Managers, 249
  sur les systèmes Windows, 66, 88
liste de systèmes autorisés, sécurité, 218

M

Manager-of-Managers
  mise à niveau à partir de Data Protector A.05.10 et A.05.50, 276
  présentation de la mise à niveau, 249
masque de sous-réseau, TCP/IP, 392
MC/ServiceGuard
  désinstallation de Gestionnaire de cellule, 234
  désinstallation de Serveur d'installation, 234
  importation, 210
  installation des clients, 187
  installation du Gestionnaire de cellule, 186
  journalisation excessive dans un fichier inet.log, 223
  mise à niveau à partir de Data Protector A.05.10, A.05.50 et A.06.00, 264
  mise à niveau du Gestionnaire de cellule, 298
Media Management Daemon (MMD), 60
Microsoft Cluster Server
  configuration de clients avec Veritas Volume Manager, 441
  configuration de Gestionnaire de cellule avec Veritas Volume Manager, 441
  exportation, 213
  importation, 208
  installation des clients, 197
  installation du Gestionnaire de cellule, 188
  mise à niveau de clients, 305
  mise à niveau du Gestionnaire de cellule, 302
Microsoft Installer, 54, 248, 302, 337
migration
  Gestionnaire de cellule sous HP-UX, PA-RISC vers IA-64, 289
  Gestionnaire de cellule sous Windows, 32 bits vers 64 bits, 294
  licences, 364
minimisation du trafic réseau sur les clients Novell NetWare, 130

mise à niveau
Application Recovery Manager, 286
avant la mise à niveau, 247
commande omnisetup.sh, 254
commande omnisv, 251
de Windows NT vers une nouvelle version de Windows, 288
dépannage, sous Windows, 336, 343
fichier global , 261
fichier omnirc, 262
limites, 248
manuelle, sous UNIX, 345
modification des fichiers de configuration, 442
modifications apportées à l'interface en ligne de commande, 445
omnisetup.sh, 251
présentation, 247
résolution des problèmes de la base IDB, 343
résolution des problèmes, sous UNIX, 343
séquence, 248
SSE vers Data Protector A.06.10, 284, 285
mise à niveau à partir de Data Protector, 365
mise à niveau à partir de Data Protector A.05.10 et A.05.50
Gestionnaire de cellule sous HP-UX, 254
Intégration de Sybase, sous UNIX, 270
intégration EVA, 273
Intégration Informix, sous UNIX, 268
Intégration Informix, sous Windows, 269
intégration Oracle, 265
intégration SAP R/3, 267
Intégration Sybase, sous Windows, 272
Manager-of-Managers, 276
mise à niveau à partir de Data Protector A.05.10, A.05.50 et A.06.00
clients, 263
clients, sur MC/ServiceGuard, 264
clients, sur Microsoft Cluster Server, 305
commande omnisv, 251
configuration requise, 251
Gestionnaire de cellule sous HP-UX, 251
Gestionnaire de cellule, sur MC/ServiceGuard, 298
Gestionnaire de cellule, sur Microsoft Cluster Server, 302
présentation, 250
Serveur d'installation sous HP-UX, 251
Serveur d'installation sous Windows, 256
vérification des changements de configuration, 261
Mise à niveau vers HP-UX 11.23, 289
MMD
Voir service Media Management Daemon (MMD)
modification
composants logiciels, 242
nom du Gestionnaire de cellule, 397
port par défaut, 398
MSI.
Voir Microsoft Installer

N

netstat, 398
noms de fichier
conversion
Voir conversion de nom de fichier de l'IDB
encodage
Voir conversion de nom de fichier de l'IDB
Novell NetWare Cluster Services
importation, 210
installation des clients, 201
limites, basculement, 201

noyau
ajout de pilote de robot SCSI, sous HP-UX, 410
configuration sur des clients Linux, 107
recréation, sous HP-UX, 410
nsswitch.conf
fichier, 402

O

obtention de mots de passe permanents pour les licences, 322, 328
omnicc, 318
omnisetup.sh, 239
option debug
présentation, 347
outil de vérification DNS, 397

P

Packs Starter, licence, 307
passerelle par défaut, TCP/IP, 392
périphérique VLS, importation, 207
périphériques de sauvegarde
définition d'ID SCSI, pour une bibliothèque HP StorageWorks 330fx, 422
périphériques de sauvegarde, connexion
bibliothèque HP StorageWorks DLT 28/48 logements, 430
chargeur automatique HP Surestore 12000e, 428
clients AIX, 111
clients HP-UX, 96
clients Linux, 108
clients SCO, 117
clients Siemens Sinix, 112
clients Solaris, 102
clients sous Windows, 92
clients Tru64, 115
lecteur de bande DAT 24 HP StorageWorks, 426
lecteur de bande Seagate Viper 200 LTO, 434
lecteurs de bibliothèque ADIC/GRAU, 119
présentation, 423
port par défaut, modification, 398
préparation d'un serveur NIS, 401

présentation
attribution des licences, 319
changement de composants logiciels, 242
composants logiciels, 73
connexion de périphériques de sauvegarde, 423
désinstallation, 230
fichiers de trace de l'exécution, 347
importation de packages de clusters d'applications, 208
importation d'un client compatible cluster, 208
installation de Serveur d'installation, 61
installation des clients, 70
installation des intégrations, 145
installation des intégrations compatibles cluster, 148
installation distante de clients, 78
intégrations, 146
mise à niveau, 247
mise à niveau à partir de Data Protector A.05.10, A.05.50 et A.06.00, 250
option debug, 347
structure du produit, 307
processus
Media Management Daemon (MMD), 60
serveur gestionnaire de clés (KMS), 51, 60
service Cell Request Server (CRS), 51, 59
service Inet, 51, 60
service Media Management Daemon (MMD), 51
service Raima Database Server (RDS), 51, 60
service UIProxy, 60
processus omniinet
Voir service Inet
public, 19

R

RDS
Voir service Raima Database Server (RDS)
recréation du noyau, sous HP-UX, 410
refus d'accès par des hôtes, 222
résolution des problèmes de mise à niveau
Base IDB non disponible, 343
correctifs Data Protector, 343
fichiers de configuration non disponibles, 343
logiciel Data Protector, sous Windows, 336
problèmes liés à Microsoft Installer, 336
résolution des problèmes d'installation
clients, sous HP-UX, 339
commande omnicheck, 334
débogage, 348
démon swagent, 340
fichiers de trace de l'exécution, 347
fichiers journaux, 345
Gestionnaire de cellule, sous Solaris, 338
Gestionnaire de cellule, sous UNIX, 52
Gestionnaire de cellule, sous Windows, 61
installation à distance, sous Linux, 105
installation à distance, sous UNIX, 339
installation à distance, sous Windows, 340
interface utilisateur localisée, 183
logiciel Data Protector, sous Windows, 336
option debug, 347
problèmes liés à Microsoft Installer, 336
robots
Voir interface SCSI
robots
Voir interface SCSI
robots SCSI
Voir interface SCSI

S

sécurisation
cellule, 220
client, 218
sécurité
activation de la sécurité pour un client, 218
activation de la sécurité pour une cellule, 220
fichier allow_hosts, 220, 222
fichier deny_hosts, 222
journalisation excessive dans un fichier inet.log, 223
liste de systèmes autorisés, 218
problèmes potentiels, 217
refus d'accès par des hôtes, 222
suppression de la vérification d'accès sur un client, 222
Serveur d'installation
concepts, 29
configuration requise pour l'installation, sous UNIX, 62
configuration requise pour l'installation, sous Windows, 65
désinstallation, de MC/ServiceGuard, 234
désinstallation, sous HP-UX, 234
désinstallation, sous Linux, 240
désinstallation, sous UNIX, 238
désinstallation, sous Windows, 232
importation dans une cellule, 207
installation, sous HP-UX, à l'aide d'outils natifs, 379
installation, sous Linux, à l'aide d'outils natifs, 384
installation, sous Solaris, à l'aide d'outils natifs, 380
installation, sous UNIX, 62
installation, sous Windows, 65
mise à niveau à partir de Data Protector A.05.10, A.05.50 et A.06.00, sous HP-UX, 251
mise à niveau manuelle, sous UNIX, 345
présentation de l'installation, 61
séquence d'installation, 42
structure des répertoires, sous UNIX, 48
Serveur d'installation A.05.10, A.05.50 et A.06.00, sous Windows
mise à niveau à partir de Data Protector, 256
Serveur d'installation HP-UX
installation, utilisation d'outils natifs, 379
Serveur d'installation Linux
installation, utilisation d'outils natifs, 384
Serveur d'installation Solaris
installation, utilisation d'outils natifs, 380
serveur d'interface Java, 45, 53, 60
modification du numéro de port, 400

serveur gestionnaire de clés (KMS), 51, 60
serveur IAP, importation, 207
serveur NIS, préparation, 401
serveur virtuel, importation dans une cellule, 208
service Cell Request Server (CRS), 51, 59
service Inet, 51, 60
service Media Management Daemon (MMD), 51
service Raima Database Server (RDS), 51, 60
service UIProxy, 60
signalement des licences manquantes, 307
sites Web
  HP , 28
  HP Subscriber's Choice for Business, 28
  manuels produits, 19
SSE, 284
SSE.
  Voir Edition serveur unique
STK ACS
  Voir bibliothèque ACS StorageTek
Subscriber's Choice, HP, 28
support technique
  HP, 27
  localisateur de services, site Web, 28
suppression
  composants logiciels, présentation, 242
  composants logiciels, sous UNIX, 243
  composants logiciels, sous Windows, 242
  Data Protector, manuellement, sous UNIX, 241
  vérification d'accès sur un client, 222
système de noms de domaine
  Voir DNS
système d'exploitation
  mise à niveau de Windows NT vers une nouvelle version de Windows, 288

T

TCP/IP
  adresse IP, 392
  configuration, sous Windows, 391
  masque de sous-réseau, 392
  passerelle par défaut, 392
  vérification de la configuration, sous Windows, 395

U

utilisation
  fichiers journaux, 345
  licences, 247, 250
  pilotes de bandes SCSI, sous Windows, 402
utilitaire AutoPass
  attribution des licences, 322
  désinstallation, sous HP-UX, 234
  désinstallation, sous Solaris, 238
  désinstallation, sous Windows, 233
  installation, sous UNIX, 47
  installation, sous Windows, 58
utilitaire pkgadd, 238
utilitaire pkgrm, 237
utilitaire rpm, 239

V

variables d'environnement, configuration sous Gestionnaire de cellule UNIX, 51

vérification
configuration TCP/IP, sous Windows, 395
connexions DNS dans une cellule, 334
correctifs, 228
fichiers journaux, installation, 345
installation de l'Agent général de support, sous Novell NetWare, 436
installation des clients, 342
installation sur les clients, 342
licences, 307
mots de passe de licences, 328
Veritas Cluster
importation, 210
installation des clients, 200
limites, basculement, 200
Veritas Volume Manager
configuration de clients, sur Microsoft Cluster Server, 441
configuration de Gestionnaire de cellule, sur Microsoft Cluster Server, 441
vues, interface graphique utilisateur, 38

W

Windows NT, mise à niveau vers une nouvelle version de Windows, 288